جمهورية العراق
وزارة التعليم العالي والبحث العلمي
الجامعة التكنولوجية

تقويم فاعلية المنحنيات الاهليلجية في أنظمة التشفير

رسالة

مقدمة إلى قسم العلوم التطبيقية في الجامعة التكنولوجية وهي جزء من متطلبات نيل درجة ماجستير علوم في الرياضيات التطبيقية

من قبل

شاكر محمود سلمان العزاوي

بإشراف

الاستاذ الدكتور المهندس

ستار بدر سدخان المالكي

ذو القعدة ١٤٢٣هـ **كانون الثاني ٢٠٠٣م**

إقــرار المشــرف

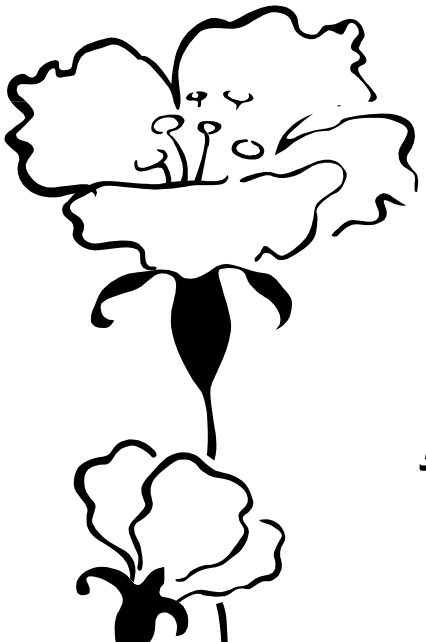
أشـهد إن إعداد هذه الرسالة الموسومة ((تقويم فاعلية المنحنيات الاهليلجية في أنظمة التشفير **)) والمقدمة من قبل الطالب (**شاكـر محمـود سلـمان**) تمت تحت إشرافي في قسم العلوم التطبيقية / الجامعة التكنولوجية ، وهي جزء من متطلبات نيل درجة ماجستير علوم في الرياضيات التطبيقية.**

التوقيـــــــــع:
الاستاذ الدكتور المهندس
ستـار بـدر سدخان المالـكي
شركة الميلاد العامة/ هيئة التصنيع العسكري

إقــرار المقــوّم اللغــوي

أُقر بأن إعداد هذه الرسالة الموسومة ((تقويم فاعلية المنحنيات الاهليلجية في انظمة التشفير)) **والمقدمة من الطالب** ((شاكــر محمــود سلــمان)) **في قسم العلوم التطبيقية فرع الرياضيات التطبيقية ، قد تمت مراجعتها من الناحية اللغوية تحت اشرافي وبذلك اصبحت بأسلوب سليم خالٍ من الاخطاء والتعبيرات اللغوية غير الصحيحة ولأجله وقعت .**

التوقيــع :
الاســم : أ.د. جاسم الحلو
المرتبة العلمية : أستـاذ
التاريــخ : / ١ / ٢٠٠٣



الإهـــــداء

إلى الواحد الأحد الفرد الصمد... رافع السماء بلا عمد

إلى مدينة العلم اهدي اقل من قطرة لأعظم بحر

إلى من اختار الطريق الاصعب من اجلنا

إلى عنوان التضحية ورمز الإيثار ... والدي العزيز

إلى من سهرت الليالي لترعاني ... أمي الغالية

إلى شموع دربي ومصابيحه ... إخواني وأخواتي الأعزاء

إلى المرآة التي أرى فيها صورتي ... أصدقائي

أهدي باكورة أعمالي

شاكـــر

شُكر وتقدير

الحمد لله رب العالمين والصلاة والسلام على خير الخلق والمرسلين محمد واله الطيبين واصحابه المنتجبين .

لا يسعني في نهاية المطاف ألا أن أتقدم بجزيل الشكر و الامتنان إلى الاستاذ الدكتور المهندس ستار بدر سدخان المالكي لما بذله من جهد سخي ومتابعة قيمة طوال فترة البحث متمنيا له الموفقية الدائمة .

كما أتقدم بالشكر الجزيل إلى أعضاء الهيئة التدريسية في قسم العلوم التطبيقية وبالأخص أساتذة فرع الرياضيات التطبيقية لما أبدوه من تسهيلات في إنجاز هذا البحث .

ويسرني ان اشكر أساتذة قسم الرياضيات في كلية التربية ابن الهيثم ، والدكتور جورج موشي في قسم العلوم التطبيقية ،كذلك الأخوة والأصدقاء صادق عنيد و سعد عبد الكاظم و أريج جعفر و نضال موسى وطالبي الدراسات العليا في الجامعة التكنولوجية رشدي إبراهيم و علي مكي لما أبدوه من مساعدة .

كما اشكر منتسبي المكتبة المركزية في الجامعة التكنولوجية وبالأخص كل من الست زهرة والست سحر والست ثورة ،ومنتسبتي القسم الست ماجدة والست نضال .

واخيرا لا يفوتني ان اشكر كل من اسهم برأي أو أبدى مساعدة مما لا يسمح المجال لذكر أسمائهم وعدم نسيان افضالهم فجزاهم الله عني خيرا.

ومن لا توفي كل كلمات الشكر حقهم أفراد عائلتي لما وفروه لي من الأسباب لاكمال دراستي وبالخصوص والدي العزيز .

ومن الله التوفيق

الباحث

المستخلـــــص

تعد زمرة نقاط المنحنى الاهليلجي (*EC*) (*Elliptic Curve*) اختياراً موفقاً لبناء أنظمة تشفير قائمة على فكرة صعوبة حل مشكلة اللوغاريتم المنفصل في المنحنيات الاهليلجية (*Elliptic curves Discrete Logarithm*) والتي أحدثت تحولاً ملموسا في علم التشفير، ففتحت آفاقا جديدة في التعامل مع زمر خاصة وعمليات غير اعتيادية .

وفي هذا البحث تم استعراض التعريف والخواص الرياضياتية لهذه المنحنيات ودراسة خواص الزمرة المتكونة بنقاطها، والوقوف على كيفية استخدامها في أنظمة التشفير والتقنيات المستخدمة في ذلك، وتناول نقاط القوة في هذه الزمرة والتي جعلتها مناسبة للاستخدام في أنظمة تشفير المفتاح المعلن .

كذلك قدم البحث دراسة تحليلية لبعض طرائق مهاجمة الأنظمة التي توظف الـ (*EC*) وتمييّز نقاط الضعف فيها، إضافة لتصميم برمجيات لتنفيذ بعض هذه الأنظمة التشفيرية وتطبيقها على نصوص مختلفة.

وحصلنا على مبرهنات ونتائج يمكن أن تسهم في تسهيل العمليات الحسابية يعطي البعض منها طرائق استنتاج عدد نقاط منحنيات دون حسابها، واستخدام واحدة من هذه المبرهنات في اقتراح خوارزمية للبحث العشوائي عن منحني بعدد نقاط محدد، إضافة إلى بناء برنامج لعملية ضرب النقطة بعدد صحيح تم فيه جمع كل من خوارزمية الجمع والمضاعفة الاعتيادية وخوارزمية الجمع والمضاعفة باستخدام دالة الاتزان وحساب نظير النقطة، وتم الحصول على فرق في الوقت اللازم للعمليات الحسابية.

قائمة المختصرات

المختـصر	*Term*	المصطلـح
DSA	***Digital Signature Algorithm***	خوارزمية التوقيع الرقمي
ECDSA	***Elliptic Curve Digital Signature Algorithm***	خوارزمية التوقيع الرقمي باستخدام المنحنى الاهليلجي
RSA	***RSA Cryptosystem***	نظام تشفير
ECC	***Elliptic Curves Cryptisystems***	أنظمة تشفير المنحنيات الاهليلجية
$\widetilde{E}$	***Quadratic twist***	التدوير التربيعي للمنحنى
<G>	***Group generated by G***	الزمرة المتولدة بالنقطة G
gcd	***Greatest Common Divisor***	العامل المشترك الأكبر
ECDLP	***Elliptic Curve Discrete Logarithm Problem***	اللوغاريتم المنفصل في المنحنى الاهليلجي
DLP	***Discrete Logarithm Problem***	اللوغاريتم المنفصل
$\|x\rangle$	***Quantum variable x***	المتغير الكمي x
$P^2(k^2)$	***Projective Plane***	المستوى الإسقاطي
EC	***Elliptic Curve***	المنحنى الاهليلجي
$E(F_p)$	***Elliptic Curve Defined Over Finite Field***	المنحنى الاهليلجي المعرف على الحقل F_p
O_E	***Point at Infinity***	النقطة في المالانهاية
q.r	***Quadratic Residue***	باقي تربيعي
q.n.r	***Quadratic Non Residue***	باقي غير تربيعي
w	***Invariant Differential of EC***	ثابت الاشتقاق
j	***Invariant of EC***	ثابت المنحنى الاهليلجي
$p\Theta Q$	***Points Subtraction***	حاصل جمع النقطتين P ونظير النقطة Q
$p \oplus Q$	***Points Addition***	حاصل جمع نقطتين Q,P في المنحنى
F_p	***Finite Field of Characterstic p***	حقل ذو مميز p

$\tilde{\tilde{E}}$	***Lifting of Curve***	مرفوع المنحنى
$GF(p^n)$	***Galois Field***	حقل كالوا
SEA	***Schoof-Elkies-Atkin Algorithm***	خوارزمية سكوف – الكس – اتكن
Z(x)	***Zeta-Function***	دالة Z (Zeta function)
t	***Trace of Curve***	دالة الأثر للمنحني
$DH_{E,G}$	***Diffie-Hellman Function***	دالة دايف – هيلمان
Φ	***Frobenius Mapping***	دالة فروبينس
|G|	***Order of Group G***	رتبة الزمرة
#E	***Number Point of Elliptic Curve E***	رتبة المنحنى (عدد نقاط المنحنى)
$\left(\frac{a}{p}\right)$	***Legendre Symbol for a***	رمز ليجندر للعدد a في الحقل F_p
Z/pZ	***The System of Residue mod p***	نظام البواقي قياس p
$E_{tors}[M]$	***m-Torsion Subgroup***	زمرة الالتواء m
SSSA	***Semaev-Smart-Satoh-Araki Attack***	طريقة مهاجمة سميف – سمارت – ساتو – اراكي
MOV	***Menezes-Okamoto-Vanstone Attack***	طريقة مهاجمة منسيز–اوكاموتو–فنسون
F_R	***FR-Reduction***	طريقة اختزال F_R
χ^*	***Conjugate Characteristic of Group***	مرافق المميز χ
Char.F	***Characteristic Field***	مميز الحقل F
χ	***Characteristic of Group***	مميز الزمرة
Δ	***Discriminant of Curve***	مميز المنحنى
$E_{(a,b)}(F_2e)$	***Subfield Curve***	منحنى الحقل الجزئي
E^M	***EC in Montgomery Form***	منحنى اهليلجي بصيغة مونتجومري

المحتويات

الفصل الثالث

انظمة تشفير المنحنيات الاهليلجية

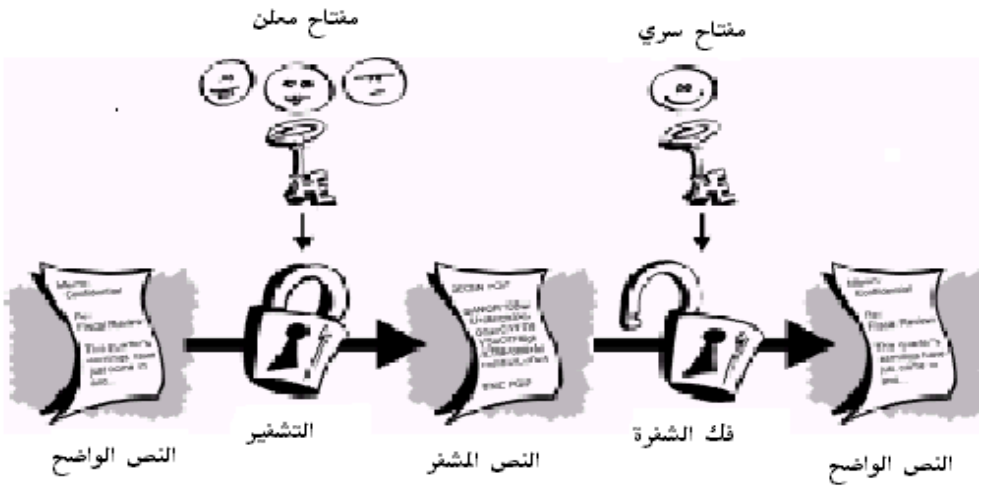
١-١ المقدمة

أخذت تطبيقات علم التشفير تشغل مساحة كبيرة وتكسب اهتماماً واسعاً، وبسبب زيادة استخداماتها في الاتصالات الإلكترونية والتبادلات المالية والمعلومات التجارية أخذت تندفع للأمام من خلال زيادة المتطلبات لتحقيق أكبر قدر من الأمنية لهذه التعاملات في شبكة المعلومات (الانترنيت) وازدادت هذه المتطلبات باستحداث تعاملات البنوك على الشبكة والتسوق بالانترنيت، والحاجة لسرية بعض الأشخاص وتعاملاتهم وما يتعلق بها جعلت على التشفير ان يصل إلى نقاط متقدمة في قيمته التجارية، فضلاً عن تبادل المعلومات العسكرية الخاصة التي كانت هي الأساس لإيجاد أنظمة التشفير في بادئ الأمر. ومن الممكن إن يقال عن التشفير (*Cryptography*) بأنه العلم الذي يوفر أمنية تبادل الرسائل والمعلومات بين المرسل والمستلم. أما أنظمة التشفير (*Crcryptosystems*) فهي عبارة عن مجموعة خوارزميات تشمل خوارزميات لإدخال النص الواضح (*Plaintext*) كشفرة (*encrypt*) وخوارزميات استرجاع النص الواضح من المشفر (*decrypt*) لغرض تحقيق الأمنية المطلوبة ونظرا لتطور الحواسيب وانتشارها بشكل هائل تطورت وتعددت تقنيات التشفير [31].

وتشير الأدبيات إلى أن تاريخ علم التشفير يعود إلى أيام الإمبراطورية الرومانية حيث كان يوليوس قيصر(٢٥٠) قبل الميلاد (*Julius Caesar*) يتبادل المعلومات مع قادته العسكريين برسائل مشفرة وكانوا يستخدمون فكرة إزاحة الحروف [27] والتي تعتمد في استرجاعها على مفتاح سري، وعلى امتداد الزمن أخذت هذه الفكرة تتطور وصارت إزاحة الحروف تتخذ شكل تحويل خطي ومن ثم استخدام المصفوفات وبدأت شيئا فشيئا تتبنى أفكارا رياضياتية اعمق واعقد حسابياً وذلك لتوفير أمنية اكبر. والقاسم المشترك لجميع هذه الأنظمة هو إن معرفة المفتاح السري تكون شرطاً اساسياً لاسترجاع النص الأصلي لذلك تسمى هذه الأنظمة بأنظمة تشفير المفتاح السري.

وفي عام ١٩٧٦م احدث بحث كل من دايف وهيلمان (*Diffie-Hellman*) والموسوم "الاتجاه الجديد في علم التشفير" (*New Direction in Cryptography*) ثورة كبيرة ليس في علم التشفير فحسب بل في مجال الاتصالات بصورة عامة حيث بعد هذا البحث انتفت الحاجة إلى وجود قناة أمينة لتبادل المعلومات السرية وصار بحثهما ولادة لأنواع جديدة من أنظمة التشفير يطلق عليها أنظمة تشفير المفتاح المعلن (*public Key Cryptosystems*)[5] وهذه الأنظمة تستغل بعض الخواص لعدد من الدوال المسماة دوال الاتجاه الواحد (*One*

Way Functions) أو دوال باب المصيدة (*Trapdoor Functions*) وهي دوال سهلة الحساب باتجاه معين ولكنها صعبة جداً ومعقدة بالاتجاه الآخر ألا بشروط معينة [42]. وهو ما سهل تبادل مجموعة من المستخدمين رسائل خاصة على شبكة اتصالات عامة حيث يكون لكل واحد منهم مفتاح معلن خاص به (*Public Key*) ينشره بدليل كدليل الهاتف ويحتفظ هو بالجزء الآخر الخاص وهو المفتاح السري (*Secrete Key*) والذي يجب إن لا يعرفه أحد سواه حيث يمكنه من استرجاع النصوص المرسلة إليه. والشكل (١-١) يوضح مخططاً عاماً لأنظمة تشفير المفتاح المعلن.

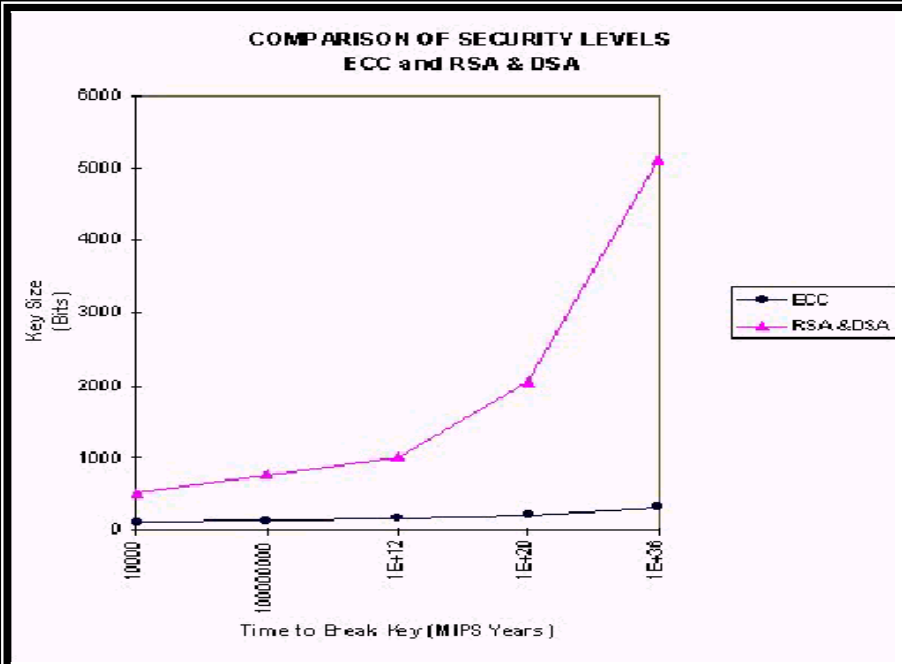


شكل (١-١) : مخطط عام لأنظمة تشفير المفتاح المعلن .

وبتطور تقنيات الاتصالات الحديثة وتنامي سعة وقدرة الحاسوب لجأ العاملون في علم التشفير إلى استخدام بعض الزمر الخاصة (*groups*) وإشراكها بتصميم أنظمة تشفير مناسبة وكانت زمرة نقاط المنحنى الاهليلجي (*Elliptic curve*) واحدة من هذه الزمر والتي حققت نجاحاً كبيراً في هذا المجال، فبعد نجاح لنسترا (*Lenstra*) عام ١٩٨٥ في استخدام المنحنيات الاهليلجية في تجزئة الأعداد إلى حاصل ضرب عددين أوليين (*Integer Factorization*) [27] صار التفكير جدياً لتوظيف هذا المفهوم في أغراض التشفير[5]، بعدها نجح كل من كوبلتز (*Neal Koblitze*) من جامعة (*Washington*) وميللر (*Victor Miller*) من شركة (*IBM*) كل على حدة في تصميم أنظمة تشفير معتمدة على نقاط المنحنيات الاهليلجية وبذلك اصبحت هناك أنظمة تعرف بأنظمة تشفير المنحنيات الاهليلجية (*Elliptic Curve Cryptosystems*) ويرمز لها اختصاراً (*ECC*) وتوصف هذه الانظمة بانها الاسرع والاقوى والأكثر اقتصاداً وتميزاً وملائمةً

للعديد من التطبيقات [5] حيث قام ميللر بتصميم مشابه لنظام دايف – هيلمان (*Diffie-Hellman*). وقدم كوبلتز (*Koblitz*) أنظمة مشابهة لخوارزمية الجمال (*EL-Gamal*) ونظام تشفير ميسي– اومورا (*Massey- Omura*) عام ١٩٨٧م [25] في حين كان أول نظام مشابه لِـ (*RSA*) وثلاث دوال باب المصيدة (*TOFs-Trapdoor One-Way Functions*) جديدة معتمدة على المنحنيات الاهليلجية قدمها عام ١٩٩١م كل من كوياما (*Koyama*) وموريز (*Maurer*) واوكاموتو (*Okamoto*) وفنستون (*Vanstone*) [25].

من الملاحظ إن أنظمة (*RSA*) مع المنحنيات الاهليلجية تعطي أمنية اكبر وان كانت اعقد حسابيا بالإضافة إلى كونها تقاوم بعض أنواع طرائق الهجوم التي لا تعتمد على تحليل الأعداد إلى عواملها الأولية حيث وجد إن الأمنية المتحققة من حجم مفتاح مقداره (1024-*bits*) في (*RSA*) تكافئ الأمنية المتحققة من حجم مفتاح مقداره (128-*bits*) في المنحنيات الاهليلجية وهذه العلاقة لاتكون منتظمة حيث إن أمنية (2048-*bits*) من (*RSA*) مكافئة لتلك المتحققة من (210-*bits*) في (*ECC*) أي إن النسبة تزداد من 1 إلى 7 في الحالة الأولى لتصبح 1 إلى 10 بزيادة حجم المفتاح إلى الضعف، ويوضح الشكل (١–٢) العلاقة بين أمنية كل من (*RSA*) و(*ECC*) من ناحية العلاقة بين حجم المفتاح والزمن المستغرق لكسرها [54].



شكل (١–٢) : مقارنة بين أمنية (RSA) و (ECC)

وفي عام ١٩٩٢ قدم فنستون (*Vanstone*) منظومة خاصة للتوقيع الرقمي باستخدام المنحنيات الاهليلجية كان الأول من نوعه وأطلق عليه خوارزمية التوقيع الرقمي باستخدام المنحنيات الاهليلجية (*Elliptic Curve Digital Signature Algorithm*) والتي يرمز لها اختصاراً (*ECDSA*) بعدها كان هناك العدد من خوارزميات التوقيع الرقمي في الأعوام ١٩٨٨و ١٩٩٩ و ٢٠٠٠ و... [25].

ولتعميم هذا كله يمكن القول إن جميع أنظمة التشفير المعتمدة على اللوغاريتم المنفصل (*Discrete Logarithm*) يمكن تصميم مشابه لها باستخدام المنحنيات الاهليلجية ولكن العكس ليس صحيحاً فقد كانت هناك أنظمة تشفير منحنيات اهليليجية لا يوجد مشابه لها في الأنظمة التي تعتمد على اللوغاريتم المنفصل الاعتيادي مثل نظام منسيز – فنستون (*Menzese-Venston*) [31]. وفي عام ١٩٩٣ قدم ديماتكو (*Demytko*) نظاماً جديداً آخر مشابهاً لأنظمة (*RSA*) [44].

وفي الاتجاه المقابل كانت هناك بحوث ودراسات لإيجاد طرائق مهاجمة لهذه الأنظمة وقد نجح عدد منها في بعض أنواع المنحنيات الاهليلجية، ففي عام ١٩٩١م قدم مينسز (*Menzese*) واوكاموتو (*Okamoto*) وفنستون (*Vanston*) طريقة تحليل (*Cryptanalysis*) لأنظمة (*ECC*) بالاعتماد على خواص بعض المنحنيات، كما قام سمارت (*Smart*) بتقديم طريقة ثانية للتحليل قابلة للتطبيق على نوع آخر من المنحنيات ثم قام كل من ساتوا (*Satoh*) واراكي (*Araki*) عام ١٩٩٧ وكذلك قدم سيميف (*Semeave*) مجموعة خوارزميات من نوع آخر لمهاجمة الأنظمة المعرفة على هذه الأنواع من المنحنيات ونشر ذلك كله عام ١٩٩٨م [5] .

وبرغم هذا كله تبقى أنظمة (*ECC*) هي الأقوى في أمنيتها والاوطأ في كلفتها والأقل في متطلبات سعة الذاكرة. فقد بين أحد الإصدارات لمؤسسة (*Certicom*) البحثية إنها وضعت مجموعة من التحديات تتمثل بالمنافسة لحساب المفاتيح السرية لـ (*ECC*) من مجموعة المفاتيح المعلنة والمتغيرات المقترنة بها وقد وضع ذلك على مستويين الأول كان لحساب مفتاح مكون من (109-*bits*) و(131-*bits*) والآخر كان لحساب مفاتيح تتكون من (163-*bits*) و(191-*bits*) و(239-*bits*) و(359-*bits*) على الترتيب. وقد أمكن حساب (109-*bits*) خلال عدة شهور، فقد تمكن فريق باحثين من مؤسسة (*INRA*) في فرنسا في نيسان عام ٢٠٠٠م من ذلك حيث استغرقت هذه العملية أربعة شهور وتم استخدام 9500 جهاز حاسوب (*Computer*) و

1300 متطوع من 40 دولة وهذا الكم من المتطلبات يساوي 50 مرة من الكمية المطلوبة لكسر نظام (*RSA*) بـ (512-*bits*). هذه النتائج ساندت توقعات العاملين في (*Ceticom*) بأن مفتاحاً مكوناً من (160-*bits*) يمكن نشره حتى للأغراض العسكرية [53]

ويمكن إن نتوقع صعوبة كسر أنظمة (*ECC*) إذ علمنا إن كسر واختراق هذه الأنظمة بحجم مفتاح مقداره (163-*bits*) يتوقع له إن يتطلب جهداً يساوي 100 مليون مرة بقدر الجهد المبذول لكسرها في حالة (109-*bits*) [53].

بقي أن نذكر في هذه المقدمة أن مؤسسة (*Certicom*) تعتبر حاملة لواء أنظمة تشفير المنحنيات الاهليلجية (*ECC*) و اشهر الرقاقات الإلكترونية التي تعتمد في معالجاتها على هذه الأنظمة هي (*Siemens*) والمعروفة بأسم (*Plue-IC*) و(*In finean*) الذي يرمز له (*SLE66XXP*) و(*Motorola*) المعروف بـ(*MPC180X*) وكذلك (*Philips*) بالرمز (*Smart XA*). ومعظم هذه الرقاقات يتم فيها استخدام منحنيات اهليليجية معرفة على حقل أولي (*Prime Field*) [38].

وتوجد مؤسسات أخرى غير (*Certicom*) لها نتاجات وبحوث في ECC مثل مجموعة RSA التي أخذت تُضْمِن ألـ ECC في إصداراتها كذلك المجموعات المعروفة (*Cryptomathic*) و(*Secured*) و(*Entrust*) أيضا تمتلك معالجات لأنظمة تشفير المنحنيات الاهليلجية وغيرها الكثير من الشركات والمؤسسات التي أخذت إمتيازاً من المؤسسة الرئيسية (*Certicom*) [53]. [38].

أما عن الجهد الأكاديمي في قطرنا العزيز، فأن المنحنيات الاهليلجية (*Elliptic Curves*) بصورة عامة لم تحظ باهتمام اغلب الباحثين سواء كانوا في مجال الرياضيات أو الحاسبات حيث– وحسب معلوماتنا– فأن الأعمال في هذا الموضوع لا تتعدى بحثين في اختبارات الأعداد الأولية على مستوى الماجستير أحدهما في قسم الحاسبات [53] فيه تم استخدام المنحنيات الاهليلجية مع خوارزمية (*Coldwasser- Kilian*) لاختبار الأولية حيث بإدخال هذه المنحنيات تم الوصول إلى اختبار أعداد كبيرة نسبياً.

والآخر كان في قسم العلوم التطبيقية [40] قد تطرق أيضا لإستخدام المنحنيات الاهليلجية في الاختبارات الأولية.

١-٢ هدف البحث

يهدف هذا البحث إلى تقويم فاعلية المنحنيات الاهليلجية (*Elliptic Curve*) في أنظمة التشفير وذلك من خلال الجوانب الآتية :-

أ- استعراض التعريف والخواص الرياضياتية للمنحنيات الاهليلجية.

ب- دراسة خواص الزمرة المتكونة بنقاط المنحنى الاهليلجي.

ج- الوقوف على كيفية تطبيق هذه المنحنيات في أنظمة التشفير والتقنيات المستخدمة في ذلك.

د- التعرف على نقاط القوة في زمرة نقاط المنحنى الاهليلجي التي تجعل منها مناسبة للاستخدام في أنظمة تشفير المفتاح المعلن.

هـ- دراسة تحليلية لبعض الطرائق المستخدمة لمهاجمة هذه الأنظمة ونقاط الضعف فيها.

و- تصميم وبناء برمجيات لتنفيذ بعض أنظمة تشفير المنحنيات الاهليلجية على نصوص واضحة مختلفة.

١-٣ محتويات البحث

يشتمل هذا البحث على أربعة فصول بالإضافة إلى الفصل الأول حيث يعرض الثاني الجوانب الرياضياتية الأساسية الجبرية والهندسية وما يتعلق منها بنظرية الأعداد وكذلك الحسابات الكمية في جزئه الأول أما الجزء الآخر فيتم فيه دراسة الخواص الرياضياتية للمنحنيات الاهليلجية وتعريف المنحنى الاهليلجي على حقول الأعداد المختلفة وخواص زمرة المنحنى والعمليات الرياضياتية على النقاط ثم حساب عدد نقاط تلك المنحنيات والتقنيات المستخدمة في ذلك ودراسة بعض أنواع المنحنيات بينما يجري في الفصل الثالث دراسة أنظمة التشفير التي تستخدم هذه المنحنيات وكل ما يتعلق بذلك من أنواع هذه الأنظمة وطرائق مهاجمتها وكيفية اختيار منحني لغرض التشفير وما يتعلق به وكيفية مقاومة بعض طرائق المهاجمة.

أما الفصل الرابع فتم فيه إضافة جهد علمي جديد من خلال وضع ثلاث مبرهنات وبرهان اثنين منها إضافة إلى نتيجة واحدة ، كما يحتوي الفصل على المخططات الانسيابية للبرامج التي تخص الموضوع. علما ان البرامج مكتوبة بتطبيق الـ*MATLAB* R12 [48]. وطبق البرنامج على حاسبة نوع (PIII 833*MHZ*). واخيراً، فأن الفصل الخامس يتحدث عن الاستنتاجات والأعمال المستقبلية.

٢-١ المقدمـة

أنظمة التشفير بكل أنواعها التقليدية والحديثة تعتمد في بنائها على أفكار رياضياتية تعتبر البنية الأساسية لهذه الأنظمة، يعرض هذا الفصل موجزاً لهذه الأفكار والمفاهيم والمبرهنات التي ستكون بفرعين الأول يستعرض معلومات عامة موزعة بين الجبر والهندسة الاسقاطية ونظرية الأعداد بالاضافة الى مدخل بسيط للحسابات الكمية أما الفرع الثاني فسوف يتعرض الى كل ما يخص المنحنيات الاهليلجية (*Elliptic Curves*) ويمكن الاحتياج إليه في هذا البحث.

٢-٢ مفاهيم رياضياتية أساسية

٢-٢-١ مفاهيم جبرية أساسية

يشمل هذا البند بعض التعاريف ومصطلحات ومبرهنات جبرية قد تكون مطلوبة لتساعدنا في إعطاء بناء رياضياتي مقبول لأنظمة تشفير المنحنيات الاهليلجية (*Elliptic Curve Cryptosystems*) واستخداماتها.

تعريف (٢-١) : الزمرة (*Group*) [13]

مجموعة ليست خالية G مع عملية ثنائية + تكون زمرة إذا حققت الشروط الآتية :-

١. العملية + تجميعية (*Associative*) :- أي لكل ثلاثة عناصر c,b,a تنتمي للمجموعة G يتحقق : $a + (b + c) = (a + b) + c$

٢. العنصر المحايد (*Identity*) :- أي يوجد عنصر e في المجموعة G بحيث انه لكل عنصر a في G يكون :- $e + a = a + e$
بشرط إن يكون e وحيداً.

٣. النظير (*Inverse*) :- لكل عنصر $a \varepsilon G$ يوجد عنصر وحيد $a^{-1} \varepsilon G$ بحيث أن :
$a + a^{-1} = a^{-1} + a = e$

فإذا تحققت هذه الشروط الثلاثة يقال أن (G,+) تكون زمرة (*Group*).

تعريف (٢-٢) : الزمرة الابدالية (الابيلية) (*Abelian Group*)

يقال للزمرة (G,+) زمرة ابيلية (ابدالية) إذا وفقط إذا كانت العملية + ابدالية [13].

يقال عن الزمرة (G,+) منتهية (*finite group*) إذ كانت G مجموعة منتهية. ويسمى العنصر a مولداً (*generator*) للزمرة G إذا أمكن التعبير عن جميع عناصر الزمرة G بدلالة a وتكتب $G = \langle a \rangle$ ويقال الزمرة متولدة بـ a ،عند وجود مثل هذا العنصر في زمرة فتسمى زمرة دوارة (*Cyclic group*) أي إن الزمرة الدوارة هي زمرة متولدة بعنصر واحد [15]. وتعتبر $(Z/nZ,+_n)$ زمرة دوارة لكل $n \geqslant 1$ كما إن 1 هو المولد لهذه الزمرة وكذلك $n - 1 = -1$.

تعريف (٢-٣) :

إذا كانت (G,+) زمرة وكان $S \subset G$ ، فان (S,+) تكون زمرة جزئية من G إذ كانت (S,+) زمرة.[13].

تعريف (٢-٤) : الزمرة المتولدة بعدد منته من العناصر (*finitely generated group*)

لتكن G زمرة وليكن $a_i \in G$ لكل $i \in I$ فان اصغر زمرة جزئية من G تحوي $\{a_i \mid i \in I\}$ وإذا كانت هذه الزمرة الجزئية هي G فان $\{a_i \mid i \in I\}$ تولد G فان G تكون متولدة بعدد منته من العناصر (*finitely generated*) [13].

أو بعبارة أخرى إن الزمرة المتولدة بعدد منته هي الزمرة التي تمتلك مجموعة منتهية من المولدات [42].

مبرهنة (٢-١) :- كل زمرة دوارة تكون ابدالية والعكس ليس صحيحاً [13].

مبرهنة (٢-٢) :- كل زمرة جزئية من زمرة دوارة (*cyclic group*) تكون دوارة [13].

تعريف (٢-٥) :

تعرف رتبة الزمرة (*group's order*) بأنها عدد عناصرها سواء كانت منتهية أو غير منتهية ويرمز لرتبة الزمرة بالرمز |G| [15].

تعريف (٢-٦) :

تعرف رتبة العنصر (*element's order*) بأنها اصغر عدد صحيح موجب n يحقق العلاقة $g^n = e$ حيث إن e هو المحايد وإذ لم يوجد مثل هذا العدد فيقال إن g ذا رتبة غير منتهية (*infinite order*) [15].

مبرهنة (٢-٣) :- إذا كانت (S,+) زمرة جزئية من (G,+) فان رتبة S تقسم رتبة G[13].

مبرهنة (٢-٤) :- في أي زمرة منتهية فأن رتبة أي عنصر تقسم رتبة الزمرة [13].

تعريف (٢-٧) :

الدالة (*Function*) من المجموعة A إلى المجموعة B هي قاعدة اقتران تربط كل عنصر $a \in A$ بعنصر واحد فقط $b \in B$. تسمى المجموعة A منطلق الدالة (*Domain function*) وتسمى B مستقر الدالة (*Codomain function*) وإذا كانت الدالة تنقل a إلى b فيسمى b صورة العنصر a بفعل الدالة [15] .

ويطلق على الدالة أحيانا اسم التطبيق (*Mapping*).

تعريف (٢-٨) :التشاكل (هوموموروفزم *Homomorphism*) [42]

إذا كانت كل من (G,+) و(H,*) زمرة فان الدالة f المعرفة من G إلى H تكون هوموموروفزم إذا حققت [42] :-

$$f(a + b) = f(a) * f(b) \quad ; \quad a,b \in G$$

وتسمى ايضا تشاكلاً زمرياً (*group Homomorphism*).

تعريف (٢-٩) : التماثل (الايزوموروفزم *Isomorphism*) [42]

إذا كانت f دالة معرفة من (G,+) إلى (S,*) فان f تسمى ايزوموروفزم إذا كانت f دالة شاملة (*anto*) ومتباينة (*one- to- one*) وتحقق تعريف التشاكل (*Homomorphism*). وعندئذ يقال أن الزمرة G تماثل الزمرة H ويرمز لذلك $G \cong H$.

وللتماثل الزمري (*Isomorphism group*) خواص كثيرة مهمة منها :-

مبرهنة (٢-٥) :- إذا كانت f دالة تماثل (*Isomorphism*) من G إلى H فإن [42] :-

١. G وH تمتلكان العدد نفسه من العناصر أي أن $|G| = |H|$.
٢. إذا كانت G زمرة ابدالية فان H تكون زمرة ابدالية.
٣. إذا كانت G زمرة دوارة (*Cyclic*) فان H تكون زمرة دوارة.

٤. إذا كانت G تمتلك زمرة جزئية (*Subgroup*) ذات رتبة n فان H تمتلك زمرة جزئية ذات رتبة n أيضا.
٥. إذا كان g عنصراً ذا رتبة n في الزمرة G فان H يجب أن تحوي عنصرا ذا رتبة n وهذا العنصر هو f(g).
٦. إذا كان كل عنصر في G هو نظير نفسه فان كل عنصر في H هو نظير نفسه .
٧. إذا كان كل عنصر في G ذا رتبة منتهية فان كل عنصر في H يكون ذا رتبة منتهية.

مبرهنة (٢-٦) :- التماثل هو علاقة تكافؤ (*equivalence relation*).

مبرهنة (٢-٧) :- إذ كان p عدد أولى و G زمرة ذات رتبة p فان $G \cong Z \setminus pZ$ [42].

ومن مبرهنة (٢-٧) يمكن القول بوجود تشاكل بين أي زمرتين تمتلكان العدد نفسه من العناصر.

تعريف (٢-١٠) :

التشاكل الذاتي (*Automorphism*) هو تماثل (*Isomorphism*) من الزمرة إلى نفسها.[42]

تعريف (٢-١١) :

نموذج جبري (F,+, .) حيث أن F مجموعة مغلقة مع العمليتين الثنائيتين +,. و(F,+) تكون زمرة ابدالية في حين (F\{0},.) تكون زمرة أيضا بالإضافة إلى تحقيق قانون التوزيع أي أن $a.(b+c) = a.b + a.c \quad ; a, b, c \in F$

فان F تسمى حقلاً (*Field*).[13]

ويمكن أن يعبر عن تعريف الحقل بالقول أن الحلقة (*Ring*) F تكون حقلاً إذا كان لكل عنصر غير صفري في F يوجد نظير ضربي (أي نظير بالنسبة للعملية الثانية).[13]

تعريف (٢-١٢) : مميز الحقل (*Characteristic of field*)

مميز الحقل هو اصغر عدد صحيح n يحقق العلاقة $n*1= 0$ حيث أن 1 هو المحايد الضربي و 0 هو المحايد الجمعي، أما إذا لم يكن مثل هذا العدد n موجوداً فيقال أن الحقل ذا مميز يساوي صفراً (وأحيانا يطلق عليه ذي مميز ما لانهاية ∞).ويرمز لمميز الحقل بالرمز (*Char.F*).[42]

مبرهنة (٢-٨) :- [42]

إذا كان $(F,+,.)$ حقلا فانه يحقق الخواص الآتية :-

١. تقاطع كل الحقول الجزئية من F تكون حقلا يدعى حقلاً أولياً من F (*Prime field of F*).
٢. مميز الحقل (*Char.F*) أما ان يكون عدداً أولياً او صفراً.
٣. إذا كان مميز الحقل عدد أولي p فانه لكل $a,b \in F$ يتحقق $(a+b)^p = a^p + b^p$.
٤. إذا كان F حقلا وكان $a,b \in F$ و $a \neq 0$ فان المعادلة $ax + b = 0$ تمتلك حلا وحيدا في F.
٥. إذا كان n عدد غير أولي فان Z/nZ لاتكون حقلا لان $Z-\{0\}$ لاتحقق شرط الانغلاق مع عملية الضرب.

تعريف (٢-١٣) : توسيع الحقل (*Extension Field*) [13]

إذا كان كل من F,E حقلاً فيقال E هو توسيع للحقل F إذا كان E يحوي حقلاً جزئياً (*Subfield*) يكون متماثلاً (*Isomorphism*) مع الحقل F.

وغالباً ما يكون F هو نفسه حقل جزئي من E فمثلاً يكون حقل الأعداد الحقيقية هو توسيع لحقل الأعداد النسبية و حقل الأعداد المركبة هو توسيع لكل من الأعداد الحقيقية والأعداد النسبية وكذلك فان كل حقل هو توسيع للحقل نفسه.

إذا كان E هو توسيع للحقل F فالعنصر $a \in E$ يقال له عنصر جبري على الحقل F (Algebraic element over F) إذا كان a هو حلاً لمتعددة حدود في F.

فمثلا $\sqrt{2}$ عنصر جبري في حقل الأعداد النسبية ذلك لانه حل لمتعددة الحدود $x^2 - 2 = 0$ في حين لا تعتبر كل من e,δ,π عناصر جبرية في Q [13] ،كما يسمى الحقل E بأنه توسيع جبري للحقل F (*Algebraic extension*) إذا كان كل عناصر E هي عناصر جبرية على F وبذلك يمكن القول بان حقل الأعداد المركبة هو توسيع جبري للأعداد النسبية.

ويقال عن الحقل F انه مغلق جبرياً (*Algebraically closed field*) إذ كانت كل متعددة حدود $P(x)$ في F تمتلك حلاً في الحقل نفسه. ومن ذلك فإن الأعداد المركبة هي حقل مغلق جبريا بينما لاتكون الأعداد الحقيقية أو الأعداد النسبية كذلك. ويكون E انغلاقاً جبرياً (*Algebraic closure*) للحقل F ويرمز له $\overline{F}$ عندما يكون E حقل مغلق جبرياً وتوسيعاً

للحقل F في الوقت نفسه. [13] والانغلاق الجبري لحقل الأعداد النسبية هو حقل جزئي من الأعداد المركبة يعرف باسم حقل الأعداد الجبرية (*field of algebraic numbers*) [42].

تعريف (٢-١٤) : حقل كالوا (*Galois Field*) [15]

التوسيع الجبري$f(x)/ [x]Z/pZ$ للحقل المنتهي Z/pZ حيث p عدد أولي و$f(x)$ متعددة حدود في Z/pZ من الدرجة n غير قابلة للتحليل (*irreducible*) يسمى حقل كالوا ويرمز له بالرمز $GF(P^n)$.

ولحقل كالوا أهمية كبيرة في الكثير من التطبيقات الرياضياتية [13] .

كما وتوجد عدة خواص أخرى للحقول (Fields) نوضح بعضا منها بالمبرهنة الآتية :-

مبرهنة (٢-٩) :- [13]

١. لكل عدد أولي p و n عدد صحيح موجب يوجد بالضبط حقل واحد يمتلك P^n من العناصر هو $GF(P^n)$.
٢. كل حقل ذي مميز صفر (Char.=0) يكون متماثلاً (*Isomorphic*) مع أحد الحقول الموسعة لحقل الأعداد النسبية ويكون حقل الأعداد النسبية حقل أولي (*prime field*) فيه.
٣. كل حقل ذو مميز عدد أولي (Char.=p) يكون متماثل (*Isomorphic*) مع حقل يكون توسيع للحقل (Z /pZ) ويحوي (Z /pZ) كحقل أولي فيه.
٤. $GF(P^n)=(Z/pZ[x]/f(x) =\{C_{n-1}\alpha^{n-1} +... + C_1\alpha + C_o|C_i \in Z /pZ ;I\}$.
٥. حقل كالوا $GF(P^n)$ هو حقل لـ P^n من جذور المعادلة $\left(x^{p^n} - x\right)$ والتي هي متعددة حدود في Z/pZ[x].
٦. إذا كان F حقلاً منتهياً فان :-
   - F يمتلك p^n من العناصر حيث أن p عدد أولي و n عدد صحيح موجب.
   - F ذو مميز عدد أولي.
   - F هو توسيع للحقل Z/pZ.
٧. إذا كان F حقلاً ذا رتبة p^n فان كل حقل جزئي F برتبة p^k يجب أن يتحقق k|n لجميع قيم k الممكنة.
٨. الزمرة الضربية (*Multiplicative group*) للعناصر الغير صفرية في الحقل المنتهي تكون زمرة دوارة.

٩. إذا كان F حقلا يحوي m من العناصر فان الرتبة الضربية لكل عنصر غير صفري في F تكون أحد قواسم (m-1).

١٠. إذا كان F حقلا يحوي m من العناصر وكان d يقسم (m-1) فانF يحوي عنصرا من الرتبة d.

٢-٢-٢ مفاهيم هندسية أساسية

يعد فهم بعض المفاهيم والخواص الهندسية خطوة تمهيدية مهمة لدراسة خواص المنحنيات الاهليلجية في نظرية الأعداد (*Number Theory*) [46] ويحوي هذا البند بعض المفاهيم البسيطة المرتبطة بمعنى الإحداثيات التآلفية والاسقاطية وكيفية تمثيل النقاط والمستقيمات بهذه الإحداثيات وطريقة التعامل معها.

تعريف (٢-١٥) :

المستوى الاسقاطي (*Projective plane*) على الحقل k هو مجموعة صفوف التكافؤ للمركبات $(X_o,X_1,X_2,...,X_n)$ والتي لاتكون جميعها أصفاراً ويقال عن اثنين من هذه الصفوف بأنهما متكافئان إذا وفقط إذا أمكن الحصول على أحدهما بعد ضرب الآخر بثابت [38] .

ولا يحتاج موضوع المنحنيات الاهليلجية إلى فضاءات ذات أبعاد كبيرة [38]، وحيث أن نقاط المستوى الاسقاطي تمثل بمستقيمات والمستقيمات بمستويات فان كل نقطة في الفضاء الاقليدي تمثل بثلاثي من الأعداد الحقيقية (X,Y,Z) حيث أن X,Y,Z تمثل أبعاد النقطة عن المستويات الثلاثة المتعامدة (التي تقابل الإحداثيات X,Y,Z على الترتيب).

ومن مفهوم التكافؤ تمثل الثلاثيات الآتية النقطة نفسها :-

$$(X,Y,Z),(2X,2Y,2Z),.....(\lambda X, \lambda Y, \lambda Z) \quad ; \quad \lambda \in I$$

والمستوى التآلفي ناتج من مستوي إسقاطي بعد حذف مستقيم منه وهذا معناه حذف نقطة واحدة من كل مستقيم لذلك تمثل النقطة في المستوى التآلفي بزوج مرتب من الأعداد على شرط أن لا يكون الإحداثي الثالث صفراً حتى نحصل على:-

$$(X,Y,Z) \rightarrow (\frac{X}{Z},\frac{Y}{Z},1)$$

كذلك فانه في المستوى التآلفي لاناخذ النقاط بالشكل (X,Y,0) ونستبعد المستقيم Z= 0 أي (0,0,1) ولذلك فان أي نقطة تمثل بزوج مرتب نقصد بها نقطة في المستوى التآلفي [١] .

كذلك يمكن تحويل أي نقطة من المستوى التآلفي إلى الاسقاطي حيث يكون :-

$(x,y)\in k^2 \rightarrow (X,Y,1)\in P^2(k^2)$

حيث أن P^2 هو المستوى الاسقاطي.[١]

تعريف (٢-١٦) :

يسمى المنحنى C منحنى أملس (*Smooth Curve*) إذا كان C لا يقطع نفسه [46].

٢-٢-٣ مفاهيم أساسية في نظرية الأعداد

تعتبر نظرية الأعداد (*Number Theory*) من أهم واقدم فروع الرياضيات المعروفة اليوم، وهي لا تستمد أهميتها هذه من قدمها فحسب بل أن هذه الأهمية أخذت تزداد وتكبر بزيادة تقدم علم الحاسبات [20]. وتعد نظرية الأعداد العمود الفقري والأساس الذي يقوم عليه علم التشفير لذلك سوف نذكر بعض التعاريف والمبرهنات التي تخص ذلك ومفاهيم أخرى تخص المنحنيات الاهليلجية واستعراض ذلك بشكل مختصر.

مبرهنة (٢-١٠) :- خوارزمية القسمة (*Division Algorithm*) [8] .

إذا كان a عدداً صحيحاً وكان b عدداً صحيحاً موجباً، فانه يوجد عددان صحيحان r,q بحيث أن :-

$a=q*b + r \; ; \quad 0 \leqslant r \leqslant b$

العدد q يدعى القاسم و r يسمى الباقي من قسمة a على b.

وتعتبر خوارزمية القسمة هي المبرهنة الأساسية في الحساب المعياري (*Modular arithmetic*) [8].

تعريف (٢-١٧) : الحساب المعياري (*Modular Arithmetic*) [8]

إذا كان كل من a,n عددا صحيحا فان a (mod n) هو الباقي المحسوب بعد قسمة a على n باستخدام خوارزمية القسمة ويحقق

$0 \leqslant a \pmod n < n$

تعريف (٢-١٨) :

ليكن n عدد صحيحاً موجباً فيقال للعددين الصحيحين a,b بأنهما متطابقان للمعيار n (قياس n) (*Congruence Modulo n*) إذا كان كلاهما يمتلك الباقي نفسه عند قسمته على n وبالعكس، وبعبارةٍ أخرى :-

$$a \pmod n \equiv b \pmod n \leftrightarrow a \equiv b \pmod n$$

وبالاعتماد على التعريف أعلاه توجد عدة خواص للحساب المعياري تتعلق بعمليات الجمع والطرح والضرب وعملية الرفع إلى أس معين يمكن مراجعتها في [42,8,4].

مبرهنة (٢-١١) [8] :- إذا كان $c*a \equiv c*b$ فان $a \equiv b \pmod{n/d}$ حيث أن $d=\gcd(c,n)$ (gcd تعني القاسم المشترك الأعظم).

ومن المبرهنة (٢-١١) نلاحظ أن قانون الحذف يتحقق في الضرب المعياري (الضرب قياس n) إذا كان d=1. وهذا يقودنا لمناقشة عملية القسمة في الحساب المعياري.حيث نلاحظ أن القسمة في هذا الحساب قد تكون ممكنة في بعض الأحيان ولكنها ليست كذلك في أحيان أخرى فإذا كان المعيار n عددا أوليا تكون ممكنة والعدد $a/b \pmod n$ معرف دائما أما إذا كان n عدداً قابلاً للتحليل فان العدد $a/b \pmod n$ ربما يكون غير معرف أو ليس وحيدا، وما يجب ملاحظته هو أن $a/b \pmod n = a^* (1/b) \pmod n$ وهذا يعني أن عملية القسمة ممكنة إذا وفقط إذا كان $1/b \pmod n$ معرفا.[55]

مبرهنة (٢-١٢) :- ليكن $n > 0, a, m \in Z$ فانه يوجد عدد صحيح c بحيث يحقق $a*c \equiv 1 \pmod n$ إذا وفقط إذا كان $\gcd(a,n) = 1$ ويكون c وحيدا. ويسمى c النظير الضربي للعدد a ضمن المعيار n.

وتكسب عملية أيجاد النظير الضربي (المعكوس) لعدد صحيح ضمن معيار معين أهمية كبيرة في التشفير وتوجد عدة طرائق لحسابه حيث أن أيجاد المعكوس هو عبارة عن حل المعادلة $a*x \equiv 1 \pmod n$ ونذكر منها:-

١- طريقة توظيف مبرهنة فيرما (*Fermat*) وفيها يشترط أن يكون المعيار عدداً أولياً [27].

٢- طريقة تستخدم فيها الخوارزمية الاقليدية.

٣- طريقة استخدام مبرهنة الفضلة الصينية (*Chinese Remainder Theorem*)وهي طريقة عامة لإيجاد حلول المعادلات.[55] وتستخدم مبرهنة الفضلة الصينية مع الأعداد الكبيرة جدا

عن طريق تجزئة هذه الأعداد إلى عدة مركبات واختيار المعيار عدد كبير m وتمثيله كحاصل ضرب لمجموعة أعداد أولية [4].

مبرهنة (٢-١٣) :- مبرهنة الفضلة الصينية (*Chinese Remainder Theorem*) لتكن $m_1, m_2, \ldots, m_r$ أعداداً صحيحة موجبة بحيث أن $\gcd(m_i, m_j) = 1$ لكل $i \neq j$ فان نظام المتطابقات $x \equiv b_1 \pmod{m_1}, x \equiv b_2 \pmod{m_2}, \ldots, x \equiv b_r \pmod{m_r}$ يمتلك حلا وحيدا للمعيار $(m_1.m_2 \ldots .m_r)$.[55].

تعريف (٢-١٩) :

ليكن p عدداً أولياً فردياً و $\gcd(a,p) = 1$ فإذا كانت المتطابقة $x^2 = a \pmod{p}$ تمتلك حلا فان a تسمى باقي تربيعي (*quadratic residue*) للمعيار p ويرمز له (q.r) وبخلاف ذلك فان a يسمى باقي غير تربيعي (*quadratic non residue*) للمعيار p ويرمز له (q.n.r).[8]

مبرهنة (٢-١٤) :- ليكن p عدداً أولياً فردياً وليكن $\gcd(a,p)=1$ فان a هو باقي تربيعي للمعيار p إذا وفقط إذا كان :- $a^{(p-1)/2} \equiv 1 \pmod{p}$

ويطلق على المبرهنة (٢-١٤) قيد اويلر (*Eulers Criterion*) [7].

تعريف (٢-٢٠) : رمز ليجندر (*The Legendre Symbol*) [7]

ليكن p عدداً أولياً و n عدداً صحيحاً ، يعرف $\left(\frac{n}{p}\right)$ رمز ليجندر بأنه 0 إذا كان p يقسم n و1+ إذا كان n باقي تربيعي للمعيار p و1- إذا كان n باقي غير تربيعي.

مبرهنة (٢-١٥) :- إذا كان p عدد أولي اكبر من 2 وكان $\gcd(p,a) = 1$ فان المتطابقة $x^2 \equiv a \pmod{p}$ تمتلك بالضبط حلّين للمعيار p^n إذا كان a باقياً تربيعياً للمعيار p ولا تمتلك حلاً إذا كان a باقياً غير تربيعي [8].

ومن المبرهنة (٢-١٥) يمكن القول بان العدد a يكون باقياً تربيعياً في الحقل F_p^n إذا كان باقياً تربيعياً في الحقل F_p.

مبرهنة (٢-١٦) :- إذا كان p >2 عدداً أولياً ،فيوجد بالضبط $\left(\frac{p-1}{2}\right)$ من البواقي التربيعية غير الصفرية للمعيار p .[26].

مبرهنة (٢-١٧) :- خواص البواقي التربيعية [26]

١. $(\frac{a^2}{p}) = +1$ أي أن كل عدد مربع هو باقي تربيعي.

٢. حاصل الضرب:- باقي تربيعي × باقي تربيعي = باقي تربيعي.

باقي غير تربيعي × باقي غير تربيعي = باقي غير تربيعي.

باقي غير تربيعي × باقي غير تربيعي = باقي تربيعي.

مبرهنة (٢-١٨) :- [26]

١. إذا كان $p \equiv 1 (\mod 4)$ فان $\left(\frac{p}{q}\right) = \left(\frac{p-q}{p}\right)$ أي إذ كان a باقي تربيعي (q.r) فان a هو باقي تربيعي (q.r) أيضا. -

٢. إذا كان $p \equiv -1 \pmod 4$ فان $\left(\frac{p}{q}\right) = -\left(\frac{p-q}{p}\right)$ أي إذ كان a باقي تربيعي (q.r) فان a- هو باقي غير تربيعي (q.n.r) والعكس بالعكس.

٣. إذ كان كل من q , p عدداً أولياً فان :-

- $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ إذا كان $p \equiv 1 (\mod 4)$ أو $q \equiv 1 (\mod 4)$.
- $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ إذا كان $p \equiv q \equiv 3 \pmod 4$.

وتوجد بعض البواقي التربيعية لاعداد معينة محسوبة بصورة عامة نذكر منها:[26]

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & if\ p \equiv 1 (\mod 4) \\ -1 & if\ p \equiv -1 (\mod 4) \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & if\ p \equiv \mp 1 (\mod 8) \\ -1 & if\ p \equiv \mp 1 (\mod 8) \end{cases}$$

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & if\ p \equiv \mp 1 (\mod 12) \\ -1 & if\ P \equiv \mp 5 (\mod 12) \end{cases}$$

ويمكن الاستمرار لإيجاد أعداد أخرى ولكن سوف يتطلب الأمر تعقيدا اكبر وحسابات اكثر.

مبرهنة (٢-١٩) :- إذ كان كل من p ,1+2p أعداداً أوليةً فان العدد الصحيح $2^{*}{}^{(p-}(-1)^{1)/2}$ يكون جذراً ابتدائياً (*primitive root*) للحقل F_{2p+1}.[8]

مبرهنة (٢-٢٠) :- البواقي التربيعية لعدد فردي أولي p تكون مطابقة للقوى الزوجية للجذر الابتدائي r للمعيار p، والبواقي غير التربيعية تكون مطابقة للقوى الفردية للجذر الابتدائي r .[8]

مثـــــال (٢-١) :-

ليكن p=13 ,2 جذراً ابتدائياً في الحقل F_{13} فان البواقي التربيعية تكون 1,10,9,12,3,4 والتي تطابق على الترتيب $2^{12},2^{10},2^{8},2^{6},2^{4},2^{2}$. بينما تكون البواقي غير التربيعية 7,5,11,6,8,2 والتي تطابق $2^{11},2^{9},2^{7},2^{5},2^{3},2^{1}$

مبرهنة (٢-٢١) :- [26]

١- العدد الكلي للأعداد الصحيحة a بحيث أن a و a+1 يكون كلاهما باقياً تربيعياً للمعيار p هو:- $\frac{1}{4}(p-4-(\frac{-1}{p}))$

٢- العدد الكلي للأعداد الصحيحة a بحيث أن كل من a+1,a يكون كلاهما باقياً غير تربيعياً للمعيار p هو:- $\frac{1}{4}(p-2+(\frac{-1}{p}))$

بحيث إذا كان $p \geqslant 5$ يجب أن يكون هناك على الأقل زوج من الأعداد المتتالية كلاهما باقياً غير تربيعياً.

٣- يوجد (p-1) ½ من الأعداد الصحيحة المتتالية بحيث يكون أحدهما باقي تربيعي والآخر باقي غير تربيعي أو بالعكس.

ولإيجاد الجذور التربيعية للعدد a للمعيار p يجب أولا حل المعادلة $y^2 \equiv a \pmod p$ حيث أن هذه المتطابقة تمتلك [$\frac{a}{p}$ +1] من الجذور وهذا يعني إنها تمتلك جذرين إذا كان a باقي تربيعي ولا تمتلك جذورا إذا كان a باقي غير تربيعي، فإذا كان x هو أحد الجذور فان p - x هو الجذر الآخر، أما إذا كان $a \equiv 0 \pmod p$ فان هناك جذر واحد فقط للمعادلة وهو $x \equiv 0 \pmod p$ والخوارزمية الآتية تبين كيفية إيجاد جذور العدد a ضمن المعيار p،[21].

ليكن p عدداً أولياً فردياً وليكن g عدداً صحيحاً يحقق $0 < g < p$ ، إذا كان :-

$g^{(p-1)/2} \equiv -1$ فان g يمتلك جذرا في الحقل F_p بعبارة أخرى يوجد عدد صحيح g يحقق $y^2 \equiv g \pmod p$ أما إذا كان $g^{(p-1)/2} \equiv 1$ فان g لا تمتلك جذرا .

فإذا كان g يمتلك جذرا في الحقل F_p فيمكن إيجاده من خلال أحد الحالات الآتية :-

١- إذا كان $p \equiv 3 \pmod 4$ فهذا يعني أن $p=4*k + 3$ حيث k عدد صحيح فيتم حساب جذر g بالعلاقة:- $y = g^{k+1} \pmod p$

٢- أما إذا كان $p \equiv 5 \pmod 8$ فهذا معناه $p=8*k + 5$ حيث أن k عدد صحيح ، فالجذر التربيعي للعدد g يتم حسابه بالخطوات الآتية :-

$r = (2g)^k \pmod p$
$i = 2*g*v \pmod p$
$y = g*v\ (i-1) \pmod p$

٣- طريقة عامة تتضمن إيجاد ρ بحيث ($\rho^2 - 4g$) لاتمتلك جذرا تربيعيا للمعيار p، (وسيكون هذا متحقق لنصف القيم الممكنة للعدد تقريبا) ويمكن إيجاد جذر العدد g للمعيار ρ باستخدام متتابعة لوكاس *Lucas Sequence* :-

تعريف (٢-٢١) :

تعرف متتابعة لوكاس *Lucas Sequence* بأنها متتابعة من الأعداد ضمن العلاقة :- $L_n = L_{n-1} + L_{n-2}$,$n \geqslant 3$ ويمكن ان نعوض $L_1=1$ و $L_2 =2$ فتكون المتتابعة 1,3,4,7,11,18,29,... [8].

تعريف (٢-٢٢) :

تسمى عملية إيجاد العدد x في العلاقة $a^x = b$ بمسألة اللوغاريتم (*logarithm problem*) حيث أن كل من b,a معلوم، يسمى x الدليل (*Index*) للعدد b بالنسبة الى a. ويرمز لذلك بـ $x = \log_a b$ أو $x = ind_a(b)$ [8].

كما تسمى مسألة اللوغاريتم بدالة اللوغارتيم (*Logarithm mapping*) وعندما تعرف مسألة اللوغاريتم ضمن حقل منته أو زمرة منتهية فيطلق عليها عندئذ مسألة اللوغاريتم المنفصل (*Discrete logarithm problem*) [10] وهي من المسائل التي لم يتمكن أحد من حلها حتى

هذا الوقت باستثناء وجود بعض الخوارزميات المعقدة في حساباتها للتعامل مع بعض مسائل اللوغاريتم والتي تقسم إلى:- [55]

١- خوارزميات تعمل على مختلف أنواع الزمر وهذا يعني إنها لا تستغل أي من خواص الزمرة مثل خوارزمية شانك (*Shank*) والتي تعرف أيضاً بأسم طريقة الخطوة الصغرى-الخطوة العظمى (*baby- step giant- step method*) وطريقة بولارد-رو (*pollard* ρ *-method*) وكذلك طريقة (λ*-Method*) والمعروفة بطريقة الكنغر (*Kangaroo's method*).

٢- الطرائق التي تعمل جيدا في الزمر المنتهية (*finite group*) التي تكون رتبتها لا تمتلك عوامل أولية كبيرة أي مع الزمر التي لا تتحقق خاصية النعومة (*smoothness*) لرتبتها ومثال هذه الطرائق خوارزمية (*Silver- pohling- Hellman*) التي تعتمد على مبرهنة الفضلة الصينية.

٣- الخوارزميات التي تستغل تمثيل عناصر الزمرة كحاصل ضرب أعداد أولية صغيرة نسبيا وهي أيضا تستخدم مبرهنة الفضلة الصينية ومن أمثلتها طرائق تحليل الدليل (*Index Calculus Methods*).

تعريف (٢-٢٣) :

يقال للعدد بأنه أملس (*Smooth*) إذا لم يمتلك عوامل أولية كبيرة ويدعى ذا نعومة y (y-*smooth*) إذ كانت عوامله الأولية اقل من y.

٢-٢-٤ الحساب الكمي (*Quantum Computing*)

الحساب الكمي هو الحساب المعتمد بشكل أساس على متغيرات مأخوذة من نظرية الكم الفيزيائية، وجد ليواكب تطور مواضيع الفيزياء ويلبي متطلبات هذا التطور[٢].

تعريف (٢-١٩) : البت الكمي (*Quantum bit*)

البت الكمي (*Quantum bit*) ويرمز له اختصارا (*qubit*) عبارة عن نظام كمي من مستويين.وبسبب عدم وجود خوف من حدوث تداخل او تشوش فان فضاء هلبرت الثنائي H_2 (*two dimension Hilbert space*) يمكن أن يطلق عليه بت كمي. حيث ان H_2 ذو اساس

ثابت $B=\{|0\rangle , |1\rangle\}$ والذي يسمى الاساس الحسابي (*Computational basis*) والحالات $|0\rangle, |1\rangle$ يطلق عليها اساس الحالة (*basis state*).[19]

والحالة العامة لمتغير مكون من بت كمي واحد تكون:-

$$C_o|0\rangle + C_1|1\rangle \; ; \qquad |C_o|^2 + |C_1|^2 = 1$$

حيث ان $|0\rangle,|1\rangle$ هي الحالة الكمية لكل من 1,0 على الترتيب او الحالة المكممة كما يطلق عليها في الفيزياء[٢].

تعريف (٢-٢٥) :

العملية الحسابية في البت الكمي (*Qubit*) والتي تدعى (*Unary quantum gate*) عبارة عن تطبيق ذاتي :- [19]

$$V : H_2 \rightarrow H_2$$

أو بعبارة أخرى فان البوابات الكمية (*Unary quantum gate*) تعرف العملية الخطية الآتية :-

$$|0\rangle \rightarrow a|0\rangle + b|1\rangle$$
$$|1\rangle \rightarrow c|0\rangle + d|1\rangle$$

بحيث تكون $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ مصفوفة وحدة.

وبهذا الترتيب يمكن تعريف بوابات كمية (*quantum gate*) مشابهة للبوابات المنطقية الاعتيادية [19].

تعريف (٢-٢٥) :

المسجل الكمي (*quantum register*) أو اكثر عموما الكومبيوتر الكمي (*quantum computer*) هو مجموعة مرتبة من عدد منتهٍ من البتات الكمية (*qubit*)[55].

ويمكن التعبير عن نظام مكون من بتين كميين (*two qubits*) بفضاء هلبرت رباعي الأبعاد $H_4 = H_2 \otimes H_2$ ذي أساس متعامد (*orthonormal basis*)

$\{|00\rangle , |01\rangle , |10\rangle , |11\rangle\}$ والذي يحقق الحالة الآتية :-

$$C_o|00\rangle + C_1|01\rangle + C_2|10\rangle + C_3|11\rangle$$

بحيث أن $|C_o|^2 + |C_1|^2 + |C_2|^2 + |C_3|^2 = 1$.

ويمكن استخدام التعابير $|0\rangle|0\rangle = |00\rangle$ و $|0\rangle |1\rangle = |10\rangle$ و... [19].

وباستخدام التعريف (٢-٢٤) يمكن تصميم بوابات كمية كدالة من H_4 إلى H_4.

تعريف (٢-٢٧) :

تحويل فورير الكمي (*Quantum Fourier transformation*) ويرمز له اختصارا (*QFT*) هو العملية :-

$$\sum_{i=1}^{n} f(g_i)|g_i\rangle \rightarrow \sum_{i=1}^{n} \hat{f}(g_i)|g_i\rangle$$

أو بعبارة أخرى QFT هو الحالة العامة لتحويل فورير (*Fourier transformation*) للدالة f المعرفة من الزمرة G حيث أن $G = \{g_1, g_2, \ldots, g_n\}$ إلى حقل الأعداد المركبة تكون بالحالة :-

$C_1 |g_1\rangle + C_2 |g_2\rangle + \ldots + C_n |g_n\rangle$.

والتي نحصل منها على $f(g_i) = C_i$ بحيث ان $||f|| = 1$ [19].

مبرهنـــة (٢-٢٢) :- تركيـب تحويـل فـورير (*Fourier transformation decomposition*)

لتكن $G = U \otimes V$ هي الضرب الديكارتي للزمر الجزئية U, V ولتكن المجموعة $\{|u\rangle, |v\rangle | u \in U, v \in V\}$ هي التمثيل الكمي لعناصر G فان:

$$|u_i\rangle|v_i\rangle \rightarrow \left(\frac{1}{\sqrt{r}}\sum_{k=1}^{r}(\chi_i^u(u_k))^*|u_k\rangle\right)\left(\frac{1}{\sqrt{s}}\sum_{l=1}^{s}(\chi_i^v(v_k))^*|v_k\rangle\right)$$

$$= \frac{1}{\sqrt{rs}}\sum_{k=1}^{r}\sum_{l=1}^{s}\chi_{ij}^*(u_i + v_l)|u_k\rangle|v_l\rangle$$

هو تحويل فورير في الزمرة G. حيث أن المجموعة $\{\chi_i, i = 1,2,\ldots,n\}$ هي المميز للزمرة G[19]. χ_k^* ويمثل المرافق (*Conjugate*) للعدد χ_k [39].

كما يمكن التعبير عن تحويل فورير في مجموعة الأعداد الصحيحة أو الزمر الجزيئة منها [19]. وشأنه شأن الحسابات الاعتيادية وبالاعتماد على حالات تعقيد الحساب الكمي (*quantum Complexity classes*) يمكن توزيع المسائل في هذا النوع من الحساب إلى :-

١-(QP) وهي مجموعة المسائل التي يمكن أن تحل في (*Polynomial Time*) في الحسابات الكمية.

٢-(BQP) وتمثل مجموعة المسائل التي يمكن حلها في (*Polynomial Time*) في الحساب الكمي ولكن باحتمالية فشل مقدارها $\varepsilon < 1/3$.

٣-(ZQP) يمثل مجموعة المسائل المتوقع حلها بـ (*Polynomial Time*) بنسبة فشل تساوي صفراً (*Zero- error probability*).

وهذه المستويات الثلاثة مناظرة لمستويات أخرى موجودة في الحسابات الاعتيادية [55] وتعد مسألة تجزئة العدد إلى حاصل ضرب عددين أولين (*Integer Factorization*) ومسألة اللوغاريتم المنفصل (*Discrete Logarithm*) من أهم المسائل التي تم إيجاد خوارزميات كمية لحلها [بند ٢ -٥-١].

٢-٢-٤-١ خوارزمية حل اللوغاريتم المنفصل

يمكن استخدام خوارزمية تجزئة العدد إلى عوامله الأولية مع بعض الإضافات لحساب اللوغاريتم المنفصل وفيما يأتي سنبين خوارزمية شور (*Shor's Algorithm*) حيث إذا كان g و p عدداً أولياً ولغرض إيجاد عدد صحيح r بحيث أن $g^r \equiv x \pmod p$, $x \in N$. ان وجد مثل هذا العدد الصحيح r فيجب استخدام ثلاث مسجلات كمية لحسابه وكالاتي :

١. إيجاد عدد q يكون قوى صحيحة للـ 2. بحيث يكون $p < q < 2p$.

٢. نعوض في أول مسجلين من الكومبيوتر الكمي الحالات المتطابقة بانتظام لكل $|a\rangle$, $|b\rangle$ للمعيار (p-1) ونحسب $g^a x^{-b} \pmod p$ في المسجل الثالث مما يجعل الكومبيوتر الكمي في الحالة $|\Psi_1\rangle$:-

$$\Psi_1 = \frac{1}{p-1} \sum_{a=0}^{p-2} \sum_{b=0}^{p-2} |a, b, g^a x^{-b} (\mathrm{mod}\, p)\rangle$$

٣. باستخدام تحويل فورير A_q للتطبيق $|a\rangle \rightarrow c$, $|b\rangle \rightarrow d$ والمبرهنة (٢-٢٢) تكون :-

$$\frac{1}{q} e^{(\frac{2\pi i}{4}(ac+bd))}$$

فان الحالة $|a,b\rangle$ سوف تتحول إلى الحالة :-

$$\frac{1}{q} \sum_{c=0}^{q-1} \sum_{d=0}^{q-1} e^{(\frac{2\pi i}{4}(ac+bd))} . |c, d\rangle$$

وهذا يجعل النظام في الحالة $|\Psi_2\rangle$:-

$$|\psi_2\rangle = \frac{1}{(p-1)q} \sum_{c=0}^{q-1} \sum_{d=0}^{q-1} e^{(\frac{2\pi i}{4}(ac+bd))} . |c, d, g^a x^{-b} (\mathrm{mod}\, p)\rangle$$

٤-بتعويض حالة الكومبيوتر واستخراج المعلومات المطلوبة فان احتمالية تعويض الحالة $|c,d,g^a x^{-p} \pmod p\rangle$ تكون:-

$$|\frac{1}{(p-1)q}\sum e^{(\frac{2\pi i}{4}(ac+bd))}|^2$$

حيث أن المجموع يؤخذ على (a,b) ويحقق :- $a - r\,b \equiv k \pmod{p-1}$

وهذا هو افضل ناتج يمكن الحصول عليه [55].

ويوجد العديد من المفاهيم والمبرهنات الرياضياتية في الجبر والهندسة والتحليل تم تكميمها وحسب الحالات التي يتطلبها المجال [39].

٢-٣ المنحنيات الاهليلجية (*Elliptic Curves*)

المنحنيات الاهليلجية (*Elliptic Curves*) هي واحدة من روائع الرياضيات في القرن التاسع عشر ولفت انتباه الكثيرين أمثال ابيل (*Abel*) وكاوس (*Gauss*) وجاكوبي (*Jacobi*) وليجندر (*Leqendre*) ووابرسترس (*Wieirstrass*) والعديد غيرهم وقد لاحظ الكثير من الباحثين آنذاك بان هذه المنحنيات ليست قطوع ناقصة (*Ellipses*) ولكنها فقط تعبير لطول قوس القطع الناقص عن طريق تكامل الجذور التربيعية لمتعددة حدود تربيعية. وكلمة اهليلج (*Elliptic*) مأخوذة من نظرية تكامل الاهليلج (*Elliptic Integral*) الذي يكون بالصيغة :-

$$\int R(x,y)dx$$

حيث أن R(x,y) هي دالة نسبية بـ x,y وتكون y^2 متعددة حدود بمتغير x من الدرجة الثالثة أو الرابعة والتي لا تمتلك جذورا مكررة وتكامل الاهليلج كان دافعا مهما لدراسة دوال الاهليلج (*Elliptic Functions*) [55]. والتي تعرف بأنها دوال دورية بمتغيرات معقدة [9]. ولمعلومات اكثر يمكن مراجعة [46,28,41,9].

ومن الجدير بالذكر أن مصطلح الاهليلج أحيانا يطلق على المنحنيات ذوات مؤشر 1 (*genus*1) والمعرفة على حقول غير حقل الأعداد المركبة C ولكن هذا يجب أن لايدل ضمنا على أن هذه المنحنيات تمتلك متغيرات وخواص الدوال الاهليلجية (*Elliptic Functions*) التي هي دوال مركبة بمتغيرات مركبة وليس لها معنى في أي حقل آخر [9].

أو بعبارة أخرى منحنى اهليلج (*Elliptic Curve*) أو منحنى ابيلي (*Abelian Curve*) نعني بـه منحنـى كـاملاً غيـر مفرد (*Complete non-singular curve*) ذا مؤشـر (*genus*) يسـاوي١ ، بالإضـافة إلـى نقطـة خاصـة، وفـي عـام ١٩٣٢ ظهـر توجـه جديـد لدراسـة الخـواص الحسابية للمنحنيات الاهليلجية وخواص نقاط تلك المنحنيات [8 2].

تعريف (٢-٢٨) :

ليكن E منحنٍ و P = (x,y) نقطة فيه فان P تكون نقطة مفردة (*Singular Point*) في E إذا كانت المشتقتان $\frac{\partial E}{\partial x}, \frac{\partial E}{\partial y}$ تساويا صفرا في P ،أي منحنى يمتلك على الأقل نقطة مفردة واحدة يسمى منحنى مفرداً (*Singular Curve*) وعكس ذلك يسمى المنحنى ليس مفرداً (*non-singular curve*) [46].

تعريف (٢-٢٩) :

يمكن تمثيل المنحنيات الاهليلجية بمعادلة عامة ذات إحداثيات غير متجانسة تعطى بصيغة وايرسترس العامة (*Weierstrass Equation*) بشرط أن لا تمثل هذه المعادلة منحنيات مفردة(*singular curves*) :-

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad .....(1)$$

بالإضافة إلى نقطة خاصة تسمى النقطة في المالانهاية (*Point at infinity*) التي يرمز لها O_E وجميع الحدود a_i تقع ضمن الحقل المعرف عليه ذلك المنحنى [46] ، وإذا كان مميز الحقل لا يساوي 2 (char.(F) ≠ 2) فانه يمكن الحصول على صيغة مبسطة لمعادلة وايرسترس بطريقة إكمال المربع واستخدام التحويل ($y \rightarrow \frac{1}{2}(y-a_1x-a_3)$) فنحصل على :-

$$E: y^2 = 4x^3 + b_2x^3 + 2b_4x + b_6$$

حيث ان :

$$b_2 = a_1^2 + 4a_2$$
$$b_4 = 2a_4 + a_1a_2$$
$$b_6 = a_3^2 + 4a_6$$

وكذلك يكون :-

$$b_8 = a_1^3 a_6 + 4a_2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$
$$C_4 = b_2^2 - 24b_4$$

$C_6 = b_2^3 + 36b_2b_4 + 216b_6$
$\Delta = -b^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$
$j = C_4^3/\Delta$
$w = dx / (2y + a_1x + a_3) = dy / (3x^3 + 2a_2x + a_4 - a_1y)$

حيث يسمى Δ المميز (*discriminate*) و j ثابت المنحنى الاهليلجي E (j-*invariant*) أما w فهو ثابت اشتقاق المنحنى (*invariant deferential*) المقترن بصيغة وايرسترس. وبالاعتماد على Δ يمكن معرفة أن المنحنى ليس مفرداً (*non singular*)، وبمعرفة j يمكن تحديد التماثلات (*Isomorphism*) ، أما ثابت اشتقاق المنحنى فيمثل المشتقات الجزئية. ولكون صيغة وايرسترس العامة مطولة واحيانا يصعب التعامل معها فقد تم اختزالها في بعض الحقول العددية إلى صيغ اكثر اختصارا ليسهل التعامل معها [46].

٢-٣-١ المنحنيات الاهليلجية في الحقول المنتهية

يمكن إيجاد صور مختلفة للمنحنيات الاهليلجية باستخدام تحويلات خطية بسيطة وذلك لتسهيل إجراء العمليات على نقاط هذه المنحنيات في بعض الحقول العددية ومن التعريف(٢-٢٨) فان المنحنى يكون معرفاً على الحقل F إذ كان a_i تنتمي له.

آ- المنحنيات المعرفة على الحقل ذو المميز 3

يمكن تمثيل المنحنيات الاهليلجية في هذا الحقل بإحدى المعادلتين :-

$$E: y^2 = x^3 + a_2x^3 + a_6 \quad \dots (2)$$

حيث ان $j = -a_2^3/a_6$ و $\Delta = -a_2^3a_6$ ، ويجب ان يكون $j \neq 0$.

أما إذا كان $j = 0$ فيعرف المنحنى بالمعادلة :-

$$E: y^2 = x^3 + a_4x + a_6 \quad \dots (3)$$

حيث ان $j = 0$ و $\Delta = -a_2^3$.

ويجب أن لا تكون المعادلتان (2) و(3) قابلة للتحليل (*reducible*) ،علما إن التعويض المستخدم للحصول عليهما هو

$x \to x$ & $y \to y - 1/2(a_1x + a_3)$

ثم :

$$x \to x + \frac{a'_4}{a'_2} \quad , \quad y \to y$$

حيث ان a'_2 و a'_4 هما الحدان الناتجان من التعويض الأول [46].

اذا كانت Q,P نقطتين في المنحنى E تُعرّف عملية الجمع $P \oplus Q$ كالآتي :-

$$(x_3,y_3) = P \oplus Q$$
$$x_3 = \lambda^3 - a_2 - x_1 - x_2$$
$$y_3 = \lambda\,(x_1 - x_3) - y_1$$

حيث إن:-

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & if\ p \neq Q \\ \dfrac{3x_1^2 + 2x_2 + a_4}{2y_1} & if\ \ p = Q \end{cases}$$

ب- المنحنيات الاهليلجية المعرفة على الحقول الثنائية

الحقول الثنائية (*Binary Fields*) او الحقول ذوات المميز 2 والتي يكون عدد عناصرها أحد القوى الصحيحة للعدد 2 ويعرف المنحنى الاهليلجي في مثل هذه الحقول العددية بالمعادلات الآتية:-

إذا كان ثابت المنحنى j (j-*invariant*) يساوي صفرا وباستخدام التحويل الخطي :-

$$(x,\ y) \to \left(a_1^2 x + \frac{a_1}{a_4},\quad a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3} \right)$$

على معادلة (1) نحصل على منحنيات مفردة مفرطة (*Supersingular*) او تسمى ايضا مفردة فائقة، والتي تعرّف بالمعادلة

$$E:\ y^2 + a_3 y = x^3 + a_4 x + a_6 \qquad \ldots.(4)$$
$$\Delta = a_6$$

اما اذا كان ثابت المنحنى j (j-*invariant*) لا يساوي صفرا وباستخدام التحويل الخطي :-

$$(x,y) \to (x + a_2, y)$$

نحصل على منحنيات ليست من النوع المفرد المفرط (*non-supersingular*) معرفة بالمعادلة :-

$$E:\ y^2 + xy = x^3 + a_2 x + a_6 \qquad \ldots.(5)$$

وفيها يكون

$$a_1 = 0\ ,\ \Delta = a_3^4$$

بالاضافة الى النقطة في المالانهاية O_E [46]، وفي المعادلتين (4) ، (5) قد تكون المعادلة التكعيبية قابلة للتحليل (*reducible*) [55].

وتعرف عملية جمع النقاط في المنحنيات الاهليلجية في هذه الحقول بالآتي :-

اذا كانت $P = (x_1 , y_1)$, $Q = (x_2 , y_2)$ نقطتين في منحنى اهليلجي معرف ضمن حقل ثنائي ، فيمكن تعريف مجموع $P \oplus Q = (x_3 , y_3)$ في المعادلة (4) من خلال :-

$$x_3 = \lambda^2 + x_1 + x_2$$
$$y_3 = \lambda (x_1 + x_3) + y_1 + a_3$$

حيث ان $\lambda = \frac{y_1 + y_2}{x_1 + x_2}$ عندما $P \neq Q$

وعندما $P = Q$ فان $\lambda = \frac{x_1^2 + a_4}{a_3}$ و

$$x_3 = \frac{x_1^4 + a_4^2}{a_3^2}$$
$$y_3 = \lambda (x_1 + x_3) + y_1 + a_3$$

ويكون $P \oplus Q = O_E$ اذا وفقط اذا كان $(x_1 = x_2 \text{ and } y_1 = y_1 + x_1)$ [46].

وتعرف عملية جمع النقاط $P \oplus Q = (x_3,y_3)$ ، حيث ان $P=(x_1,y_1)$, $Q=(x_2,y_2)$ في المنحنيات المعطاة بالمعادلة (5) كما يأتي :-

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a_2$$
$$y_3 = \lambda (x_1 + x_3) + y_1$$

حيث ان $\lambda = \frac{y_1 + y_2}{x_1 + x_2}$ اذ كانت $P \neq Q$.أما إذا كانت $P = Q$ فان $\lambda = x_1 + \frac{y_1}{x_1}$و

$$x_3 = \lambda^2 + \lambda + a$$
$$y_3 = x_1^2 + (\lambda + 1) x_3$$

ويكون $P \oplus Q = O_E$ ، إذا وفقط إذا كان $(x_1 = x_2 \text{ and } y_1 = x_1 + y_1)$ [46].

جـ- المنحنيات المعرفة على الحقل الأولي

يمكن الحصول على صيغة مبسطة للمعادلة (1) لتعريف المنحنيات الاهليلجية على الحقول الأولية (*prime fields*) أي الحقول التي يكون مميزها عدداً أولياً حسب تعريف (٢-٢٩)، وباستخدام التحويلين :-

$$y \to y - \frac{1}{2}(a_1 x + a_3)$$
$$x \to x - \frac{1}{3} a_2$$

على الترتيب لنحصل على الصيغة :-

$$E: y^2 = x^3 + a_4 x + a_6 \quad \ldots.(6)$$

والمميز (Discriminant) لهذه الصيغة هو $\Delta = 4a_4^3 + 27a_6^2$ [46].

وتشير بعض المصادر إلى انه (-16Δ) وأخرى (16Δ) [9,28,41,55,...] ، فإذا كانت $P = (x_1, y_1)$ و $Q = (x_2, y_2)$ نقاط في منحنى اهليلج فان عملية الجمع $P \oplus Q = (x_3,y_3)$ تكون :-

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda (x_1 - x_3) - y_1$$

حيث أن:-

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & if\ p \neq Q \\ \dfrac{3x_1^2 + a_4}{2y_1} & if\ p = Q \end{cases}$$

ويكون $P \oplus Q = O_E$ إذا وفقط إذا كان ($x_1 = x_2$ and $y_1 = -y_2$) [46].

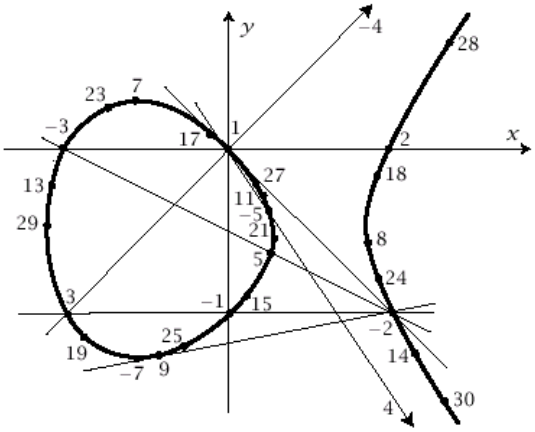
وبذلك فان كل نقطة تحقق أي واحدة من المعادلات (2) أو(3) أو(4) أو(5) أو(6) فإنها تعتبر نقطة في ذلك المنحنى بشرط إن تكون إحداثيات تلك النقطة تقع ضمن الحقل المعرف عليه المنحنى والنقطة في المالانهاية O_E تحقق جميع المعادلات أعلاه وتعتبر العنصر المحايد لعملية جمع النقاط في المنحنيات الاهليلجية . [34]

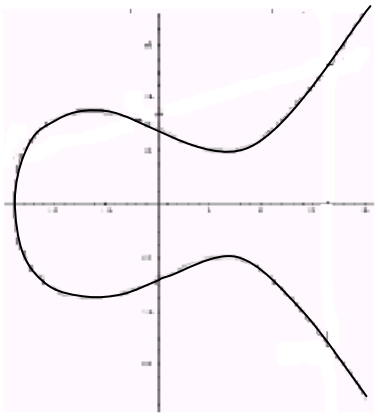
كمـــا يعـــرف المنحنـــى الاهليلجـــي علـــى الحقـــل ذي مميـــز عـــدد غيـــر أولـــي (*Composite Field*) بالمعادلة (6) نفسها بشرط أن يحقق المميز :-

$$\gcd(\Delta,6) = 1 \quad ; \quad \Delta = 4a_4^3 + 27a_6^2$$

٢-٣-٢ التمثيل الهندسي للمنحنيات الاهليلجية

كل منحنى اهليلج هو عبارة عن منحنى جبري أملس (*smooth*) أي لا يقطع نفسه، يعبر عنه بمعادلة وايرسترس (*Weierstrass*) غير المفردة (*non singular*) [46]. ويوجد شكلان واسعا الانتشار للمنحنيات الاهليلجية ، يوضحها الشكل (٢-١).





شكل (٢-١) : أشكال المنحنيات الاهليلجية.

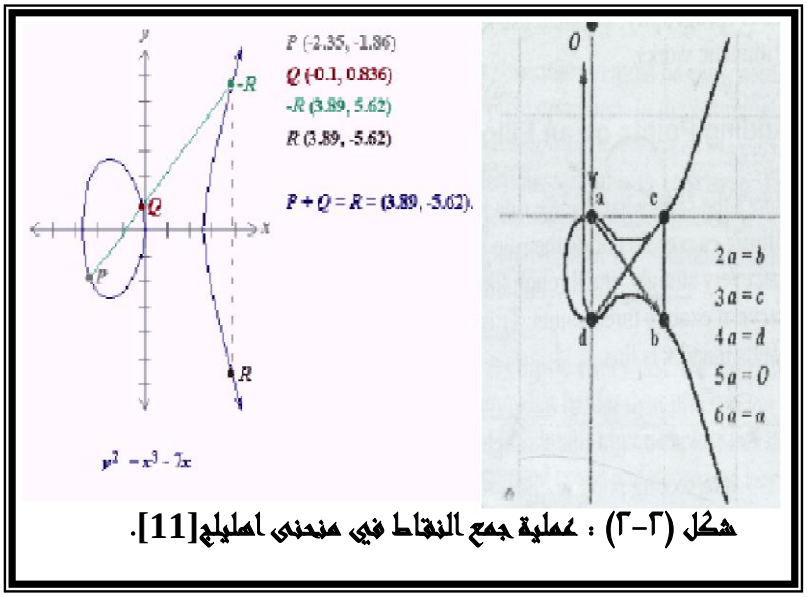
وبالعكس فان معادلة أي منحنى غير أحادى بصيغة وايرسترس تكون منحنى اهليلج حتى وان لم نستطيع تمثيل تلك المعادلة في المستوى [46]، أما المنحنى الذي يمتلك نقطة مفردة واحدة على الأقل فهو منحنى مفرد (*Singular Curve*) سواء كانت هذه النقطة عقدة (*node*) أو نتوء (*cusp*).

ومن البند (٢-١-٢) يمكن القول بان النقطة في المالانهاية O_E تمثل مستقيماً تم رفعه من المستوى الاسقاطي.

وتمتلك المنحنيات الاهليلجية خاصية مهمة جدا وهي أن الخط المار من نقطتين في المنحنى فانه يمر بنقطة ثالثة فيه [55,46,41,28] ولذلك يمكن تمثيل عملية الجمع هندسياً في المستوى الإحداثي بآلاتي :-

إذا كانت P, Q نقطتين في المنحنى E فان الخط الذي يصل بينهما سوف يمر بنقطة ثالثة في المنحنى ولتكن R- فان R، التي تمثل انعكاس R- حول محور التناظر الأفقي (والذي يكون المحور السيني في اغلب الاحيان) هي حاصل جمع $P \oplus Q$ ، أما إذا كان الخط مماساً للمنحنى في نقطة واحدة فان حاصل الجمع $2P = P \oplus P$ أيضا انعكاس النقطة R- التي تقع على المنحنى. كذلك فان أي خط عمودي يقطع المنحنى في نقطة أو نقطتين، يمر بالنقطة في المالانهاية O_E [38]. ومن ذلك ندرك أن الخط الذي يمر من نقطة واحدة ، هو الخط الذي يمر من تلك النقطة مرتين، وهو ما يمثل عملية المضاعفة للنقطة [17].

وحسب [46] فان المفهوم الهندسي لعملية جمع النقاط والمضاعفة يكافئ القواعد التي ذكرت في (٢-٢-١).ويوضح الشكل (٢-٢) التفسير الهندسي لعملية جمع النقاط في المنحنى الاهليلجي.



شكل (٢-٣) : عملية جمع النقاط في منحنى اهليلج[11].

وهذا يوفر لنا فهما اعمق للمبرهنة الآتية :-

مبرهنـة (٢-٢٣) :- مجموع ثلاث نقاط مختلفة في منحنى اهليلج يمر بها خط مستقيم، يساوي العنصر المحايد (النقطة في المالانهاية) [41].

٢-٣-٣ زمرة نقاط المنحنى الاهليلجي (*Group Point of Elliptic Curve*)

في هذا البند سنركز على مجموعة نقاط المنحنى الاهليلجي المعرف على الحقول المنتهية والتي تعتبر جزءً من حقل الأعداد النسبية والتي هي :-

$$E(F) = \{(x,y): y^2 + a_1x_1 + a_3y = x^3 + a_2x^2 + a_4x + a_6 \,|a_i \in F;\ I = 1,\ldots 6\}$$

فان هذه المجموعة والنقطة في المالانهاية (*Point at Infinity*) تكون زمرة تسمى زمرة النقاط النسبية للمنحنى E (*E-Rational Points*) وتسمى بالنسبية لكون عملية جمع النقاط في المنحنيات هي عبارة عن تطبيق نسبي [28].

آ- تحقيق شروط الزمرة

إذا كانت $P = (x_1, y_1)$ و $Q = (x_2, y_2)$ و $R = (x_3, y_3)$ ثلاث نقاط في المنحنى E.

١-عملية جمع النقاط في المنحنى تكون ثنائية أي تحقق شرطي الانغلاق (*Closed*) والتعريف الجيد (*Well-define*) أي إذا كان :-

$(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$

فإننا نستطيع أن نعبرعن y_3, x_3 بصيغ رياضياتية تعتمد على y_2, x_2, y_1, x_1 فقط.

وباستخدام حقيقة أن مجموع جذور متعددة حدود مساو لسالب معامل ثاني أعلى أس في المعادلة يكون قد تحقق الشرطان [27] والشيء ذاته يتحقق في حالة المضاعفة $P = P \oplus P$.

٢- تكون النقطة في المالانهاية هي العنصر الصفري (المحايد *Zero element*) لزمرة نقاط المنحنى الاهليلجي وبذلك فان لأي نقطة P في المنحنى :-

$P_1 \oplus O_E = O_E \oplus P_1 = P_1$

إما عملية المضاعفة فتكون :-

$2O_E = O_E \oplus O_E = O_E$

٣-النظير (*Inverse*) :- يعرف نظير النقطة P بأنه النقطة التي لها الإحداثي السيني نفسه، ونظير الإحداثي الصادي، وبعبارة أخرى [38].

$-(x, y) = (x, -y)$

ومتى ما كان (x,y) في المنحنى فان (x, −y) تقع في المنحنى أيضا [27]. ويمكن استنتاج ذلك مباشرة باستخدام التمثيل الهندسي.

٤-التجميع (*Associative*) :- لبرهان هذه الخاصية نحتاج إلى المبرهنة الآتية والتي سنأخذها بدون برهان :-

مبرهنة (٢-٢٤) :- ليكن L_3, L_2, L_1 ثلاث مستقيمات تقطع منحنى E في تسع نقاط هي $P_9,\ldots,P_3,P_2,P_1$ وليكن L'_3, L'_2, L'_1 ثلاث مستقيمات أخرى تقطع المنحنى في تسع نقاط $Q_9,\ldots,Q_3,Q_2,Q_1$ فإذا $P_i = Q_i$ لكل $i = 1,2,\ldots,8$ فان $P_9 = Q_9$ [38].

فإذا كانت R,Q,P ثلاث نقاط في المنحنى الاهليلجي E وكانت المستقيمات L_3, L_2, L_1 تمر من النقاط :-

$P, Q, -(P \oplus Q), O_E, R, -R, -P, -(Q \oplus R), P \oplus (Q \oplus R)$

والمستقيمات L'_3, L'_2, L'_1 تمر من النقاط :-

$P, Q, -(Q \oplus R), O_E, P, -P, -R, -(P \oplus Q), (P \oplus Q) \oplus R$

على الترتيب. وباستخدام المبرهنة أعلاه نحصل على [38].

$P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$

وبذلك تكون قد تحققت شروط الزمرة.

كذلك فان زمرة نقاط المنحنى الاهليلجي هي زمرة ابدالية (*Abelian Group*) [34] بالإضافة إلى إنها زمرة متولدة بعدد منته من النقاط (*Finitely Generated Group*) [46].

ب- زمرة الالتواء الجزئية (*Torsion Subgroup*)

إذا كانت P نقطة في منحنى اهليلج E فان عملية ضرب النقطة P بعدد صحيح k تعرف بأنها عملية جمع النقطة P مع نفسها k من المرات أي أن :-

$$k*P = \underbrace{P \oplus P \oplus P \oplus \ldots \oplus P}_{k - \text{من المرات}}$$

وتوجد كثير من الطرائق والتقنيات لحساب k *P والتي تسمى ضرب النقطة بثابت (*Scalar Multiplication*) وذلك لأهميتها في كافة تطبيقات المنحنيات الاهليلجية [30]. ومن اكثر هذه الطرائق شيوعا واستخداما طريقة مشابهة لخوارزمية الأس السريعة (*Fast Expnential*).

تعريف (٢-٣٠) :

يقال للنقطة P إنها ذات رتبة m إذا وفقط إذا كان m اصغر عدد صحيح يحقق $m*P = O_E$ وان لم يكن مثل هذا العدد الصحيح موجوداً فيقال أن النقطة P ذات رتبة غير منتهية (*Point of Infinite Order*) [49].

ورتبة النقطة في منحنى اهليلجي تحقق مبرهنة (٢-٤) أي أن رتبة كل نقطة تقسم رتبة الزمرة (*Group's Order*) (أي عدد نقاط المنحنى) وكل نقطة ذات رتبة m يقال إنها نقطة التواء من الرتبة m (m – *Torsion Point*) [34].

تعريف (٢-٣١) :

ليكن E منحنى اهليلج وليكن m عدداً صحيحاً لا يساوي صفرا فان زمرة الالتواء الجزئية للرتبة m والتي يرمز لها $E_{tors}[m]$ هي مجموعة نقاط المنحنى ذات الرتبة m. وبعبارة أخري فان زمرة الالتواء الجزئية (*Torsion Subgroup*) هي [34] :-

$E_{tors}[m] = \{P \in E \mid m*P = O_E \; ; \; O_E \; \textit{is point at infinity}\}$

وتلعب زمرة الالتواء الجزئية دوراً كبيراً جدا في إكمال المفهوم الرياضياتي للمنحنيات الاهليلجية وتطبيقاتها.

مبرهنة (٢-٢٥) :- (مبرهنة مورد يل *Mordell*) [34].

زمرة النقاط النسبية في المنحنى الاهليلجي E المعرف على الحقل F هي زمرة متولدة بعدد منته من النقاط (*Finitely Generated*) ويكون :-

$$E(F) \cong E(F)_{tors} \oplus Z^r$$

حيث أن $E(F)_{tors}$ هي زمرة الالتواء التي تحوي كل النقاط ذوات الرتبة المنتهية في E المعرف على الحقل F.

مبرهنـــة (٢-٢٦) :- تعرف زمرة الالتواء لمنحنى اهليلج في حقل الأعداد النسبية Q بالآتي [3] :-

$$E[F]_{tors} \cong \begin{cases} Z_m & \text{for } 1 \le m \le 12 \ ; \ m \neq 11 \\ Z_2 \otimes Z_n & \text{for } 1 < n < 4 \end{cases}$$

وتذكر بعض المصادر وجود فجوة كبيرة في حساب زمر الالتواء الجزئية في الحقول الأخرى غير حقل الأعداد النسبية [46,34,28].

مثـــال (٢-٢) :-

في المنحنى $E(F_{71})$ المعرف بالمعادلة :-

$$E(F_{71}) : y^2 = x^3 - x$$

وحيث أن $\#E = 72$ فتوجد بالضبط أربع نقاط بضمنها النقطة في المالانهاية ذات رتبة تساوي 2 وهي (0,0) و(1,0) و(70,0) وO_E وبذلك فان هذه النقاط الأربع هي الزمرة الجزئية ذات الالتواء 2 [34].

٢-٣-٤ المنحنيات الاهليلجية في الإحداثيات الاسقاطية

يتم تمثيل المنحنى الاهليلجي في المستوى الاسقاطي بتحويل معادلة وايرسترس (*Weierstrass Equation*) إلى معادلة متجانسة (*Homogenous*) بالمتغيرات X، Y، Z فتصبح :-

$$E(F): Y^2Z+a_1XYZ+a_3YZ^3=X^3+a_2X^2Z+ a_4XZ^2 + a_6Z^3 \quad \ldots.(7)$$

حيث أن a_i هي عناصر ضمن الحقل F [46].

كل نقطة في منحنى اهليلج يتم تمثيلها بثلاثي مرتب من الأعداد، والنقطة (X,Y,Z) في المستوى الاسقاطي تكافئ النقطة (X/Z, Y/Z) في المستوى التآلفي بشرط أن يكون $Z \neq 0$ وفي المنحنيات الاهليلجية فالنقطة الاسقاطية (أي النقطة بالتمثيل الاسقاطي) (X,Y,Z) تتحول إلى $(X/Z^2, Y/Z^3)$ حيث أن $Z \neq 0$ في المستوى التآلفي [18]. توجد صور أخري لهذه النقطة وحسب التحويل المستخدم [38,30,18] ، ففي الحقل الثنائي (*Binary Fields*) تتحول المعادلة إلى الصيغة :-

$$E(F_{2^m}): Y^2Z + XYZ = X^3 + aX^2Z + bZ^3 \quad \ldots.(8)$$

وتعرّف عملية جمع النقطتين بالاحداثيات الاسقاطية بالتعويضات الآتية :-

إذا كان $(X_3, Y_3, Z_3) = (X_1, Y_1, Z_1) \oplus (X_2, Y_2, Z_2)$ فان :-

$$Z_3 = \lambda_7 . Z_2$$
$$X_3 = aZ^2_3 + \lambda_6. \lambda_9 + \lambda^2_3$$
$$Y_3 = \lambda_9 X_3 + \lambda_8. \lambda^2_2$$

حيث أن :-

$$\lambda_1 = X_1Z^2_2$$
$$\lambda_2 = X_2Z^2_1$$
$$\lambda_3 = \lambda_1 + \lambda_2$$
$$\lambda_4 = Y_1Z^3_1$$
$$\lambda_5 = Y_2Z^2_3$$
$$\lambda_6 = \lambda_4 + \lambda_5$$
$$\lambda_7 = Z_1 \lambda_3$$
$$\lambda_8 = \lambda_6 X_2 + \lambda_7 Y_2$$
$$\lambda_9 = \lambda_6 + Z_3$$

أما عملية المضاعفة للنقطة $2(X_1, Y_1, Z_1) = (X_3, Y_3, Z_3)$

$Z_3 = X_1 Z^2_1$
$X_3 =(X_1 + bZ^2_1)^4$
$Y_3 = X^4_1 Z_3 + \lambda X_3$

حيث إن $\lambda = Z_3 + X_1^2 + Y_1 Z_1$

وفي الحقل الأولي (*Prime field*) فان عملية الجمع تتحقق بالآتي :-

$Z_3 = Z_1 Z_2 \lambda_3$
$X_3 = \lambda_6^2 - \lambda_7^2 \lambda_3^2$
$Y_3 = (\lambda_9 \lambda_6 - \lambda_8 \lambda_3^2) / 2$

حيث إن :-

$\lambda_1 = X_1 Z_2^2$
$\lambda_2 = X_2 Z_1^3$
$\lambda_3 = \lambda_1 - \lambda_2$
$\lambda_4 = Y_1 Z_2^3$
$\lambda_5 = Y_2 Z_2^3$
$\lambda_6 = \lambda_4 - \lambda_5$
$\lambda_7 = \lambda_1 + \lambda_2$
$\lambda_8 = \lambda_4 + \lambda_5$
$\lambda_9 = \lambda_7 \lambda_2^2 - 2X_3$

في كلا الحقلين الأولي والثنائي نلاحظ إن $P_1 = \pm P_2$ يكافئ $\lambda_3 = 0$ وإذا كان $\lambda_6 = 0$ فهذا يعني إننا سوف نستخدم المضاعفة أي أن $P_1 = P_2$ والتي تكون [38].

$Z_3 = 2Y_1 Z_1$
$X_3 = \lambda_1^2 - 2\lambda_2$
$\lambda_1 = 3X_1 + 9Z_1^4$
$\lambda_2 = 4X_1 Y_1^2$

اهم ما يميز عمليات جمع ومضاعفة النقاط في الإحداثيات الاسقاطية هو عدم وجود عمليات المعكوس (*Inverse*) لعناصر الحقل المعرف عليه المنحنى والتي تعتبر من اكثر العمليات الحسابية كلفة في الحقل لذلك، تكون الأكفأ في الحسابات برغم احتوائها على عمليات جمع وضرب اكثر مما هو موجود في الإحداثيات التآلفية [38].
ونلاحظ أن معادلة المنحنى الاهليلجي المعرف على الحقل الأولي بالصيغة الاسقاطية تكون:-

$E (F_p): Y^2Z = X^3 + aXZ^2 + bZ^3$

وعند تعويض Z = 0 نحصل على $X^3 = 0$ ومنه على X = 0 ولكن Z = 0 معناه نقطة في المالانهايـة، كـذلك فـان X=0,Z=0 يـوفر تكـافؤاً يمثـل تقـاطع المسـتوى X مـع المسـتقيم فـي المالانهاية (المستقيم المحذوف عند التحويل من المستوى الاسقاطي إلى المستوى التآلفي)وبذلك فـان النقطـة فـي المالانهايـة تكـون إحـداثياتها (0,1,0) وهـي نقطـة مقبولـة رياضـياتياً، وكـذلك يظهر واضحا إنها العنصر المحايد لعملية الجمع والمضاعفة.[1]

٢-٣-٥ العمليات الحسابية والجبرية في زمرة النقاط

إذا كانت P نقطة في المنحنى E المعرف على حقل منته، فلإيجاد النقطة m*P بحيث m عدد صحيح هناك عدة طرائق نذكر منها :-

آ- العمليت باستخدام متعددات حدود القسمة

ليكن E منحنٍ اهليلجي معرف على حقل أولي بالمعادلة :-

$E(F_p): y^2 = x^3 + ax + b$

فتعرف متعددات حدود القسمة ψ_m في الحلقة Z[a,b,x,y] بالتتابع كالآتي:-

$\psi_1 = 1 \quad , \psi_2 = 2y$

$\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$

$\psi_4 = 4y\,(x^6 + 5ax^4 + 20bx^2 - 5ax^2 - 4abx - 8b^2 - a^3)$

.

.

.

$\psi_{2m+1} = \psi_{m+2}\,\psi_m^{\,3} - \psi_{m-1}\,\psi_{m+1}^{\,3} \quad ; m \geq 2$

$2y\,\psi_{2m} = \psi_m\,(\psi_{m+2}\,\psi_{m-1}^{\,3} - \psi_{m-2}\,\psi_{m+1}^{\,2}) \quad ; m \geq 2$

وبالاعتماد على قيم ψ_m تحسب كل من Φ_m وω_m حيث :-

$\Phi m = x\psi_m^{\,2} - \psi_{m+1}\,\psi_{m-1}$

$4ywm = \psi_{m+2}\,\psi_{m-1}^{\,2} - \psi_{m-2}\,\psi_{m+1}^{\,2}$

وباستخدام هذه العلاقات مجتمعة نحصل على :-

$$(x_m, y_m) = \left(\frac{\phi_m(p)}{(\psi_m(p))^2}, \frac{\omega_m(p)}{(\psi_m(p))^3}\right)$$

حيث $m*P = (x_m, y_m)$.[46]

---

[1] النقطة في المستوى الإسقاطي تكتب بين أقواس كبيرة [ ] ولكن للظروف الطباعية، ولأننا نكتب المصادر بين أقواس كبيرة لذا تم تمثيل النقاط داخل أقواس صغيرة.

وقد ظهرت هذه الطريقة في عدد من المصادر مع بعض الاختلافات، شمل بعضها $\psi_o=0$ أو $\psi_{-1} = -1$ أو غير ذلك من الاختلافات [46,34,28,22,16].

ب- عملية حساب الإحداثي السيني

تعتمد هذه الطريقة على حساب الإحداثي السيني فقط ، فبالامكان حساب إحداثيات النقطة (2r+1)*P وذلك بحساب r*P أولاً ومن ثم حساب (2r+1)*p باستخدام القضيتين الاتيتين :-

قضية (٢-١) :- ليكن E منحنى اهليلج ولتكن $(x_2,y_2) =2(x_1,y_1)$ وبشرط أن يكون $y\neq0$ فان :-

$$x_2 = \frac{(x_1^2 - a)^2 - 8bx_1}{4(x_1^3 + ax + b)}$$

ومن السهل جدا تحقيق واثبات هذه القضية وذلك عن طريق التعويض المباشر.

قضية (٢-٢) :- ليكن E منحنٍ اهليلجي، ولتكن (x_r,y_r) = r.P و (r+1)P = (x_{r+1},y_{r+1}) نقاط في المنحنى بشرط أن يكون $x_r \neq x_{r+1}$ و $x \neq 0$ بحيث أن P = (x,y) فان :-

$$x_{2r+1} = \frac{(a - x_r x_{r+1})^2 - 4b(x_r + x_{r+1})}{x(x_r - x_{r+1})^2}$$

عندما (x_{2r+1},y_{2r+1}) = (2r+1)P .

ومن الجدير بالذكر أن هذه الطريقة ذكرت في المصدر [6] فقط من المصادر التي اطلعنا عليها.

جـ- عمليات الجمع والمضاعفة

تعد عملية ضرب النقطة بعدد صحيح في المنحنيات الاهليلجية من أهم العمليات الحسابية واكثرها استخداما، لذلك ظهرت العديد من التقنيات والبحوث في هذا الجانب واكثر هذه التقنيات انتشارا هي عملية الجمع والمضاعفة (*Addition and doubling*) وهي طريقة مشابهة إلى حد ما خوارزمية الأس السريعة (*Fast exponential algorithm*) ويمكن أيجاز هذه الطريقة بالآتي :-

ليكن E منحنٍ اهليلجي ولتكن P نقطة فيه فلايجاد النقطة Q = k*P حيث k عدد صحيح يتم اولا تحويل k إلى النظام الثنائي (binary Form) وليكن $k = e_o\ e_1\ e_2 \dots e_r$ ثم نأخذ البتات من e_1 إلى e_r فإذا كان $e_i = 1$ فأننا نضاعف النقطة ونجمعها مع P أما إذا كان $e_i = 0$ فأننا نضاعفها فقط وهكذا مع جميع البتات [52].

مثـــال (٢-٢) :-

لحساب 37 نحسب:-

37 = 1 0 0 1 0 1

37P = 2 (2 (2 (2 (2P)))) + 2(2P) + P

وبذلك نحصل على 37P عن طريق 7 عمليات مضاعفة للنقطة P وثلاث عمليات جمع وبالتأكيد هي اقل بكثير من عملية جمع النقطة P مع نفسها 37 مرة.

مثـــال (٢-٣) [55] :-

لحساب 105P يكون :-

105 = 1 1 0 1 0 1

105 = 2 (2 (2 (2 (2 (2P + P)) + P))) + P

وهذه العملية تتطلب 6 عمليات مضاعفة و3 عمليات جمع، وهي اقل بكثير من عملية جمع النقطة 105 مرة مع نفسها [55].

د-العمليات باستخدام دالة الاتزان

تعتمد هذه الطريقة على فكرة عملية الجمع والمضاعفة بعد إجراء بعض العمليات على بتات التمثيل الثنائي (*binary string*) للعدد الصحيح k ، وذلك للتوصل إلى صورة لهذا التمثيل يكون فيها عدد البتات المساوية للواحد $e_i = 1$ اقل ما يمكن ليتم اختزال عدد العمليات لاقل عدد وتوصف طريقة الاتزان (*blanced method*) بالاتي :-

عند تحويل العدد إلى النظام الثنائي (binary system) وبوجود عدد من البتات المتتالية المساوية للـ 1 فيتم تحويل البت الذي يسبق هذه المتتابعة من البتات، من 0 إلى 1 وتُحوّل البتات البقية إلى اصفار عدا البت الأخير في المتتابعة، الذي يتحول إلى 1- وبالمحصلة يكون الناتج مساويا للعدد الأصلي من حيث القيمة ، يتم بعدها تطبيق طريقة

الجمع والمضاعفة وكما تم وصفها في الفقرة (جـ) من البند (٢-٣-٥) . فقط عندما يكون $e_i = -1$ فأننا نضاعف ونطرح P (أي نضيف P –) [43].

وبذلك سوف يتم اختزال كثير من العمليات الحسابية ومما يزيد من فاعلية هذه الطريقة هو أن عملية حساب نظير النقطة في المنحنى الاهليلجي هي عملية سهلة جداً.

مثـــــال (٢-٤) [43] :-

لحساب النقطة 10045*P علينا اجراء الحسابات الآتية :-

10045 = 1 0 0 1 1 1 0 0 1 1 1 1 0 1

وبعد التحويل يكون :-

10045 = 1 0 1 0 0 –1 0 1 0 0 0 –1 0 1

حيث نلاحظ انه في التمثيل الاعتيادي يكون e_5, e_4, e_3, e_2 هي متتابعة من الواحدات وكذلك يكون كل من e_{10}, e_9, e_8 فان دالة الاتزان تكون بتعويض $e_6 = 1$ و $e_2 = -1$ وكذلك نعوض $e_{11} = 1$ و $e_8 = -1$. وبذلك نلاحظ اننا نحتاج 13 عملية مضاعفة و 5 عمليات جمع بدلاً من 13 عملية مضاعفة و8 عمليات جمع، باعتبار أن عملية الطرح مكافئة لعملية الجمع.

هـ-عملية الضرب بعدد صحيح باستخدام تشاكلات ذاتية كفوءة :-

تمتلك المنحنيات الاهليلجية خصائص اضافية مهمة وكثيرة ولم يكن من المبالغة ان توصف بانها من جواهر رياضيات القرن التاسع عشر [55]. واحدى هذه الخصائص هي التشاكل الذاتي (*Endomorphism*) حيث توجد ضمن الزمرة الواحدة عدة تشاكلات، منها عملية الضرب بعدد صحيح ودالة فروبينيس (*Frobinous map*) وغيرها الكثير وقد استغلت بعض منها وفق ضوابط معينة في تطوير خوارزميات سريعة لحساب حاصل ضرب النقطة بعدد صحيح وكانت هذه الخوارزميات كفوءة جدا من ناحية الوقت اللازم لتنفيذها[14]. ويوضح المثال الاتي فكرة واحدة منها.

مثـــال (٢-٥) [٤٧] :-

ليكن E منحنٍ اهليجي معرف على الحقل الاولي F_{23} ولتكن P نقطة في المنحنى E المعرف على الحقل (F_{23}^n) فاذا اردنا حساب m*P و $m = 10^6$ يكون :-

$$m*p = 2^6 (P \oplus 2^3 (P \oplus 2^5 (P \oplus 2^2 (P \oplus 2 (P \oplus 2 (P \oplus 2P))))))$$

وفي هذه الحالة نحتاج الى 6 عمليات جمع و 19 عملية مضاعفة كذلك فان اسوأ حالة نعوضها لعدد مكون من 6 بتات (6-bit) سوف نحتاج فيها الى 19 عملية جمع و 19 عملية مضاعفة ،ولكن باستخدام توسيع فروبينيس (Frobinous Expahtion) نحصل على :-

$$m*P = \phi(\phi(\phi(\phi(\phi(\phi(\phi(-\phi(P) \oplus 2P)) \oplus 7P) \Theta 3P) \Theta 9P) \Theta 5P) \Theta 4P) \Theta 8P) \oplus 6P$$

ونلاحظ ان عدد العمليات قد اصبح عبارة عن 9 عمليات جمع و 9 عمليات مضاعفة وتطبيق دالة فروبينيس 9 مرات. وفي اسوأ الحالات يمكن ان نحتاج الى 12 عملية جمع و 12 مرة لتطبيق دالة فروبينيس.ومما يجب ذكره ان هذه الطريقة لاتعتبر طريقة عامة يمكن ان تستخدم لكل المنحنيات ، وكذلك ليست كل التشاكلات كفوءة [14].

٢-٣-٦ طرائق حساب عدد نقاط المنحنى

المنحنيات الاهليلجية المعرفة على حقول منتهية (*finite fields*) تمتلك عدد منته من النقاط [34]، وبعبارة أخرى، مجموعة نقاط أي منحنى معرف على حقل منته تكون منتهية.

حساب عدد نقاط المنحنى أو رتبة المنحنى (*order of curve*) تكسب اهمية كبيرة في حقل التشفير حيث أن عدد نقاط المنحنى يؤثر في الكثير من الخواص الحسابية للمنحنيات وبالتالي يؤثر حتى على أنظمة التشفير المعتمدة عليها. وسنرمز لعدد نقاط المنحنى E بالرمز # E .

مبرهنة (٢-٢٧) :-

ليكن E منحنٍ اهليلجي معرف على الحقل F_q الذي يحوي q من العناصر فيكون [46] :-

$$| \# E (F_q) - q - 1 | \leq 2 \sqrt{q} \qquad ....(10)$$

وهذه المبرهنة يطلق عليها مبرهنة هاس (*Hasse*) نسبة إلى واضعها عام 1933 والمعادلة (10) تسمى معادلة قيود هاس. ويمكن أن تمتلك المعادلة 10 صيغة ابسط هي :-

$$\# E (F_q) = q - t + 1 \quad ; |t| < 2 \sqrt{q}$$

حيث ان t هي دالة الأثر للمنحنى (*trace of curve*).

مبرهنة (٢-٢٨) :-

ليكن N عدد طبيعي و $t = N - q - 1$ حيث أن $q = p^r$ و p عدد أولي و r عدد طبيعي فالزمرة G من الرتبة N يمكن أن تكون متماثلة مع زمرة نقاط منحنى اهليلجي معرف على الحقل F_q إذا وفقط إذا تحقق أحد هذه الشروط :-

$$1-\gcd(q,t)=1,|t|<2\sqrt{q},then,G=Z/lZ\times Z/mZ;where,m|l,m|(t-2)$$

$$2-r\ is\ even,\ t=2\sqrt{q},then,G=(Z/lZ)2$$

$$3-r\ is\ odd,\ p\equiv 1(\mathrm{mod}\,3),|t|=\sqrt{pq}=p^{\frac{r+1}{2}},then,G=Z/NZ$$

$$4-\ r\ is\ odd,\ p=2 or p=3,t=\sqrt{pq}=p^{\frac{r+1}{2}},then,G=Z/NZ$$

$$5-\ r\ is\ odd,\ p\equiv 3(\mathrm{mod}\,4) or (r-even),\ p\equiv 1(\mathrm{mod}\,4),|t|=0,then,G=Z/NZ.$$

$$6-\ r\ is\ odd,\ p\equiv 3(\mathrm{mod}\,4),|t|=0,then,G=Z/NZ,or,G=Z/lZ\times Z/2Z$$

وتحسب هذه النظرية كل القيم الممكنة لعدد عناصر E(K) [20] .وتوجد عدة طرائق لحساب عدد نقاط المنحنيات الاهليلجية اهمها :-

آ- **طريقة حساب رمز ليجندر** ***(Legendre Symbol)***

إذ كان المنحنى E معرفاً بالمعادلة : -

$E(F_p) : y^2 = x^3 + a\,x + b$

على الحقل F_p حيث p عدد أولي ،لحساب عدد نقاط E يتم تعويض عناصر الحقل F_p في المعادلة التكعيبية (الطرف الايمن)، فان كان الناتج باقياً تربيعياً فهذا يعني وجود نقطتين، أما إذا كان الناتج باقياً غير تربيعي لاتوجد أي نقطة وعندما يكون الناتج صفرا فهذا يعني هذا وجود نقطة واحدة، بالاضافة إلى النقطة في المالانهاية O_E نرى أن :-

$$\#\,E(F_p)=1+\sum_{x=0}^{p-1}\left[1+\left(\frac{x^3+ax+b}{p}\right)\right]=p+1+\sum_{x=0}^{p-1}\left[\frac{x^3+ax+b}{p}\right]. \qquad ...(11)$$

مثـــال (٢-٦) [55] :-

ليكن E منحنٍ اهليلجي معرف على الحقل F_5 بالمعادلة :-

$E(F_5): y^2 = x^3 + 3x$

وبما أن البواقي التربيعية في F_5 هي 4,1 فقط وبتعويض قيم x نحصل على :- 1,1,1,1,0

وبذلك يكون حساب عدد نقاط المنحنى كالآتي :-

$\#E(F_5) = 5 + 1 + 4 = 10$

تطبق هذه الطريقة بصورة عامة على جميع المنحنيات [17] ولكن لسوء الحظ فان هذه الطريقة لاتكون كفوءة مع المنحنيات المعرفة على حقول عددية كبيرة حتى باستخدام اسرع الحواسيب واكثرها تطوراً [5],[21],[45].

ب- طريقة استخدام خوارزمية شانك

احدى الطرائق التي تعمل بكفاءة عالية في الحقول العددية المتوسطة هي خوارزمية شانك (*Shank's Algorithm*) والتي تسمى ايضا خوارزمية الخطوة الصغرى – الخطوة العظمى (*Baby step – Giant step*) والتي يمكن وصفها كالأتي :-

لنفرض اننا اخترنا نقطة P في المنحنى E فإذا كان $\#E = x$ فان $x*P = O_E$ ولكن من المعادلة (10) نحصل على :-

$$q+1-2\sqrt{q} \le x \le q+1+2\sqrt{q}$$

فإذا وجدنا عدد y في الفترة $[q+1-2\sqrt{q} \quad q+1+2\sqrt{q}]$ ويحقق $y*P = O_E$ بحيث أن y يكون وحيدا فيجب أن يكون عندئذ $y = x$ أي عدد نقاط المنحنى. ولكن في اكثر الحالات سيكون هناك اكثر من y يحقق الخاصية $y*P = O_E$ ، وبحساب كل هذه القيم سوف تكون القيمة المطلوبة واحدة من بينها. ولاستخراجها نحسب النقاط $2s + 1$ لاي عدد صحيح s :-

$\{(x - s)P, (x-s+1)P, \ldots, (x-1)P, xP, (x+1)P, \ldots, (x+s)P\}$

والتي سوف تكون هي النقاط نفسه : -

$\{ -sP, -(s-1)P, \ldots, P, O_E, P, \ldots, (s-1)P, sP\}$

وبافتراض s عدد صغير نسبيا بحيث يكون عمليا في الحسابات وإذا وجدت أي من هذه النقاط بين نقاط $\{yP\}$ ضمن قيود مبرهنة هاس ، فيكون مساويا لـ x ولنفرض أن

$y*P = r*P$ و r تقع ضمن المجموعة $\{-s, \dots, 0, \dots, s\}$ فنجد أن $(y - r)P = O_E$

ومن ذلك نستنتج أن $x = y - r$.وعند ذلك نكون قد اكملنا الخطوة الصغرى لننتقل بعدها إلى الخطوة العظمى والتي يتم فيها البحث في الفترة $[q+1-2\sqrt{q} \quad q+1+2\sqrt{q}]$ عن النقاط في المجموعة $\{ tP \}$ بحيث أن $t - s \le s \le t$ – ونعوض :-

$$Q = (q + 1)P$$
$$R = (2s + 1)P$$
$$t = [2\sqrt{q}/ (2s + 1)]$$

وبذلك يكون من السهل ملاحظة احدى نقاط المجموعة $\{0, \pm P, \dots, \pm sP\}$ والتي ستظهر في المجموعة $\{Q, Q \pm R, \dots, Q \pm (-R)\}$ ولتقليل الحسابات يجب أن يكون s اصغرعدد ممكن.

ووجد أن افضل قيمة له هي $s \approx \sqrt[4]{q}$ ذلك لان كمية الحسابات اللازمة تكون مساوية لـ $s + 2t$ [17].

مثـــال (٢-٧) :-

حساب عدد نقاط المنحنى $E (F_p): y^2 = x^3 + 2x + 1$ حيث $p = 3023$.

الحل:-

لتكن $P = (1,2)$ فيكون :-

$$s \approx \sqrt[4]{3023} \approx 7$$

$$t = [2 \sqrt{3023}/ (2* 7 + 1)] = 7$$

$P = (1,2) , \pm 2P =(1700, \pm 1653) , \pm 3P = (1429, \pm 528),$
$\pm 4P = (806, \pm 1693), \pm 5P = (2879, \pm 772) , \pm 6P = (2274, \pm 1957) ,$
$\pm 7P = (1474, \pm 996).$

ثم نحسب كل من R,Q حيث أن :-

$Q = 3024 P = (520,2418)$
$R = 15 P = (1063,80)$

ونضع قائمة بالنقاط

$Q + 7R = (422,1880)$	$Q - 7R = (1486,1728)$
$Q + 6R = (2434,886)$	$Q - 6R = (1232,768)$
$Q + 5R = (1814,596)$	$Q - 5R = (1475,2339)$
$Q + 4R = (520,605)$	$Q - 4R = (1712,243)$
$Q + 3R = (1063,80)$	$Q - 3R = (422,1143)$
$Q + 2R = O_E$	$Q - 2R = (2434,2137)$
$Q + R = (1063,2943)$	$Q - R = (1814,2427)$
	$Q = (520,2418)$

نلاحظ أن O_E هي نفسها ظهرت بالقائمة الثانية وتحمل التسلسل Q + 2R وهذا يعني :-

$$Q + 2R = (3023 +1)P + (2*15)P$$

وبالنظر لعدم وجود تكرار لـ O_E لذا يكون عدد نقاط المنحنى هو [17] : -

$$3023 + 1 + 2 * 15 = 3054$$

جـ- طريقة استخدام خوارزمية سكوف

واحدة من أهم و أقوى الخوارزميات لحساب عدد النقاط في المنحنيات الاهليلجية هي خوارزمية سكوف (*Schoof's Algorithm*) التي تعد طريقة عامة تستخدم لكل المنحنيات المعرفة على الحقول المنتهية. وهناك العديد من المعالجات لمحاولة جعل هذه الخوارزمية اكثر كفاءة في حقول الأعداد الكبيرة جدا ومن هذه المعالجات التطوير الذي ادخله كل من اتكن (*Atkin*) واليكس (*Elikies*) والذي جعل الخوارزمية تعرف بخوارزمية سكوف- اليكس- اتكن (*Schoof-Elikies-Atkin*) ويرمز لها اختصارا (SEA) [22].

ويمكن صف عمل خوارزمية سكوف بإيجاد زمرة جزئية ذات التواء l في زمرة نقاط المنحنى E وعند تطبيق تشاكل فروبينيس الذاتي (*Frobenius Endomorphism*) :-

$$\Phi: (x,y) \rightarrow (x^p, y^p)$$

يعرف لنا مقياس تات (*Tate module*) الذي يرمز له T_e [E] ويحقق المعادلة :-

$$\Phi^2 - t\Phi + p = 0 \qquad \ldots.(11)$$

حيث تمثل t دالة الأثر (*trace map*) لتطبيق فروبينيس وبذلك يكون عدد نقاط المنحنى:-

$$\#E = p + 1 - t$$

فان وجد عدد صحيح t_l ($t \pmod l$) ويحقق :-

$$\Phi^2(P) + pP = t_l\Phi(p)$$

لكل نقطة في الزمرة الجزئية ذات التواء l (*l-toesion subgroup*) تكون بذلك حصلنا على t $\equiv t_l \pmod l$ وبالاستمرار في حساب ($t \pmod l$) لجميع قيم l والتي هي عبارة عن أعداد أولية صغيرة يتجاوز حاصل ضربها $4\sqrt{p}$ أي أن ($\prod_{i=1} l_i \geq 4\sqrt{p}$) وباستخدام مبرهنة الفضلة الصينية (*Chinese Remainder Theorm*) يتم حساب قيمة t النهائية [23].

ومن الجدير بالذكر أن جميع المعالجات على خوارزمية سكوف فقط تخص اختيار قيم الأعداد الأولية l_i أو أيجاد آلية تطبيق قوى اكبر من واحد لبعض قيم هذه الأعداد، وذلك للتقليل قدر الامكان من دوال متعددات حدود القسمة (*division polynomial*) التي نحتاجها [23].

مثـــال (٢-٨) [16] :-

إيجاد عدد نقاط المنحنى E المعرف على الحقل F_7 باستخدام خوارزمية سكوف حيث أن :-

$E(F_7): y^2 = x^3 + 3$

الحـــل :-

بما أن $3 * 5 \geq 4\sqrt{7}$ لذلك سيكون $l_1= 3$,$l_2 =5$ ولما كان $l_1=3$ فيجب أن نحسب متعددة الحدود الثالثة :-

$$\Psi_3 (x,y) =3x^4 + x \rightarrow f_3(x) = \Psi_3 (x,y) =3x^4 + x$$

كذلك نفرض أن P(x,y) ذات التواء يساوي 3 :-

$$\Phi^2(P) = (x^{q^2}, y^{q^2}) = (x^{49}, y^{49})$$

$$[q \bmod 3] (x,y) = [1 \pmod 3] (x,y) = (x,y)$$

وهذا يعني أن كل من $3x^4 + x$, $x^{49} - x$ تمتلك جذورا مشتركة كذلك أن النقاط ذات الالتواء 3 تمتلك خاصية $\Phi^2 (P) = \pm P$.

وكذلك فان $q \equiv 1 \pmod 3$ يعطينا $w = \pm 1$ هو جذر تربيعي ومنه يكون :-

$$(x^{49}, y^{49}) = \pm (x,y)$$

وبذلك فان $(x^7 - x)$ و $f_3(x)$ تمتلك جذورا مشتركة لذلك أما 1+ أو 1- يكون قيمة ذاتية (*eigen value*) للدالة Φ ، وبمقارنة الإحداثي الصادي نحصل على $y^7 = y$ وعند التعويض في معادلة المنحنى يكون :-

$$y(x^3 + 3)^3 = y$$

وبما أن y لايمكن أن يكون صفرا لذلك فان :-

$$(x^3 + 3)^3 - 1 = 0$$

حيث أن $\gcd(h_x(x),f_3(x)) =1$ ، ومنه فان 1 لايكون قيمة ذاتية وعليه فان :-

$$t = -2w \pmod 3 \equiv 1 \pmod 3$$

وعندما $l_2 = 5$ فان $P =(x,y)$ هي نقطة ذات التواء يساوي 5. ولكن $q \pmod 5 = 2 \pmod$ 5) لذلك نحتاج لحساب 2p. الإحداثي السيني يكون :-

$$\frac{(2x^4 - xy)^2}{y^2} = \frac{(x^4 - 3x)}{x^3 + 3}$$

ومن ذلك ينتج :-

$$h_x(x) = x^{49} (x^3 +3) - x^4 +3x$$

وبالمقارنة مع متعددة حدود القسمة الخامسة :-

$$\psi_5 (x,y) = 5x^{12} + 6x^9 + 3x^6 + 4x^3 + 5$$

نحصل على :-

$\gcd(h_x(x), f_5(x)) = f_5(x)$

ليكن $\Phi^2(P) = \pm P$ و 2 هو باقي غير تربيعي (*quadratic non residue*) معيار 5 (mod 5)، لذلك نستنتج أن $t \equiv 0 \pmod 5$. وباستخدام مبرهنة الفضلة الصينية يتم حساب t كالأتي :-

$$\left.\begin{array}{l} t \equiv 1 \pmod 3 \\ t \equiv 0 \pmod 5 \end{array}\right\} \rightarrow \begin{array}{l} t \equiv 1*5*2 + 0*3*2 \\ \equiv 10 \pmod{15} \end{array}$$

لكن $|t| \leq 2\sqrt{P}$ وهذا يعني $t = -5$ ومنه فان عدد نقاط المنحنى E :-

$\#E(F_7) = 7 + 1 - (-5) = 13$

وبالاعتماد على الطرائق التي تم توضيحها في هذا البند وباستخدام مبرهنات خاصة يمكن حساب نقاط بعض المنحنيات الاهليلجية المعرفة على الحقول الموسعة والتي تعتمد بالأساس على إيجاد عدد النقاط في الحقل الأصلي أولاً، ومن هذه الطرائق :-

مبرهنة (٢-٢٩) :- ليكن F_q حقلا وليكن E منحنٍ اهليلجياً معرفاً عليه فيوجد عدد صحيح a يحقق العلاقة :-

$$Z(E(F_q); T) = \frac{1 - aT + qT}{(1-T)(1-qT)}$$

حيث أن $Z(E(F_q);T)$ تعرف بأنها دالة Z (*Zeta-Function*) في المنحنيات الاهليلجية [46]. وكذلك فان a تقابل دالة الأثر في تطبيق فروبينيس أي أن :-

$\#E(F_q) = q + 1 - a$

وإذا كان $q = 2^r$ فتوجد طريقة مباشر للحصول على عدد نقاط المنحني باستخدام المبرهنة (٢-٢٩) فيكون :

$$N_r = \begin{cases} 2^r + 1 & \text{if } r \text{ is add} \\ 2^r + 1 - 2(-2)^{r/2} & \text{if is even} \end{cases}$$

حيث N_r يمثل عدد نقاط المنحنى [38].

مبرهنة (٢-٣٠) :- ليكن F_q حقلاً منتهٍ ، و E منحنٍ اهليلجياً معرفاً عليه، إذا كان $\#E(F_q) = q + 1 - c_1$ فان $\#E(F_q) = q^r + 1 - c_n$ حيث

$C_0 = 2$, $C_n = c_1 c_{n-1} - q\, c_{n-2}$

تكون هذه المبرهنة ملائمة للتطبيق في الحقول الموسعة التي يكون مميزها عدداً صغيراً [47].

٢-٣-٧ نماذج من المنحنيات الاهليلجية

هناك تسميات خاصة لبعض من المنحنيات وتعد هذه التسميات بمثابة تصانيف لتلك المنحنيات برغم إنها لا تشمل جميع المنحنيات ، بعض منها يعتمد على عدد النقاط والبعض الأخر يعتمد على كيفية الحصول عليها أو حتى على علاقات هذه المنحنيات بعضها ببعض كما توجد تسميات تعتمد على شكل المحل الهندسي لهذه المنحنيات مثل المنحنى متصل أو مفكك وعموما النوع الأخيرلم تظهر له أي اهمية عند استخدام المنحنيات الاهليلجية في أنظمة التشفير أوفي باقي التطبيقات حتى الوقت الحاضر.

آ- المنحنيات المفردة المفرطة (*Supersingular Curves*)

يسمى المنحنى مفرداً مفرطاً (*supersingular*) أو مفرداً فائقاً إذا كان ثابت المنحنى (j-*invariant*) يساوي صفرا للمنحنيات المعرفة في الحقول الثنائية (*binary field*) أو بعبارة أخرى فان المنحنى في الحقل الثنائي يكون مفرداً مفرطاً، إذا عرف بالمعادلة (4) حيث $\alpha_6 = 0$ ،أما في الحقل الأولى (*prime field*) فان المنحنى المعرف على الحقل (F_p) يكون مفرد مفرط (فائق) إذا كان عدد نقاطه يساوي (p+1) أو بمعنى أخر يكون المنحنى مفرداً مفرطاً إذا كانت دالة الأثر (*trace function*) لتطبيق فروبينيس تساوي صفراً، أي أن مجموع رمز ليجندر يساوي صفراً $\sum(\frac{x^3+ax+b}{p})=0$

اما في الحقول الموسعة فيكون المنحني مفرداً مفرطاً اذا وفقط اذا كان[33] :-

$$t=\sqrt{i*p^m} \qquad ;i=1,2,3,4.$$

ب- المنحنيات الشاذة (*Anomalus Elliptic Curves*)

تسمى المنحنيات الشاذة في الحقول الثنائية بمنحنيات كوبلتز (*Kobiltz curve*) ،وهي المنحنيات المعرفة بالمعادلة (5)، وفيها يكون a_6,a_2 أما 0 او 1 ولكن $a_6 \neq 0$ في المعادلة (5) لذلك، تعرف المنحنيات الشاذة (Anomalous curve) في الحقول الثنائية بإحدى المعادلتين الآتيتين [51] :-

$E(F_{2m})$: $y^2 + xy = x^3 + 1$ ....(12)

$E(F_{2m})$: $y^2 + xy = x^3 + x^2 + 1$ ....(13)

أما في الحقل الأولي فان المنحني الاهليلجي يكون شاذاً عندما تكون دالة الأثر للمنحنى (*trace of curve*) تساوي 1 ، أو بعبارة أخرى يكون المنحنى المعرف بالمعادلة (6) من النوع الشاذ (*Anomalous*) إذا كان عدد نقاط المنحنى يساوي p . ($\#E(F_p) = p$) وفي الحقل الاولي الموسع F_{p^k} يكون المنحنى شاذاً اذا وفقط اذ كان عدد نقاطه يساوي p^n. وهذه

المنحنيات لها بعض الصفات الخاصة ، ومن المتوقع أن تحمل المنحنيات التي يكون فيها (t = 2) صفات مماثلة [24].

جـ- المنحنيات بصيغة مونتجومتري (*Montgomery –Form*)

تسـمى المنحنيـات المعرفـة بالمعـادلات (1),(2),(3),…,(6) بالمنحنيـات المعرفـة بصـيغة وايرسـترس (Weierstrass – Form) وهنـاك صـيغة أخـري للمنحنيـات تعـرف بصـيغة مونتجـومري (Montgomery –Form) وفيهـا يرمـز للمنحنـى بـالرمز (E^M) ويمثـل بالمعادلة :-

$$E^M: By^2 = x^3 + Ax^2 + x \ldots\ldots\ldots(14)$$

والمعادلـة (14) تعرف منحنيات اهليلجيـةٌ تكّون نقاطهـا مـع النقطـة فـي المالانهايـة زمـرة ابدالية ، تمتلك خواص زمرة نقاط المنحنى الاهليلجي بالإضافة إلى أن عدد نقاط هذه النحنيات يقبـل القسـمة علـى 4. يمكـن تحويـل المنحنـى المعـرف بصـيغة وايرسـترس إلـى منحنـى معـرف بالمعادلـة (14) بإيجـاد تماثـل زمـري (Isomorphism group) بين E و E^M حيث إذا كان كل من Eو E^M معرفاً علـى الحقل F_p ، فيوجد $s,t,\alpha,\beta \in F_p$ حيث أن $s \neq 0 \neq t$ ويكون التحويل:-

$$(x,y) \in E(F_p) \rightarrow (s(x-\alpha), t(y-\beta))$$

هو التماثل المطلوب، ومنه نحصل على:-

$$\# E = \# E^M$$

ولكـن عـدد نقـاط E^M يجـب أن يقبـل القسـمة علـى 4، لـذلك لـيس كـل منحنـى بصـيغة وايرسترس يمكن تحويله إلى منحنى بصيغة مونتجومري [37].

د- التدوير التربيعي للمنحنيات الاهليلجية (*quadratic twist*)

يوجد العديد من المنحنيات الاهليلجية في حقل أولي وهذه المنحنيات قد ترتبط فيما بينها بعلاقات خاصة ، التعريف الآتي أحد هذه العلاقات :-

تعريف (٢-٣٢) :

إذا كان E منحنٍ اهليلجياً معطى بالمعادلة :-

$$E: y^2 = x^3 + ax + b$$

فان التدوير التربيعي (*quadratic twist*) $\tilde{E}$ للمنحنى E يُعرف بالمعادلة :-

$$\tilde{E}: y^2 = x^3 + ag^2x + bg^3$$

حيث g باقي غير تربيعي في الحقل المعرف عليه المنحنى [17].

مبرهنة (٢-٣١) [17] :-

$$\#E(F_p) + \#\tilde{E}(F_p) = 2p + 2$$

مبرهنة (٢-٣٢) :-

ليكن العدد الأولي $p \geq 229$ ، و E منحنياً اهليلجياً معرفاً على لحقل F_p ، فأما E أو تدويره التربيعي $\tilde{E}$ ، يمتلك نقطة P تحقق خاصية وجود عدد وحيد يقع ضمن قيود هاس (*Hasse bounded*) ، ويكون $m*P = O_E$ ،حيث m عدد نقاط المنحنى [17].

ويمكن أيضا استخدام البواقي التربيعية لتعريف منحنيات أخرى تمتلك العدد نفسه من النقاط لمنحنى معلوم، فإذا كان h باقي تربيعي في الحقل F_p فان المنحنيان :-

$E_1(F_p): y^2 = x^3 + ax + b$
$E_2(F_p): y^2 = x^3 + ah^2 + bh^3$

يمتلكان العدد نفسه من النقاط ، والتطبيق أعلاه هو تشاكلاً زمرياً بين المنحنيان E_1 و E_2 [41].

هـ- منحنى الحقل الجزئي ***Subfield Elliptic Cerve***

إذ كان E منحنى معرف على الحقل (F_{2m}) بالمعادلة (5) و m = e*d فأن ($F_{2e} \subset F_{2m}$)وإذا كان a_2 , a_6 هما عناصران في الحقل (F_{2e}) فيطلق على المنحنى E منحنى حقل جزئي ويرمز له:-

$$E_{(a_2,a_6)}(F_{2e}) \subseteq E_{(a_2,a_6)}(F_{2m})$$

على شرط ان يكون العددان a_2 , a_6 نفسهما معاملا منحنى الحقل الجزئي . فإذا كان $\#E_{(a_2,a_6)}(F_{2e}) = 2^e+1-t$ ، و α,β هما جذري المعادلة :-

$$x^2 - tx + 2^e = 0$$

فان $\#E_{(a_2,a_6)}(F_{2m})$ يحسب بالمعادلة :-

$$\#E_{(a_2,a_6)}(F_{2m}) = 2^m + 1 - \alpha^d + \beta^d$$

وهذه الصيغة تعرف بنظرية ويل (*Weil's Theorem*) [51].

٣-١ المقدمـة

بعد أول ظهور لها في منتصف الثمانينات من القرن الماضي أخذت أنظمة التشفير التي تعتمد في بناءها على المنحنيات الاهليلجية تشغل مساحة اكبر في الاستخدام كونها الأسرع والأكثر أمنية بحجم مفاتيح اصغر نسبيا بالإضافة إلى كونها الأقل كلفة [53].

وفي هذا الفصل سنبحث في هذه الأنظمة كيفية عملها وتصميمها والجوانب المتعلقة بذلك، وبرغم وجود العديد من الأنظمة التي توظف المنحنيات الاهليلجية في بنائها واختلاف أفكارها إلا أن القاسم المشترك لجميع هذه الأنظمة هي الفكرة الرياضياتية المعتمدة عليها والتي تتعلق بصعوبة حل مسألة اللوغاريتم المنفصل في المنحنيات الاهليلجية والتي يرمز لها اختصاراً (*ECDLP*)، (*Elliptic Curves Discrete Logarithm Problem*) .

تعريف (٣-١) :

اذا كان E منحنٍ اهليلجياً معرفاً على الحقل F_p و p نقطة فيه فان اللوغاريتم المنفصل (*Discrete Logarithm*) في E للأساس P هو عدد صحيح k بحيث أن وجد يحقق العلاقة :-

$$k*P = Q$$

حيث أن Q نقطة أخرى معلومة في المنحنى E. [27]

من أهم ما يميز (*ECDLP*) هو عدم إمكانية تطبيق طرائق تحليل الدليل (*Index Calculus Methods*) عليه، ذلك لان زمرة نقاط المنحنى الاهليلجي متولدة بعدد منته من النقاط [5].عند بناء أنظمة تشفير باستخدام المنحنيات الاهليلجية، هناك عدة جوانب يجب أخذها بنظر الاعتبار مثل اختيار منحنى مناسب [29,5]، ونوع المنحنى المستخدم [37,24] ،وعملية جمع النقاط [46] ،وكيفية تمثيل نقاط المنحنى [38] ،وخوارزميات ضرب النقطة بعدد صحيح [30,18]، وكذلك إغمار الرسالة كنقطة في المنحنى [34,27] بالإضافة إلى كيفية التعامل مع كل هذه المتغيرات مجتمعة [21].ويمكن أن نطلق على هذه الأنظمة أنظمة تشفير المنحنى الاهليلجي (*Elliptic Curve Cryptosystems*) ويرمز لها اختصارا (*ECC*).

٣-٢ اغمار الرسالة كنقطة في المنحنى الاهليلجي

بعض أنظمة (*ECC*) تحتاج إلى أغمار النص الواضح (*Plain text*)، كنقاط في المنحنى الاهليلجي المعرف على الحقل المنته F_p ويتم ذلك بطريقة تضمن استرجاع النص الأصلي، وإحدى هذه الطرائق يمكن وصفها كآلاتي :-

لنفرض أن p عدد أولي كبير نسبيا . وليكن k عدد صحيح كبير بما فيه الكفاية ليحقق لنا نسبة فشل مقبولة مقدارها ( ) عند محاولة اغمار وحدة الرسالة الصريحة m عموما يكون (30 ≤ k ≤ 50) كاف لهذا الغرض.

$\frac{1}{2^k}$

ولنفرض أن وحدات الرسالة الصريحة m تحقق (0 ≤ m ≤ M) وبذلك يجب أن نختار p بحيث يحقق (p > M.k) و p هنا يمثل عدد عناصر الحقل المعرف عليه المنحنى. وثم نجد تطبيقا متباينا بين الاعداد (mk+j) حيث j=1,…,k وعناصر الحقل F_p [34] علما أن بعض المصادر لم تضع حدا أعلى لقيمة k [20].

وبذلك نحسب قيم x بحيث أن {mk+j , j=0,1,…} = {mk+1, mk+2, …} . x =

حتى نحصل على قيمة لـ x تكون فيها المعادلة التكعيبية ($x^3 + ax + b$) باقٍ تربيعي قياس p ، لنحصل على النقطة $(x, \sqrt{x^3 + ax + b})$ والتي تمثل نقطة بالمنحنى.

وتسترجع قيمة m الأصلية عن طريق حساب $m = \lfloor x/k \rfloor$.

وفي الأمثلة الآتية نفرض k = 30.

مثـــال (٣-١) [55] : -

ليكن E منحنٍ اهليلجياً معرفاً على الحقل F_p بالمعادلة.

$E(F_p): y^2 = x^3 + 3x$

حيث p = 4177 ولاغمار الرسالة m = 2174 نقوم اولا بحساب قيمة x حتى نحصل على قيمة x حيث أن :-

$x = \{30*2174 + j \; ; \; j = 1,2,\ldots\}$

$x = 30 * 2174 + 15 = 65235$

التي تجعل الطرف الأيمن من معادلة المنحنى باقياً تربيعياً:-

$x^3 + 3x = (30 * 2174 + 15)^3 + 3(30 * 2174 + 15)$

$= 277614407048580$

$= 1444 \bmod 4177$

$= (38)^2 \bmod 4177$

وبذلك يمكن إن نعبر عن الرسالة m بالنقطة (65235,38)

ولاسترجاع الرسالة الأصلية m نحسب :-

$m = [65235/30] = [2174.5] = 2174$

كما توجد طريقة أخرى لاغمار الرسالة لكنها تستخدم فقط في حالة الأعداد الأولية التي تحقق $p \equiv 3(\text{mod } 4)$ [44].

٣-٣ أنظمـة التشفير باستخدام المنحنيات الاهليلجيـة

توجد أنظمـة تستخدم زمرة نقاط المنحنى الاهليلجي في بنائها أو بعبارة أخرى أنظمة توظف هذه المنحنيات. بعضها شابه في بنائه أنظمة معروفة مثل نظام دايف – هيلمان (*Diffie-Hellman*) وخوارزمية الجمال (*ElGamal*) وأنظمة *RSA* [27]، والبعض الآخر أنظمة قائمة بحد ذاتها مثل نظام منسيز– فنستون (*Menezes-Vanstone*) [31] كما يوجد العديد من خوارزميات التوقيع الرقمي (*Digital Signature*) [25][(١)].

٣-٣-١ نظام دايف – هيلمان لتبادل المفاتيح باستخدام المنحنيات الاهليلجيـة (*Elliptic Curves Diffie –Hellman key Exchange*)

هذه الخوارزمية أو هذا النظام هو لتبادل المفاتيح وليس لتبادل الرسائل وفيه يتم اتفاق طرفين على اختيار مفتاح سري عبر قناة معلنة (قناة غير أمينة) [27].

تعريـف (٣-٢) : دالـة دايـف – هيلمـان (*Diffie-Hellman Function*) [6]

ليكن E منحنى اهليلج معرف على الحقل F_p ولتكن G نقطة فيه رتبتها تساوي q و q عدد أولي فتعرف دالة دايف – هيلمان (*Diffie-Hellman Function*) كالآتي:–

$DH_{E,G}(aG,bG) = abG$

حيث أن a ،b عددان صحيحان يقعان ضمن الفترة [1,q-1]. ومسالة دايف – هيلمان (*The Diffie-Hellman problem*) في E هي حساب $DH_{E,G}$ (P,Q) إذا كان كل من Q,P,G,E معلوما [6].

ويمكن ايجاز عمل نظام دايف – هيلمان لتبادل المفاتيح باستخدام منحنيات الاهليلجية بآلاتي:–

---

(١) سنلحق عبارة "باستخدام المنحنيات الاهليلجية" بعد ذكر اسم نظام التشفير للدلالة على كون النظام يوظف هذه المنحنيات بدلا من ذكر "مشابه نظام ...".

١. يتفق الطرفان المتراسلان B,A على اختيار حقل منته F_p ومنحنٍ اهليلجي E معرف عليه فان المفتاح سوف يتولد من نقطة عشوائية P في ذلك المنحنى (يفضل أن تكون رتبة النقطة عدداً أولياً كبيراً ولكن ذلك ليس ضروريا).

٢. يختار كل من B,A أعداد عشوائية سرية b,a على الترتيب ويحسب كل منها bP,aP على التوالي ويرسله للطرف الآخر.

٣. يحسب كل من B,A المفتاح السري والذي يكون :- abP = baP

٤. أي طرف ثالث متنصت (عدو) e يكون قد حصل على bP,aP,P ولحساب المفتاح abP يجب أن يكون قادرا على حل (ECDLP) [55].

ويمكـن اسـتخدام هـذه الخوارزميـة فـي أنظمـة التشـفير ذات المفتـاح السـري وإحـدى هـذه الاستخدامات هو أن يستعمل الإحداثي السيني للنقطة a bP ،كمفتاح سري لتلك الأنظمة [27].

مثـــال (٣-٢) :-

ليكن E منحنٍ اهليلجياً معرف على الحقل F_{151} بالمعادلة الآتية :-

$E(F_{151}) : y^2 = x^3 + 49x + 41$

ولتكن $P = (118,122)$ نقطة فيه. لنفرض أن A ، B اتفقا على اختيار المنحنى $E(F_{151})$ أعلاه والنقطة P مسبقا حيث ان $\# E = 150$ و P نقطة رتبتها 150 بحيث :-

١. يختار A عددا عشوائيا e_A بحيث أن $1 \le e_A \le 149$ ثم يحسب $e_A.P$ وليكن $e_A = 63$ ويحتفظ به كمفتاح سري فيكون :-

$63P = (76,3)$

ويختار B عددا عشوائيا e_B بحيث أن $1 \le e_B \le 149$ ثم يحسب e_BP وليكن $e_B = 111$ ويحتفظ به كمفتاح سري فيكون:-

$111P = (37,84)$

٢. يتبادل كل من B,A مفتاحيهما e_AP وe_BP ثم يحسب كل منهما مفتاحه السري $e_A.e_BP$ و $e_B.e_AP$ وكالآتي:-

$e_A.e_BP = 63 * (37,84) = (63,117)$
$e_A.e_BP = 111*(76,3) = (63,117)$

وبذلك يحصل كل طرف على النقطة نفسها.

٣. لايستطيع أي متنصت حصل على النقاط (118,122) ,(76,3), (37,84) حساب (63,117)، بدون حل (ECDLP) .

مثـــال (٣-٣) :-

ليكن E منحنٍ اهليلجياً معرفاً على الحقل F_{3023} بالمعادلة آلاتية:-

$E(F_{3023})$: $y^2 = x^3 + 2x + 1$

ولتكن $P = (1,2)$ نقطة فيه نلاحظ أن $\# E = 3054$.

١- يختار A العدد e_A ويحتفظ به وليكن $e_A = 1026$ ثم يحسب e_AP حيث أن

$e_AP = 1026 * (1,2) = (2750,1168)$

ويختار B العدد e_B ويحتفظ به أيضا وليكن $e_B = 523$ ثم يحسب e_BP حيث أن:-

$e_BP = 532 * (1,2) = (1088,343)$

٢- يحسب كل من الطرفين المفتاح السري من خلال:-

$e_A . e_BP = 1026 * (1088,343) = (1075,408)$

$e_B . e_AP = 523* (2750,1168) = (1075,408)$

٣- وبـدون حـل (*ECDLP*) لايمكـن الحصـول علـى أي مـن e_A أو e_B لحسـاب المفتـاح (1075,408).

٣-٣-٢ <u>نظام ميسي – اومورا باستخدام المنحنيات الاهليلجية</u>

(Elliptic Massey - Omura)

في هذا النظام يكون كل من المنحنى والحقل المعرف عليه معلنا وكذلك عدد نقاط المنحنى فإذا أراد الطرفان A ، B تبادل النص الواضح P ، التي يجب أن تكون نقطة في المنحنى الاهليلجي E، عليهما إجراء الخطوات الآتية :-

١ . يختـار الطـرف A عـدد صـحيح e_A بصـورة عشـوائية ضـمن الفتـرة [1,N] ويحقـق $gcd(e_A,N) = 1$ حيث N عدد نقاط المنحنى. ثم يحسب e_AP ويرسلها إلى الطرف B.

٢ . يختـار B عددا e_B بالطريقـة نفسـها التـي تـم بهـا اختيـار e_A ، ثـم يحسـب $e_B(e_AP)$ ، ويرسلها إلى الطرف A مرة أخرى.

٣ . الطـرف A يحسـب العـدد d_A بحيث أن $d_A = e_A^{-1}(mod\ N)$ ثـم بعـد ذلـك يحسـب $d_A(e_Be_AP) = e_BP$، ويرسلها إلى B.

٤ . يقوم الطرف B بحساب d_B بحيث أن $d_B = e_B^{-1}(mod\ N)$ ثم يسترجع الرسالة الأصلية بإجراء الحسابات آلاتية: $d_B\ d_A(e_Ae_BP) = d_B(e_BP) = P$.

٥ . أي متنصت تعرف على $P,\ e_AP,\ e_Be_AP,\ e_BP$ لا يستطيع حساب النص الواضح P بدون حل الـ(ECDLP) .[55]

مثـــال (٣-٤) :-

ليكن E المنحنى المعطى في المثال (٣-٢) ولتكن الرسالة الواضحة هي $P = (126,42)$.

الحــل :- لتشفير النص الواضح :-

١- يختار A عدداً e_A بحيث يكون $gcd(e_A,150) = 1$ وليكن $e_A = 77$ ثم يحسب:-

$e_A.P = 77 * (126,42) = (35,29)$

ويرسلها إلى الطرف الأخر B.

٢- يختار B عددا e_B بحيث يحقق $gcd(e_B,150) = 1$ وليكن $e_B = 91$ ثم يحسب $e_B.e_AP$ ويرسلها إلى A مرة أخرى أي أن:-

$e_B (e_AP) = 91 * (35,29) = (79,114)$

٣- يعود الطرف A ويحسب $d_A = e^{-1}(\text{mod } 150)$ فيكون :

$d_A = 113 \text{ (mod } 150)$

$d_A * (e_B\, e_AP) = 113 * (79,114) = (121,67)$

٤- بعد أن تسلم الطرف B الرسالة الجديدة عليه أجراء الحسابات الآتية لاسترجاع النص الواضح :-

حساب d_B والذي يحقق $d_B.e_B = 1 \text{ (mod } 150)$ أي أن

$d_B = 61 \text{ (mod } 150)$

ومن ثم :

$d_B^* (d_A\, d_B\, e_B\, e_AP) = 61 * (121,67)$

$= (126,42)$

مثـــال (٣-٥) :-

باستخدام المنحنى المعطى في المثال (٣-٣)، وضح كيفية تبادل الرسالة $G = (2557,2380)$ بين A، B .

الحــل :-

١- يختار A عدداً صحيحاً e_A بصورة عشوائية وليكن $e_A = 2683$ ثم يحسب

$e_A .P = 2683 * (2557,2380)$

$= (183,2710)$

ويرسل $e_A . P$ الى الطرف B .

٢- يختار الطرف B عدداً صحيحاً $e_B = 1763$ بصورة عشوائية ويحسب

$e_B .(e_A .P) = 1763 * (2209,2698) = (49,476)$

ويرسله الى الطرف A

٣- الطرف A يحسب d_A ويجد $d_A.(e_B.(e_A,G))$ حيث

$d_A = 1243 \pmod{3054}$

$d_A.(e_B.(e_A,G) = 1243 * (49,476)$

$= (2087,2093)$

١. يقوم B بحساب النص الصريح من خلال:-

$d_B = 1637 \pmod{3023}$

$P = 1637 * (2087,2093)$

$= (2557,2380)$

٣-٣-٣ خوارزمية تشفير الجمال باستخدام المنحنيات الاهليلجية

(*El-Gamal Algorithm using Elliptic Curve*)

تطبق المنحنيات الاهليلجية على خوارزمية الجمال أيضا وفي هذا النظام يجب أن تكون وحدات الرسالة نقاطاً في المنحنى أو تحول إلى تلك الصورة. ويمكن ايجاز عمل هذا النظام بالآتي [27] :-

١. بناء المفتاح المعلن :-

لبناء مفتاح معلن يتم اولا اختيار منحنى مناسب E معرف على حقل منته F_p ويتم كذلك اختيار نقطة G في المنحنى ويفضل أن تكون هي النقطة المولدة لأكبر زمرة جزئية من نقاط المنحنى الاهليلجي، أي انها تكون نقطة ذات اكبر رتبة. ثم يختار الطرف A عدد من الحقل F_p بصورة عشوائية ويحتفظ به كمفتاح سري ثم يحسب:-

$$Q = k * G$$

وبذلك يكون المفتاح المعلن هو

$$(G, Q, p, \#E)$$

٢. تشفير النص الواضح

لتكن P وحدة النص الواضح ، يقوم الطرف B باختيار عدد صحيح e_B ضمن الحقل F_p ويحتفظ به، ثم يحسب النص المشفر C والذي يكون

$$C = (e_B G, P + e_B Q)$$

٣. فك التشفير

لاسترجاع النص الواضح ، يقوم A باجراء الحسابات آلاتية:-

$$D = P + e_B Q - k * (e_B G) = D$$

ونلاحظ من خطوتي التشفير وفك الشفرة بان

$$e_B * Q = e_B * k * G = k * e_B G$$

وهذا ما توضحه الامثلة الآتية:-

مثـــال (٣-٦) : -

بين كيفية تبادل الرسالة المعطاة في المثال (٣-٤) باستخدام المنحنى نفسه مع خوارزمية تشفير الجمال؟

الحـــل :-

١. بناء المفتاح المعلن:-

لتكن $G = (118,122)$ وليكن $k = 52$ فان

$Q = k * G = 52 * (118,122) = (80,121)$

فيكون المفتاح المعلن هو:-

$((118,122), (80,121), 151, 150)$

٢. تشفير النص الواضح:-

ليكن $e_B = 135$ فان:-

$e_B * G = 135 * (118,122) = (58,100)$
$e_B * Q = (57,33)$
$P + e_B * Q = (126,42) + (57,33) = (137,101)$
$C = ((58,100),(137,101))$

٣. فك الشفرة:-

$k * e_B * G = 52. (58,100) = (57,33)$
$D = (p + e_B * Q) – k * (e_B * G)$
$= (137,101) + (57,118) = (126,42) = P$

مثـــال (٣-٧) :-

بين كيفية تبادل الرسالة المعطاة في المثال (٣-٥) باستخدام المعطيات نفسها مع خوارزمية تشفير الجمال باستخدام منحنيات الاهليلجية؟

الحـــل :-

الرسالة $P = (2557,2380)$ و $G = (1,2)$

١. بناء المفتاح المعلن:-

ليكن $k = 659$ فيكون:-

$Q = k * G = 659 * (1,2) = (1167,1161)$

فيكون المفتاح المعلن هو:-

$((1,2), (1167,1161), 3023, 3054)$

٢. تشفير النص الواضح:-

يختار الطرف B عدداً ضمن الحقل F_{3023} وليكن $e_B = 873$ ويحسب :-

$e_B * G = 873 * (1,2) = (2551,8)$
$e_B * Q = 873 * (1167,1161) = (536,810)$
$P + e_B * Q = (2557,2380) + (536,810)$
$= (1535,1769)$

وبذلك يكون النص المشفر:-

$C = (e_B * G, P+e_B*Q) = ((2551,8) , (1535,1769))$

ولاسترجاع النص الواضح :-

$D = (P + e_B * Q) – k * (e_B * G)$
$= (1535,1769) – (536,810) = (1535,1769) + (536,2213)$
$= (2557,2380) = P$

٣-٣-٤ نظام منسيز – فنستون (*Elliptic Curve Menezes-Vanstone system*)

وهو أحد أنظمة تشفير المنحنيات الاهليلجية (*ECC*) والذي تم تصميمه على فكرة استخدام منحنيات وليس مجرد تطبيق أو إدخال المنحنيات على نظام موجود كما في الأنظمة الثلاثة السابقة. ومن ثم أهم ما يميز هذا النظام هو عدم الحاجة الى اغمار وحدات النص الواضح كنقاط في المنحنى الاهليلجي ويمكن وصف هذا النظام بالآتي [31]:-

١. عملية بناء المفتاح المعلن:-

تكون مشابهة لتلك المستخدمة في خوارزمية تشفير الجمال باستخدام منحنيات الاهليلجية، فبعد اختيار الحقل والمنحنى المعرف عليه يتم اختيار نقطة ذات رتبة مناسبة (والتي نفضل أن تكون النقطة المولدة لأكبر زمرة جزئية في المنحنى وان لم يكن ذلك ضروريا) ولتكن G، ثم يتم اختيار عدد صحيح k ضمن الحقل F_p بصورة عشوائية وتحسب النقطة

$$Q= k * G$$

وبذلك يكون المفتاح المعلن: $(G , Q , p , \#E)$

٢. التشفير:-

لتشفير نص واضح والذي هو عبارة عن زوج مرتب من الاعداد الذي قد لايكون نقطة في المنحنى وليكن النص هو $P = (x,y)$ فيتم اختيار عدد عشوائي e وحساب النص المشفر

الذي يكون :-

$$C = (e * G, c_1x(mod\ p), c_2y(mod\ p))$$

حيث أن $(c_1,c_2) = e * Q$

٣. فك التشفير:-

لاسترجاع النص الصريح من المشفر ، يقوم الطرف الأول باجراء الحسابات *باستخدام مفتاحه السري k* لحساب كل من c_2,c_1 من خلال :-

$$(c_1,c_2) = k*e * G = e * Q$$

وبحساب c_2^{-1} , c^{-1}_1 للمعيار p ،يمكن حساب النص الواضح من خلال :-

$$D = ((c_1x)c_1^{-1}(mod\ p), (c_2y)c_2^{-1}(mod\ p))$$

مثـــال (٣-٨) :-

ليكن E المنحنى المعرف على الحقل F_{151} بالمعادلة

$E(F_{151}): y^2 = x^3 + 49x + 41$

ولـــتكن الرســـالة واضـــحة هـــي:- P=(20,130) أو P=(143,13) أو P=(50,108) أو P=(126,42) .

الحـــل :- نأخذ G = (118,122)

بناء المفتاح المعلن:-

ليكن k = 52 نحسب

$Q = k*G = 52 * (118,122) = (80,121)$

وبذلك يكون المفتاح المعلن هو:-

((118,122), (80,121), 151, 150)

تشفير النص الواضح:-

ليكن e = 91 ، $e*G = 91 * (118,122) = (72,26)$ بعد ذلك

١. إذا كان P = (20,130) فان C = (72,26,36,92)

٢. إذا كان P = (143,13) فان C = (72,26,46,130)

٣. إذا كان P = (50,108) فان C = (72,26,90,23)

٤. إذا كان P = (126,42) فان C = (72,26,106,118)

ولاسترجاع النص الواضح ، نحسب اولاً:-

$k*e*G = 52 * (72,26)$

$= (32,10) = (c_1,c_2)$

$c_1^{-1} = 118(mod\ 151)$

$c_2^{-1} = 136(mod\ 151)$

ثم نحسب $D = ((c_1x)118(\text{mod } 151), (c_2y)\ 136(\text{mod } 151))$ فيكون:-

١- $D = (36 * 118 \text{ mod } (151), 92 * 136 \text{ mod } (151)) = (20,130).$

٢- $D = (46 * 118 \text{ mod } (151), 130 * 136 \text{ mod } (151)) = (143,13).$

٣- $D = (90 * 118 \text{ mod } (151), 23 * 136 \text{ mod } (151)) = (50,108).$

٤- $D = (106 * 118 \text{ mod } (151), 118 * 136 \text{ mod } (151)) = (126,42).$

مثـــال (٣-٩) :-

ليكن E المنحنى المعرف على الحقل $p = 3023$ بالمعادلة

$E(F_p): y^2 = x^3 + 2x + 1$

ولتكن $G = (1877,371)$ وليكن $k = 149$ وليكن النص الواضح هو:-

$P_1=(311,66)$ و $P_2=(1374,2999)$ و $P_3=(100,44)$ $P_4=(2557,2380)$

لبناء المفتاح المعلن نحسب اولاً:-

$Q = k * G = 149 * (1877,371) = (1420,2750)$

وبذلك فان المفتاح المعلن هو:-

$((1877,371), (1420,2750), 3020, 3054)$

لتشفير النص الواضح نختار عددا صحيحا ضمن الحقل F_p وليكن $e = 1690$ ونحسب:

$e*P$ و $e*Q$ و (c_1,c_2) ثم نحسب

$C = (e * p, C_1x_1 \text{ mod } P, C_2y_1 \text{ mod } P)$

$e*G = 1690 * (1877,371) = (2619,1685)$

$e*Q = 1690 * (1420,2750) = (1031,2695) = (c_1,c_2)$

ثم نحسب $c_2 * y \text{ (mod p)}$, $c_1 * x \text{ (mod p)}$

١. إذا كانت الرسالة :- $P = (311,66)$

$c_1x \text{ mod } p = 1031 * 311 = 203 \text{ (mod p)}$

$c_2\ y \text{ mod } p = 66 * 2695 = 2536 \text{ (mod p)}$

وبذلك فان النص المشفر يكون:-

$C = ((2619,1685), 203, 2536)$

٢. الرسالة $P = (1374,2999)$

$c_1x \text{ mod } p = 1031 * 1374 = 1830 \text{ (mod p)}$

$c_2y \text{ mod } p = 2695 * 2999 = 1826 \text{ (mod p)}$

وبذلك فان النص المشفر يكون:-

$C = ((2619,1685), 1830, 1826)$

٣. الرسالة $P = (100,44)$ يكون:-

$c_1x \bmod p = 1031 * 100 = 318 \pmod p$
$c_2y \bmod p = 2695 * 44 = 683 \pmod p$

وبذلك فان النص المشفر يكون:-

$C = ((2619,1685), 318, 683)$

٤. الرسالة $P = (2557,2380)$ يكون:-

$c_1x \bmod p = 1031 * 25557 = 211 \pmod p$
$c_2y \bmod p = 2695 * 2380 = 2317 \pmod p$

وبذلك فان النص المشفر يكون:-

$C = ((2619,1685), 211, 2317)$

ولاسترجاع النص الواضح يتم حساب c_2,c_1 اولا من خلال:-

$(c_1,c_2) = k * e*G = 149 * (2619,1685) = (1031,2695).$

ومن ثم حساب $c_1^{-1} \pmod p$ و $c_2^{-1} \pmod p$ حيث أن:-

$c_1^{-1} = 2548 \quad , c_2^{-1} = 2129$

يسترجع النص الواضح من النص المشفر بالحسابات الآتية:-

$D = ((c_1x) * c_1^{-1} \bmod p, (c_2y) * c_2^{-1} \bmod p)$

أي أن:-

١- $D = (203 * 2548 \pmod p, 2536 * 2129 \pmod p) = (311,66)$

٢- $D = (1830 * 2548 \pmod p, 1826 * 2129 \pmod p) = (1374,2999)$

٣- $D = (318 * 2548 \pmod p, 683 * 2129 \pmod p) = (100,44)$

٤- $D = (211 * 2548 \pmod p, 2317 * 2129 \pmod p) = (2557,2380)$

مثـــال (٣-١٠) :-

وضح كيفية تبادل الرسالة الآتية :-

" Performance Evaluation of using Elliptic Curves Cryptosystems"

باستخدام نظامي الجمال ومنسيز- فنستون والمنحنى الاهليلجي E المعرف على الحقل $p = (10^7 + 19)$ بالمعادلة:-

$E(F_p) : y^2 = x^3 + 3x + 1$

وباستخدام $G = (2,4417259)$ كنقطة ذات رتبة كبيرة.

الحـــل :-

أول شيء يجب القيام به هو بناء المفتاح المعلن :-

نلاحظ أن عدد نقاط المنحنى أعلاه هو (9999846) ، وليكن $k = 5553122$ فان:-

$Q = k * G = 5553122 * (2,4417259)$
$= (1,866032)$

يكون المفتاح المعلن:-

((2,4417259), (1,866032), 10^7 + 19, 9999846)

وهو مفتاح لكل من خوارزمية الجمال ونظام منسيز- فنستون . ثم نقوم بتحويل الرسالة إلى ترميز رقمي (*Digital Code*) وتقطيعها لتكوين وحدات النص الصريح (m_i) والتي هي عبارة عن ترميز يتكون من 5 مقاطع (5-*digits*) ، والترميز الذي تم تطبيقه هو بمقابلة الـ 0 للفراغ والعدد 1 للحرف A وهكذا وصولاً للعدد 26 الذي يقابل الحرف Z .

(x_1, x_2, …,x_{25})= (16051, 80615, 18130, 11403, 5000, 12210, 12009, 15140, 1506, 211, 90914, 7000, 51212, 9162, 903, 32, 11822, 5000, 3182, 51620, 15192, 51920, 5131, 90000).

اولاً:- خوارزمية تشفير الجمال:-

أن خوارزمية الجمال تتطلب أن تكون وحدات الرسالة هي نقاط في المنحنى الاهليلجي وبذلك يكون النص الواضح متمثلا بالوحدات الآتية:-

m'_1 = (481530, 1680763)
m'_2 = (2418451, 7270346)
m'_3 = (543903, 9341691)
m'_4 = (342091, 609932)
m'_5 = (150000, 4655792)
m'_6 = (1566030, 1709957)
m'_7 = (366302, 516172)
m'_8 = (360270, 349753)
m'_9 = (454200, 7219718)
m'_{10} = (45180, 9077481)
m'_{11} = (6332, 9896500)
m'_{12} = (2727420, 6211905)
m'_{13} = (210004, 1161265)
m'_{14} = (1536361, 4008896)
m'_{15} = (274860, 9874582)
m'_{16} = (27091, 1571081)
m'_{17} = (963, 2649988)
m'_{18} = (354663, 2165051)
m'_{19} = (150000, 4655792)
m'_{20} = (95461, 4624794)
m'_{21} = (1548600, 3001142)

m'_{22} = (455763, 5247101)
m'_{23} = (1557601, 5558191)
m'_{24} = (153930, 9990849)
m'_{25} = (2700000, 3998122)

ولحساب النص المشفر نختار قيمة e_B=67235 ونستخدم المعادلة :

C_i= (67235*(2,4417259) , m_i + 67235 *(1,866032))

وبذلك يكون النص المشفر:

C_1=((8693902 , 2014050),(4851772 , 7592394))
C_2=((8693902 , 2014050),(7714495 , 7696219))
C_3=((8693902 , 2014050),(1430849 , 4022018))
C_4=((8693902 , 2014050),(7325288 , 2596807))
C_5=((8693902 , 2014050),(2354515, 4530449))
C_6=((8693902 , 2014050),(6082407 , 5878590))
C_7=((8693902 , 2014050),(551311 , 1912881))
C_8=((8693902 , 2014050),(9004404 , 5640640))
C_9=((8693902 , 2014050),(875179 , 6469340))
C_{10}=((8693902 , 2014050),(1627744 , 5550270))
C_{11}=((8693902 , 2014050),(9022308 , 4284344))
C_{12}=((8693902 , 2014050),(8566727 , 3945296))
C_{13}=((8693902 , 2014050),(5741886 , 1352242))
C_{14}=((8693902 , 2014050),(9699338 , 667285))
C_{15}=((8693902 , 2014050),(8528719 , 3534626))
C_{16}=((8693902 , 2014050),(5840189 , 887866))
C_{17}=((8693902 , 2014050),(8306885 , 7663883))
C_{18}=((8693902 , 2014050),(681500 , 9716743))
C_{19}=((8693902 , 2014050),(2354515 , 1530449))
C_{20}=((8693902 , 2014050),(1759633 , 8712698))
C_{21}=((8693902 , 2014050),(3641212 , 9937758))
C_{22}=((8693902 , 2014050),(9534095 , 4161340))
C_{23}=((8693902 , 2014050),(2584156 , 3358539))
C_{24}=((8693902 , 2014050),(4383929 , 2710688))
C_{25}=((8693902 , 2014050),(5334704 , 2208999))

ولاسترجاع النص الأصلي ، علينا إجراء الحسابات الآتية:

D_i= {m_i + 67235*(1,866032)} - 5553122* 67235 *(2,4417259)

للحصول على النص الواضح الذي يكون على الترتيب :

m'_1 = (481530, 1680763)
m'_2 = (2418451, 7270346)
m'_3 = (543903, 9341691)

m'_4 = (342091, 609932)
m'_5 = (150000, 4655792)
m'_6 = (1566030, 1709957)
m'_7 = (366302, 516172)
m'_8 = (360270, 349753)
m'_9 = (454200, 7219718)
m'_{10} = (45180, 9077481)
m'_{11} = (6332, 9896500)
m'_{12} = (2727420, 6211905)
m'_{13} = (210004, 1161265)
m'_{14} = (1536361, 4008896)
m'_{15} = (274860, 9874582)
m'_{16} = (27091, 1571081)
m'_{17} = (963, 2649988)
m'_{18} = (354663, 2165051)
m'_{19} = (150000, 4655792)
m'_{20} = (95461, 4624794)
m'_{21} = (1548600, 3001142)
m'_{22} = (455763, 5247101)
m'_{23} = (1557601, 5558191)
m'_{24} = (153930, 9990849)
m'_{25} = (2700000, 3998122)

ولاسترجاع وحدات النص الواضح الاصلية ، نعوض $x_i = \left\lfloor \frac{x'_i(m'_i)}{30} \right\rfloor$ فينتج ما يلي:

$(x_1, x_2, \ldots, x_{25})$= (16051, 80615, 18130, 11403, 5000, 12210, 12009, 15140, 1506, 211, 90914, 7000, 51212, 9162, 903, 32, 11822, 5000, 3182, 51620, 15192, 51920, 5131, 90000).

ثانياً:- نظام منسيز – فنستون (*Menzes –Vanstom*)

هذا النظام لا يتطلب اغمار الرسالة كنقطة في المنحنى لذلك سنأخذ وحدات النص الصريح التي تم تقطيعها بالجزء الاول من المثال ونأخذ كل وحدتين باعتبارها وحدة رسالة واحدة وكالآتي:-

m_1 = (16051, 80615)
m_2 = (18130, 11403)
m_3 = (5000, 52201)
m_4 = (12210, 12009)

m_5 = (15140, 1506)
m_6 = (211, 90914)
m_7 = (7000, 51212)
m_8 = (9162, 903)
m_9 = (32, 11822)
m_{10} = (5000, 3182)
m_{11} = (51620, 15192)
m_{12} = (51920, 5131)
m_{13} = (90000, 0)

ولحساب النص المشفر نختار قيمة e =67235 ونستخدم المعادلة :

C_i= (67235*(2,4417259) , 74747*x_i(mod p) , 5878626*y_i(mod p))

وبذلك يكون النص المشفر:

C_1 = ((4198190, 1103787), (8809718, 1862039))
C_2 = ((4198190, 1103787), (1594912, 924182))
C_3 = ((4198190, 1103787), (7400706, 6231980))
C_4 = ((4198190, 1103787), (6992503, 4435550))
C_5 = ((4198190, 1103787), (5689306, 2092595))
C_6 = ((4198190, 1103787), (5684320, 5993252))
C_7 = ((4198190, 1103787), (4360977, 9313279))
C_8 = ((4198190, 1103787), (4785037, 4143175))
C_9 = ((4198190, 1103787), (4711373, 1074777))
C_{10} = ((4198190, 1103787), (7400706, 2694975))
C_{11} = ((4198190, 1103787), (8644760, 5651168))
C_{12} = ((4198190, 1103787), (4688794, 9433673))
C_{13} = ((4198190, 1103787), (3212461, 0))

ولاسترجاع النص الصريح يجب أجراء الحسابات الآتية :-

(c_1,c_2) = k*e*G = 5553122 * (4198190, 1103787)
= (74747, 5878626)

وبذلك يكون:-

(c_1^{-1}(mod p), c_2^{-1}(mod p)) = (453481, 8520662)

ثم يحسب النص الواضح بالعلاقة:-

D = ((c_1x). c_1^{-1}(mod p), (c_2y). c_2^{-1}(mod p))

ويكون بالترتيب الأتي:-

m_1 = (16051, 80615)
m_2 = (18130, 11403)
m_3 = (5000, 52201)
m_4 = (12210, 12009)
m_5 = (15140, 1506)
m_6 = (211, 90914)

m_7 =(7000,51212)
m_8 = (9162, 903)
m_9 = (32, 11822)
m_{10} = (5000, 3182)
m_{11} = (51620, 15192)
m_{12} = (51920, 5131)
m_{13} = (90000, 0)

٣-٣-٤ خوارزميـة التوقيع الرقمـي باستخدام المنحنيـات الاهليلجيـة :-

(Elliptic Curve Digital Signature Algorithm)

فـي عـام ١٩٩٢ تـم تصـميم أول خوارزميـة للتوقيـع الرقمـي باسـتخدام المنحنيـات الاهليلجيـة (*ECDSA*) لمؤسسة (*NIST*) (*National Institute of Standards and technology*) بالاعتماد على خوارزمية التوقيع الرقمي (*DSA*) (*Digital Signature Algorithm*) [25].

التوقيـع الرقمـي عبـارة عـن عـدد يعتمـد علـى مفتـاح سـري ، يكـون محتـوى فـي الرسـالة الموقعة بحيث يمكن التحقق منه بدون معرفة المفتاح السري الذي يكون معروفاً من قبل الشخص صـاحب التوقيـع فقط ، كذلك فـان أي شـخص يسـتطيع حسـاب توقيـع كل الرسـائل لشـخص مـا، لايستطيع أن يوقع أي رسالة بدلا عنه [56].

لنفرض أن الطـرف A يرغـب بتوقيـع رسـالة رقميـة ويبعـث بهـا إلـى الطـرف B، فكلاهمـا يختـار حقـلاً منتـه ولـيكن F_p ومنحنـى اهلـيلج E معـرف عليـه ، ونقطـة G ذات رتبـة n فـي المنحنى. يقوم A بحساب مفتاحه المعلن والذي يكون:-

$Q = d * G$

حيث يعلن Q ويحتفظ بـ d كمفتـاح سري. ولتوقيـع الرسـالة M رقميـا ،علـى A إجراء الخطـوات الآتية:-

١. اختيار عدد عشوائي k بحيث أن $1 \leq k \leq n-1$.
٢. حساب $k*G = (x_1,y_1)$ و$r = x_1 \pmod n$ فإذا كان $r = 0$ يتم الرجوع إلى الخطوة الأولى واختيار عدد عشوائي آخر.
٣. حساب $k^{-1} \pmod n$.
٤. حساب $e = SHA^{-1}(M)$ حيث SHA^{-1} تمثل دالة هاش (*Hash Function*).
٥. حساب $s = k^{-1}(e + dr) \pmod n$ فإذا كان $s = 0$ يتم الرجوع إلى الخطوة الأولى واختيار k جديد.
٦. يكـون (r,s) توقيعـاً للرسـالة M ولمطابقتـه والمصـادقة عليـه، علـى B إجـراء الخطـوات الآتية:-

١. التحقق من أن r ، s عددان صحيحان ضمن الفترة [1,n-1].
٢. حساب $e = - SHA^{-1}(M)$.
٣. حساب $w = s^{-1} \pmod n$.
٤. حساب $U_2 = r*w \pmod n$، $U_1 = e*w \pmod n$.
٥. حساب $x = U_1G + U_2Q$ فإذا كان $x = O_E$ فان B يرفض التوقيع ، و في غير ذلك يحسب $v = x_1 \pmod n$ حيث $x = (x_1,y_1)$.
٦. قبول التوقيع إذا كان $v = r$ [38].

ومن عمليتي التوقيع والمطابقة أعلاه نلاحظ أن

$$s = k^{-1} (e + dr) \pmod n$$
$$k = s^{-1} (e + dr) = s^{-1}e + s^{-1}rd$$
$$= we + wrd = U_1 + U_2d \pmod n$$

ولكن

$$U_1G + U_2Q = (U_1 + U_2d)G = k*G$$

ومنه ، يجب ان يكون $v = r$.

يوجد العديد من إصدارات التواقيع الرقمية لكثير من المؤسسات، ويوجد العديد من الأنواع التي تم فيها استخدام المنحنيات الاهليلجية على أنظمة اعتيادية مناظرة لها [25].

٣-٤ مهاجمة أنظمة تشفير المنحنيات الاهليلجية (*Attack of ECC*)

بصورة عامة تقّوم أمنية أنظمة التشفير بالاعتماد على كمية الوقت اللازم لكسرها (اختراق النظام) وهذا يعني حساب المفتاح السري المستخدم في تشفير الرسالة والطرائق المستخدمة لكسر هذه الأنظمة تسمى طرائق المهاجمة (*attacking methods*) ، ومن الطبيعي فان كمية الوقت اللازمة لكسر أنظمة تشفير ،عملية لايمكن حسابها بصورة فعلية لان الأنظمة التي يمكن حساب وقت كسرها بالضبط تعتبر أنظمة غير مؤهلة للاستخدام، وبدلا من حساب كمية الوقت اللازمة لكسر هذه الأنظمة يمكن نظريا تخمين ذلك بأخذ مقدار الوقت اللازم لتطبيق طرائق المهاجمة وبوجود اكثر من طريقة فيتم اخذ المعدل لها [49].

سنقدم في هذا البند بعض طرائق مهاجمة أنظمة تشفير المنحنيات الاهليلجية والتي وان لم تكن طرائقا عامة إلا أن بعضها يطبق بنجاح في حالات خاصة.

٣-٤-١ هجوم سلفر- بولنـغ- هيلمـان

(*The Silver-Pohling-Hellman Attack*)

تستخدم هذه الخوارزمية لإيجاد اللوغاريتم المنفصل في الزمر الدوارة (*cyclic groups*) والفكرة الأساسية لها هو أيجاد العدد x للمعيار p^k ($x \bmod p^k$) لأكبر قوة k للعدد الأولـي p حيث p تقسم رتبـة الزمـرة (*group's order*) واسـتخدام مبرهنـة الفضـلة الصينية لحساب قيمة x النهائية [17]. ويمكن وصف عمل الخوارزمية بالخطوات الآتية:-

١ . ***لتكن كل من Q, P نقطتين فـي منحنـى اهليلج حيث أن P = x*Q و x عدد صحيح، وكل من P ، Q نقاط معلومة.***

٢ . ***نحسب أولا جميع العوامل الأولية لعدد نقاط المنحنى حيث يكون***

$$\#E = p_1^{\alpha_1}.p_2^{\alpha_2}.....p_k^{\alpha_k}$$

٣ . .***نحسب النقاط:- t_{Pi}. $J = j(\#E/p_i).p$; $0 \le p < p_I$ ونضع جميع الحسابات في جدول.***

٤ . ***نحسب اللوغاريتم المنفصل من Q للأساس P وللمعيار P_i وذلك من خلال :-***

$$x = x_0 + x_1p_1 + \ldots + x_{\alpha i-1}p^{\alpha i-1} \qquad (٤-١)$$

حيث أن $0 \le x_n < p_i-1$

- ***حيث يتم اولا حساب x_0 من خلال:-***

$$(\#E / p_i) = r_{pi,\, j}$$

ومقارنة قيمة $r_{pi,\, j}$ مع الجدول في الخطوة ٢ نحصل على قيمة ($x \bmod p_i$) في حالة كون $\alpha_i = 1$.

أما إذا كان $\alpha_i > 1$ فنستمر بحساب قيم x من خلال $x_0, x_1, \ldots, x_{\alpha i}$.

- ***ولإيجاد x_1 نحسب اولا $x_0P - R = Q$***

ومن ثم $x_1 = (\#E / P_i^2) * R$.

فإذا كان $\alpha i = 2$ يكون $x = x_0 + P_ix_1$ وفي غير ذلك نستمر حيث

-نحسب x_2 . $G = Q - x_0P - x_1R$

فيكون G . $x_2 = (\#E / P_i^3)$ و بالترتيب نفسه نستمر لإيجاد القيم المطلوبة.

(٤-٢) باستخدام مبرهنة الفضلة الصينية نحسب اللوغاريتم المنفصل x المطلوب.

مثـــال (٣-١١) [17] :-

ليكن E منحنٍ اهليلجياً معرف على الحقل F_{151} بالمعادلة:

$E\ (F_{151}): y^2 = x^3 + 49x + 41$

وليكن $P = (118,122)$ فالمطلوب أيجاد قيمة x بحيث أن $Q = x * P$ حيث أن $Q = (6,131)$.

الحـــل :- عدد نقاط المنحنى E ،هو 150 ومنه يكون:-

$150 = 2*3*5^2$

فنحسب :- $0 * P = O_E$

$(150/2)*P = 75*P = (92,0)$

$(150/3)*P = 50*P = (114,127)$, $2*(150/3)*P = 100*P = (114,24)$

$(150/5)*P = 30*P = (57,118)$, $2*(150/5)*P = 60*P = (41,1)$,

$3*(150/5)*P= 90*P = (41,150)$, $4*(150/5)*P = 120*P = (57,33)$

وبذلك فان الجدول بقيم t_{pi}، j **يكون:-**

P_i	j				
	0	1	2	3	4
2	O_E	(92,0)			
3	O_E	(114,127)	(114,24)		
5	O_E	(57,118)	(41,1)	(41,150)	(57,33)

ولحساب $(x \bmod p_i)$ يكون:-

$(150/2)*Q = (92,0)$

ومن الجدول نلاحظ أن $x \equiv 1 \pmod 2$

$(150/3)*Q = (114,127)$

ومن الجدول فان $x \equiv 1 \pmod 3$

ولحساب $(x \bmod 25)$ يكون $x = x_0 + 5x_1 \pmod{25}$ فيكون:-

$(150/5)*Q = (57,33) \rightarrow x_0 \equiv 4$

$R = Q - 4*P = (6,131) + (121,84) = (92,0)$

$(150/25)*R = 6*(92,0) = O_E \rightarrow x_1 = 0$

$\therefore x = x_o + 5*x_1 \pmod{25} = 4 + 0 = 4 \pmod{25}$

وباستخدام مبرهنة الفضلة الصينية (Chinese Remainder Theorem) نجد قيمة x حيث أن :-

$x = 1 \bmod 2$

$x = 1 \bmod 3$

$x = 4 \bmod 25$

ومن ذلك يكون:-

$x = 79 \pmod{150}$

ويمكن ان نجعل هذه الخوارزمية غير كفوءة وعديمة الفعالية باختيار منحنى اهليلج ذي عدد نقاط يمتلك على الأقل قاسماً أولياً كبيراً [25] أو إذا كان عدد نقاط المنحنى هو عدداً أولياً بشرط أن لا يساوي مميز الحقل المعرف عليه المنحنى [32].

٣-٤-٢ طريقة بولارد- رو (*Pollard ρ-method*)

لإيجاد قيمة k بحيث أن $Q = k*P$ وكل من Q, P معلومة بهذه الطريقة يتم تجزئة نقاط المنحنى إلى ثلاث مجموعات متساوية تقريبا هي S_1, S_2, S_3 بالاعتماد على قواعد بسيطة وتعرف دالة تكرارية على النقطة Z وكما يأتي:-

$$f(Z) = \begin{cases} 2Z & \text{if } Z \in S_1 \\ Z + P & \text{if } Z \in S_2 \\ Z + Q & \text{if } Z \in S_3 \end{cases}$$

واختيار A_0, B_0 ضمن الفترة [1,n-1] (حيث n رتبة النقطة P) عشوائيا وحساب متتابعة النقاط :-

$$Z_0 = A_0P + B_0Q$$
$$Z_1 = f(Z_0), \quad Z_2 = f(Z_1), \ldots..$$

وبتتبع قيم A_i , B_i بحيث أن:- $Z_i = A_i P + B_i Q$ يكون:-

$$(Z_{i+1}, A_{i+1}, B_{i+1}) = \begin{cases} (2Z_i, 2A_i, 2B_i) & \text{if } Z \in S_1 \\ (Z_i + P, A_i + 1, B_i) & \text{if } Z \in S_2 \\ (Z_i + Q, A_i, B_i + 1) & \text{if } Z \in S_3 \end{cases}$$

حيث أن كل من A_i, B_i يمكن حسابها للمعيار n (mod n) وذلك حتى لا تتزايد إلى حد بعيد ، ولما كان عدد نقاط المنحنى مجموعة منتهية لذلك فإنها سوف تعيد ، نفسها وعندما نحصل على $Z_i = Z_j$ يكون:-

$$A_iP + B_iQ = A_jP + B_jQ$$

ومن هذه المعادلة نحصل على:-

$$k = \frac{A_i - A_j}{B_i - B_j} \pmod{n}$$

مالم يكن $B_i \equiv B_j$ وهذا هو أسوأ الاحتمالات.

وبازدياد عدد نقاط المنحنى يكون استخدام مثل هذه الخوارزمية غير عملي ، لذلك تم اقتراح بعض التغيرات عليها لتكون ذات كفاءة اكبر ومن هذه التعديلات هو تقسيم نقاط المنحنى إلى 20 مجموعة متساوية تقريبا $S_1, S_2, \ldots, S_{20}$ واستخدام دالة تكرارية هي:-

$$f(Z) = \begin{cases} Z + C_1P + D_1Q \\ Z + C_2P + D_2Q \\ . \\ . \\ Z + C_{20}P + D_{20}Q \end{cases}$$

حيث يمكن اختزال C_i , D_i للمعيار n للسيطرة على تزايد قيم هذه المتغيرات ، وتستخدم الفكرة نفسها في حساب اللوغاريتم [51] ، وعدد التكرارات المطلوب لإيجاد اللوغاريتم بهذه الطريقة هو $\sqrt{\frac{\pi n}{2}}$ ،هناك معالجات ومحاولات أخرى كان الهدف منها تقليل عدد التكرارات إلى اقل حد ممكن وذلك باستغلال عملية أيجاد النظير الجمعي لكل نقطة ، والتي تعتبر طريقة سهلة جدا، [51].

٣-٤-٣ طريقة اختزال F_R (*F_R- reduction*)

تعتمد فكرة هذه الطريقة على اغمار الزمرة الجزئية $\langle G \rangle \subset E(F_q)$ في الزمرة الضربية F_{q^k} حيث F_{q^k} هو توسيع للحقل F_q ، واختزال (*ECDLP*) في $\langle G \rangle$ إلى (*DLP*) الاعتيادي في $\left(F^*_{q^k}\right)$ باستخدام اقتران وايل (*Weil's Pairing*) [46] والذي هو أساسا تماثل (*Isomorphism*) بين الزمرة $\langle G \rangle$ والزمرة F_{q^k} .

ويطبق هجوم (*FR-reduction*) على المنحنيات التي يكون فيها دالة الأثر (*trace*) تساوي 2 أو بعبارة أخرى المنحنيات المعرفة على F_p وعدد نقاطها يساوي (p-1) بالإضافة إلى أنها تطبق عندما يكون المنحنى مفرداً مفرطاً (*Supersingular*).

وسنناقش عمل هذه الطريقة مع المنحنيات ذات رتبة n حيث n تقسم (q^k-1) و q هو مميز الحقل المعرف عليه المنحنى [24].

وفيما يأتي ملخص للحالات التي يطبق فيها (*FR-reduction*):-

مبرهنة (٣-١) :-

(ECDLP) في المنحنى $E(F_q)$ يختزل إلى (*DLP*) في الزمرة $F^*_{q^3}$ باستخدام (*Fr-reduction*) إذا وفقط إذا تحقق احد الشرطين:-

١. (q,t) يمكن تمثيلها بالاتي:-

$q = 12L^2 - 1$ and $t = -1 \pm 6L$; $L \in Z$

٢. (q,t) يمكن تمثيلها بالشكل :-

$q = p^r$; r is even and $t = \pm\sqrt{q}$

أي أن المنحنى مفرد مفرط (*Supersingular*).

مبرهنة (٣-٢) [24] :-

(*ECDLP*) في المنحنى $E(F_q)$ يختزل إلى (*DLP*) في الزمرة $F^*_{q^4}$ باستخدام طريقة (*Fr-reduction*) إذا وفقط إذا تحقق احد الشروط :-

١. يمكن تمثيل (q,t) بالشكل :-

$q = t^2 + t + 1$ and $t = -L$ or $t = L + 1$; $L \in Z$.

٢. يمكن تمثيل (q,t) بالشكل :-

$q = 2^r$; r is odd and $t = \pm\sqrt{2q}$

أو بعبارة أخرى المنحنيات المفردة الفائقة (*Supersingular Curves*).

مبرهنة (٣-٣) [24] :-

(*ECDLP*) في الزمرة $E(F_q)$ يمكن أن يختزل إلى (*DLP*) في الزمرة $F^*_{q^6}$ باستخدام طريقة (*Fr-reduction*) إذا وفقط إذا تحقق أحد الشروط:-

١- يمكن تمثيل (q,t) بالشكل:-

$q = 4t^2 + 1$ and $t = 1 \pm 2L$; $L \in Z$.

٢- يمكن تمثيل (q,t) بالشكل:-

$q = 3^r$; r is odd and $t = \pm\sqrt{3q}$

أو بعبارة أخرى المنحنيات المفردة المفرطة (*Supersingular Curves*).

ومن الجدير بالذكر انه لم يتم لحد ألان أيجاد منحنٍ غير المنحنيات المفردة المفرطة أو المنحنيات التي فيها دالة الأثر للمنحنى (*trace of curve*) تساوي 2 يمكن اختزاله بهذه الطريقة على حقل موسع درجة توسيعه اقل من 6. وهناك شروط وخواص اكثر يمكن مراجعتها في [24].

مبرهنة (٣-٤) :-

إذا كان $t \geq 3$ فان درجة التوسيع k تحقق:

$$k \geq \frac{\log q}{\log(t-1)} - \varepsilon$$

حيث E عدد حقيقي يقع ضمن الفترة $0 < t < 1/10$ [24].

٣-٤-٤ طريقة مهاجمة منسيز- اوكاموتو- فنستون (*MOV*)

في هذه الطريقة يبين كل من منسيز (*Menzes*) و اوكاموتو (*Okamoto*) و فنستون (*Vanstone*) كيفية تحويل اللوغاريتم في المنحنيات الاهليلجية (*ECDLP*) إلى اللوغاريتم الاعتيادي (*DLP*) في زمرة أخرى، وهذه الطريقة تطبق في حالة المنحنيات المفردة المفرطة (*Supersingular Elliptic Curves*) بإيجاد تماثل زمري (*group isomerphism*) بين زمرتين باستخدام مبرهنة ويل (*Weil's Theorem*) حيث إذا كان E منحنٍ اهليلجياً فان:-

$e_n: E[n] \times E[n] \rightarrow F^*_q$

حيث ان E[n] هي زمرة جزئية ذات التواء n ولتطبيق اختزال (*MOV*) يجب ان تتحقق الخواص الآتية :-

١. ثنائي الخطية (*Bilinearity*) :-

لكل P_1 , P_2 , P_3 في زمرة الالتواء E[n] يتحقق الآتي:

$$e_n (P_1+ P_2 , P_3) = e_n (P_1, P_3)\, e(P_2, P_3)$$
$$e_n (P_1, P_2 + P_3) = e_n (P_1, P_2)\, e(P_1, P_3)$$

٢. التبادل (*Alternation*) :-

لكل P_1, P_2 في زمرة الالتواء E[n] (*torsion group*) :-

$$e_n (P_1, P_2) = e_n (P_2, P_1)^{-1}$$

٣. (*Nondegeracy*) :-

إذا كان $e_n (P_1, P_2)=1$ لجميع قيم $P_2 \in E[n]$ فان $P_1 = O_E$.

٤. تناغم كالوا (*Galois Compatibility*) :-

إذا كان $E[n] \subset E(F^*_q)$ فان $e_n (P_1, P_2) \in F^*_q$ لكل P_1, P_2 في زمرة الالتواء E[n] [5].

ومن تعريف المنحنيات المفردة المفرطة وعندما يكون $t \equiv 0 \pmod q$ يمكن أن نحصل منه على $t^2 = 0,q,2q,3q,4q$. [56] وبذلك يمكن ان نحدد اقل قيمة لـ k (حيث k درجة توسيع الحقل) بالقيم 2,3,4,6,1 على الترتيب [5].

وكذلك فان المبرهنات في البند (٣-٤-٣) كلها تطبق في هذه الطريقة.

٣-٤-٥ طريقة الهجوم (*SSSA*)

في طريقة قدمها (*Semav*) وكل من (*Smart*) و (*Araki*) و (*Satoh*) والتي تتكون من جزءين الأول يستغل طرائق الهندسة الجبرية و الثاني يتضمن طريقة في نظرية الأعداد والخوارزمية بجزءيها تعمل على إيجاد تماثل (*Isomorphism*) بين نقاط المنحنى $E(F_p)$ الذي يكون من المنحنيات الشاذة (*anomalous*) وزمرة الجمع F_p. حيث استغل (*Semav*) طرق الهندسة الجبرية (*Algebraic geometry*) لتوسيع المنحنى الاهليلجي إلى منحنيات ذات مؤشر (*genus*) اكبر من ١ (حيث أن المنحنيات الاهليلجية هي منحنيات ذات مؤشر يساوي ١) , [9] واستغل كل من (*Smart, Satoh & Araki*) معادلة فيرما (*Fermat equation*) وتوسيعها بتطبيقها في المنحنيات الاهليلجية، ويمكن وصف عمل هذه الخوارزمية بالآتي :-

ليكن $\tilde{\tilde{E}}$ ***منحنٍ اهليلجياً شاذاً (anomalous Elliptic Curve) معرفاً على الحقل*** F_P ***وليكن*** E ***مرفوع*** $\tilde{E}$ ***إلى الحقل ذي المميز 0 أي أن:-***

$$\tilde{\tilde{E}}(F_p): y^2 = x^3 + \tilde{\tilde{a}}_4 x + \tilde{\tilde{a}}_6 \qquad ;\tilde{\tilde{a}}_4, \tilde{\tilde{a}}_6 \in F_p$$

$$E(Q_p): y^2 = x^3 + a_4 x + a_6 \qquad ;a_4, a_6 \in Q_p \, where \;\; char.Q_p = 0$$

وتعرف عملية رفع المنحنى:-

$U: \tilde{\tilde{E}}\ (F_p) \rightarrow E\ (Q_p)$

حيث أن اللوغاريتم في $E\ (Q_p)$ ***يسمى اللوغاريتم الأساس (Formal logarithm) [46] ولكن*** $(\log_E)$ ***يقترب من*** O_E ***بجوار حقيقي*** N ***وبشذوذ المنحنى*** $\tilde{\tilde{E}}$ ***يعرف التطبيق:-***

$$\lambda_E : \tilde{\tilde{E}}(F_p \xrightarrow{u} E(Q_p) \xrightarrow{xp} N \xrightarrow{\log_E} pZ_p \xrightarrow{\bmod p} pZ / p^2 Zp \cong F_p$$

و λ_E ***هو تشاكل زمري (group Homomorphism) ولا تعتمد على كيفية اختيار التطبيق*** U ***ولكن تعتمد على*** E ***وعندما يكون*** $p > 7$ ***يجب أن يحسب كل شيء في*** (Z/p^2Z) ***[5].***

فإذا كان λ_E ***هو تطبيق غير صفري فيجب أن يكون تماثلاً وبذلك يمكن حل اللوغاريتم المنفصل في*** $\tilde{\tilde{E}}(F_p)$ ***، وفي غير ذلك فإننا نبحث عن مرفوع أخر للمنحنى*** $\tilde{\tilde{E}}$ ***وليكن*** E ***باستخدام الحدود في*** E ***بحيث يكون*** $\lambda_{E'}$ ***تماثلاً (Isomorphism).***

كما توجد طرائق أخرى غير التي تم ذكرها لحل (*ECDLP*) عن طريق تحويل المسالة من المنحنيات الاهليلجية (*Elliptic Curve*) إلى (*Hyperelliptic Curve*) وهي منحنيات ذات مؤشر (*genus*) اكبر من 1 ومن ثم تطبيق طرائق تحليل الدليل (*Index Calculus Methods*) عليها [33]. وكذلك هناك طريقة تستخدم بكثرة في الحقول الثنائية لاختزال الحقل المعرف عليه المنحنى باستخدام منحنى الحقل الجزئي (*Subfield Curve*) [51].

٣-٤-٦ هجوم القناة الجانبية

تعرف هذه الطريقة باسم (*Non-Differential Side-Channel Attack*) وهي عدة أنواع لا تتعلق بالبناء الرياضياتي للنظام ولكن تعتمد على الأجهزة المستخدمة في تنفيذه سواء كانت طريقة الحساب أم قناة الاتصال. هذه الأنواع تتمثل في مفاهيم بسيطة ولكن يصعب الحماية منها بدون خسائر [12].

ولتوفير فهم اكثر لهذه الطرائق ، نأخذ عملية ضرب النقطة بعدد صحيح k (*Scalar multiplication*) فعند تمثيل k بالنظام الثنائي تكون الصيغة العامة لخوارزمية الضرب كالآتي:-

1. $O := O_E$
2 . For i from n-1 down to 0 do
   $Q = 2Q$
   IF $k_i = 1$ then
   $Q_i = Q + P$
3. Return Q

حيث ان $k = (k_{n-1}, \dots, k_1, k_0)$

فان المهاجم يحاول حساب عدد بتات (*bits*) بملاحظة عدد المرات التي يمر بها البرنامج في فرع IF. ثم يحسب عدد المرات التي نفذت عملية المضاعفة أو بعبارة أخرى حساب عدد البتات الكلي لـ k. ولمقاومة هذه الطريقة يقترح إضافة متتابعة (*Code*) وهمية لكي توازن الفرق بين الجمع والمضاعفة [12].

٣-٤-٧ استخدام الكومبيوتر الكمي لمهاجمة أنظمة تشفير المنحنيات الاهليلجية

يمكن حل (*ECDLP*) باستخدام الحسابات الكمية أو بعبارة أخرى باستخدام الكومبيوتر الكمي [10] حيث انه بالإمكان حساب تحويل فورير المنتهي في حالة (*State*) ذات n من البتات الكمية (*n-qubit*) باستخدام هذا النوع من الحاسوب بـ $O(n^2)$ من الخطوات وبعبارة أخرى يكون النظام في الحالة:-

$$\sum_{x=0}^{2^n-1} f(x)|x\rangle$$

هناك خوارزمية لتحويل ذلك إلى الحالة:-

$$\sum_{\xi=0}^{2^n-1} \hat{f}(\xi)|\xi\rangle = \sum_{\xi=0}^{2^n-1} \left(\sum_{\xi=0}^{2^n-1} f(x) e^{2\pi i x\xi/2^n} \right) |\xi\rangle$$

حيث يمكن استخدام عدة مسجلات (*registers*) منفصلة لحساب تحويل فورير بأبعاد متعددة، ولما كان بالإمكان جعل تحويل فورير يعمل في حالة الضرب الديكارتي لزمرة دوارة (*Product of cyclic group*)، لذلك فانه يعمل على زمرة نقاط المنحنى الاهليلجي، لكن معرفة المولدات (*generators*) للزمر الدوارة ضمن نقاط المنحنى الاهليلجي تكون اصعب من حل (*ECDLP*) لذلك تقترح استخدام التشاكل (*Homomorphism*) لتحويلها إلى مسالة جديدة في زمرة أخرى يمكن التعامل معها [45].

كذلك توجد طريقة مهاجمة تعتمد على الحسابات الكمية باستخدام خوارزمية شور (*Shor's Algorithm*) المطورة على المنحنيات الاهليلجية [10].

٣-٥ طرائق اختيار منحنى مناسب للتشفير

عند تصميم أنظمة تشفير المنحنيات الاهليلجية (*ECC*) هناك ثلاثة أمور أساسية يجب أخذها بنظر الاعتبار هي:-

٣-٥-١ اختيار حقل منته

اغلب أنظمة تشفير المنحنيات الاهليلجية لمختلف الأغراض تم تصميمها على الحقول الثنائية (F_2^m) (*binary fields*) أو على الحقول الأولية (*prime fields*) حيث أن (*ECDLP*) تكون متساوية الصعوبة في هذين النوعين من الحقول عندما يكون حجمهما متساوياً تقريبا ولا يوجد أي اكتشاف رياضياتي لحد الآن يقترح بان (*ECDLP*) على الحقول الثنائية يكون اصعب أو أسهل منها في الحقول الأولية [54]. ولاختيار حجم الحقل أهمية كبيرة جدا حيث يجب أن يكون على الأقل ضعف طول حجم المفتاح ليكون الوقت اللازم لأجراء بحث شامل عن المفتاح مساو للوقت اللازم لحل (*CEDLP*) تقريبا باستخدام طريقة بولا رد- رو (*Pollard ρ-method*) المطورة على الأقل [18].

كذلك هناك بعض من المصممين يفضل اختيار الحقول الثنائية لكونها الأسهل في المعالجات على المكونات المادية (*Hardware*) [11]، و آخر يفضل استخدام الحقول الأولية في التطبيقات التي تكون فيها المعالجات ذاتية مثل البطاقات الذكية (*Smart Cards*) [38]، كما و ظهرت بعض المحاولات لتسريع أجراء عمليات الحسابية في الحقول الأولية الموسعة (F_p^m) بالاعتماد على متتابعات جمع خاصة ولكنها لم تتجاوز حجم حقل مكون من (160 *bits*) [50].

٣-٥-٢ اختيار تمثيل عناصر الحقل

إذا كان الحقل الذي تم اختياره هو الحقل الثنائي (*Binary field*) فان هناك عدة طرائق يمكن أن تمثل بها عناصر هذا الحقل أكثرها كفاءة طريقة (*Optimal Normal Basis*) و (*Polynomial Basis*) ولان عناصر الحقل في أي تمثيل بإحدى هاتين الطريقتين يمكن بسهولة تحويله إلى الطريقة الأخرى باختيار مصفوفة أساس مناسبة (*Basis Matrix*)، لذلك فان صعوبة (*ECDLP*) لا تميل إلى أي من هذين التمثيلين [54].

٣-٥-٣ اختيار المنحنى المناسب في حقل محدد

لوجود بعض الطرائق الكفوءة لمهاجمة أنواع معينة من أنظمة التشفير يجب على المصمم ان يراعي عدة جوانب في اختيار المنحنى المناسب لكي تكون الأنظمة حصينة ضد تلك الطرائق ومن أهم النقاط التي يجب مراعاتها:-

١. أن تكون رتبة المنحنى (عدد نقاطه) عدداً أولياً أو قابلاً للقسمة على عدد أولي كبير نسبيا.
٢. أن يكون المنحنى محصناً ضد طرائق الهجوم المعروفة [49].

وسوف نتعرف على كيفية اختيار هذه المنحنيات بعد التعريف الآتي:

تعريف (٣-٢) :

ليكن E منحنٍ اهليلجياً ذا مميز D (*Discriminant*) فيقال أن E يحقق شرط الاختزال الجيد (*Good Reduction*) على الحقل F_p إذا كان $D \equiv 0 \pmod p$ وكذلك لا يكون كل من a،b يساوي صفراً في الحقل F_p [28].

آ- اختيار منحنى بصورة عشوائية

يتم اختيار أي منحنى بصورة عشوائية بحيث يحقق شرط الاختزال الجيد ومن ثم حساب عدد نقاط هذا المنحنى باستخدام إحدى الطرائق في (٢-٣-٦) فإذا كان عدد النقاط يحقق الشرطين أعلاه يتحقق المطلوب وان لم يكن نستمر في الاختيار العشوائي وحساب عدد النقاط حتى يتم الحصول على المنحنى المطلوب [21]. كما توجد طريقة أخرى يمكن إيجازها بالآتي :

يتم اختيار ثلاثة عناصر من الحقل المعرف عليه المنحنى بصورة عشوائية ولتكن a,y,x ثم تعوض هذه القيم لحساب قيمة b حيث يكون:-

$$b = y^2 - (x^3 + ax)$$

ثم حساب المميز لهذه المعادلة (Discriminate) والذي يجب إن لا يساوي صفرا، أما إذا لم يتحقق ذلك فيتم الرجوع إلى البداية في غير ذلك فان النقطة (x,y) تقع على المنحنى [44].

$$. y^2 = x^3 + ax + b$$

ومن الطرائق العشوائية أيضا يمكن ان نختار عدداً معيناً N ويتم البحث عن منحنى يحقق عدد نقاطه هذا العدد.

ب- إنشاء منحنى اهليلجي باستخدام الضرب العقدي

لإنشاء منحنى اهليلجي بعدد نقاط معلوم على حقل منتهٍ معطى يتم استخدام الضرب العقدي (*Complex Multiplication*) والذي إحدى خطواته حساب متعددات حدود في فضاء هلبرت $H_D(x)$ لمعيار عدد صحيح p حيث D هو الجذر التربيعي لمتعددة حدود فروبينيس:-

$$x^2 - tx + p = 0$$

والذي غالبا ما يكون عدداً مركباً (*Complex Number*)، ومنه جاءت التسمية [41].

ولبناء منحنى اهليلجي E بعدد نقاط N علينا إجراء الخطوات آلاتية:-

١. إيجاد عدد صحيح t بحيث يحقق $N = 1 + p - t$.

٢. إيجاد $\pi, \bar{\pi}$ جذور المعادلة $x^2 - tx + p = 0$.

٣. ليكن D هو المميز (*Discriminate*) للحقل $Q[\sqrt{t^2 - 4q}]$ بعدها يتم ايجاد قيمة j (ثابت المنحنى) [41].

٤. ليكن E^+ المنحنى الاهليلجي المعرف بالمعادلة:-

$$Y^2 = X^3 + 3c^2 j/(1728 - j)X + 2c^3 j/(1728 - j)$$

حيث أن c هو باقي تربيعي (*Quadratic Residue*) في الحقل F_p .

وليكن E^- المنحنى الاهليلجي المعرف بالمعادلة

$$Y^2 = X^3 + 3c^2 j/(1728 - j)X + 2c^3 j/(1728 - j)$$

حيث أن c هو باقي غير تربيعي (*Quadratic non Residue*) في الحقل F_p .

٥. أما $E^+(F_p)$ أو $E^-(F_p)$ سوف يمتلك رتبة N [20].

جـ- اختيار منحنى بعدد نقاط أولي باستخدام زمرة الالتواء

هذه الطريقة تعتمد على رتبة زمرة الالتواء الجزئية (*Torsion Subgroup*)، حيث أن رتبتها يجب أن تقسم رتبة المنحنى (مبرهنة (٢-٣)) فيعبر عن العدد η بالأتي:

$$\eta = \frac{\#E(F_p)}{\#E_{tors}}$$

فإذا كان η عدداً أولياً كبيراً نسبيا فيمكن اختيار E منحنى مناسباً للتشفير حيث عندما يكون η عدداً أولياً كبيراً فان هجوم بولارد رو (*Pollard ρ-*) يكون غير فعال في هذه الزمرة

ولكن يجب مراعاة أن لا يكون هذا المنحنى شاذاً (*anomalous curve*) حيث يمكن ان يكون $\#E_{tors} = 1$ و $\eta = p = \#E(F_p)$ [32].

ويمكن حساب زمرة الالتواء بسهولة إذا كانت رتبتها تساوي واحد فعندما يكون كل من p_1 و p_2 عدداً أولياً لا يقسم معاملات E ولا المميز Δ يكون:-

$\#E_1$ و $\#E_2$ أوليان نسبيا (*relative prime*) فان ($\#E_{tors} = 1$) [32].

وباستخدام دالة Z (*Zeta function*) يمكن جعل هذه الطريقة تعمل في الحقول الموسعة F_{p^n} [32].

٤-١ المقدمـة

هناك صلات وثيقة بين علم التشفير (*Cryptology*) والحاسوب والخوارزميات ، حيث ان تحويل النص الواضح من حروف إلى أرقام ومن ثم تشفير هذا النص واستخدام النص المشفر لاسترجاع الأصلي بطرائق يدوية ،حتى وان استغرق ذلك وقتا طويلا فانه ينتج أنظمة تشفير غير مناسبة للاستخدام . حيث يجب أن تكون الأنظمة مصممة على شكل خوارزميات يسهل التعامل معها في الحاسوب وأمينة في الوقت نفسه، وللحاسوب دور كبير في أنظمة المفتاح المعلن من ناحية السرعة والدقة علما ان هذه الأنواع تعتمد على مسائل معقدة (التحليل إلى العوامل الأولية *Integer Factorization* واللوغاريتم المنفصل *Discrete logarithm* واللوغاريتم المنفصل في المنحنيات الاهليلجية *Elliptic Curve Discrete Logarithm Problem*).

يقدم هذا الفصل الجوانب البرمجية والمخططات الانسيابية لنظامي تشفير الجمال ومنسيز – اوكاموتو باستخدام المنحنيات الاهليلجية وكذلك بعض البرامج الساندة مثل حساب عدد نقاط المنحنى وعمليتي جمع ومضاعفة النقاط وبعض خوارزميات ضرب النقطة بعدد صحيح إضافة إلى برامج مساندة أخرى تتعلق بعناصر الحقل المعرف عليه المنحنى باستخدام تطبيق (*MATLAB R12*) على حاسبة (PIII 833 MHZ). كما تقدم بداية هذا الفصل بعض المبرهنات والنتائج التي تم التوصل أليها من خلال الجهد البحثي المبذول في هذا الموضوع والتي نتوقع أن يكون لها دور في تسهيل الحسابات ، ومن ثم استخدام النتائج التي حصلنا عليها في برامج ومقارنة النتائج مع البرامج الأخرى .

٤-٢ المبرهنات المقترحة لاختيار منحنى في الحقل الأولي

عند التعامل مع المنحنيات الاهليلجية (*Elliptic Curves*) المعرفة بالمعادلة (6) أي المنحنيات التي تعرف على الحقل الأولي وبالاعتماد المتغيرات a, b في تعريف منحنى اهليلجي يجب ان تكون المعادلة التكعيبية في الطرف الأيمن غير قابلة للتحليل (*irreducible*) وهذا ما يتحقق عندما يكون مميز المعادلة (*Discriminate*) لا يساوي صفرا أي أن $4a^3 + 27b^2 \neq 0$ (بالاعتماد على قانون الدستور لحل معادلات من الدرجة الثالثة).

مبرهنة (٤-١) :-

عدد المنحنيات الكلي في الحقل F_p هو $p\ (p-1)$

البرهان :-

بأخذ جميع قيم b في الحقل F_p فان $27*b^2$ سيكون أحد عناصر الحقل F_p أيضا، ولكن $4a^3$ هو أحد التباديل (*Permutations*) المعرفة في الحقل F_p، وذلك لانه تطبيق شامل ومتباين (1-1 and anto).

لذلك فان لكل قيمة $b \in F_p$ يوجد عدد وحيد $a \in F_p$ و بحيث يحقق $4a^3 + 27b^2 \equiv 0$ وباستبعاد قيمة $b \equiv 0$ ذلك لان $b^2 \neq 0 \pmod p$ ما لم يكن $b \equiv 0$ لان p عدد أولي.

وبذلك فان المجموع الكلي للقيم التي يمكن ان تكوّن منحنٍ اهليلجياً هي$(p-1)(p-1)$.

لكن عندما يكون $b = 0$ فيوجد $(p-1)$ من المنحنيات التي يكون فيها المميز $4a^3 \neq 0 \bmod p$ حيث $a \neq 0$ أيضا.وبذلك فان مجموع هذه المنحنيات هو

$$(p-1)(p-1) + (p-1) = (p-1)\ ((p-1) + 1)$$
$$= (p-1)p = p(p-1)$$

وبالسياق نفسه سنأخذ النتيجة الآتية بدون برهان:-

نتيجة (٤-١) :-

العدد الكلي للمنحنيات المفردة المفرطة (*Supersingular*) في الحقل F_p يكون احد مضاعفات $(p-1)$.

والجدول (٤-١) يوضح عدد المنحنيات في بعض الحقول العددية، ونلاحظ منه إن عدد المنحنيات المفردة المفرطة متباينة في الحقول العددية ولكنها تبقى من مضاعفات $(p-1)$ في كل الأحوال، علما إننا لم نتمكن من التوصل إلى القاعدة نفسها أو قاعدة مشابهة فيما يخص المنحنيات الشاذة (*anomalous curves*) ،كما ويمكن التعرف على بعض المنحنيات، فيما اذا كانت مفردة مفرطة (*supersingular*) أم لا وحسب الحالات المعطاة بالمبرهنة (٤-٢).

جدول (٤-١) عدد المنحنيات الكلي وعدد المنحنيات المفردة المفرطة في بعض الحقول العددية

مميز الحقل (F_p)	عدد المنحنيات الكلي $p(p-1)$	عدد المنحنيات المفردة المفرطة (*supersingular*)	(عدد المنحنيات المفردة المفرطة) / (p-1)
23	342	66	3
67	429	132	2
89	7832	528	6
101	10100	700	7
131	17030	1300	10
163	26406	324	2
167	27722	1826	11
181	32580	900	5
193	37056	384	2
227	51302	2260	10
239	56882	3570	15
251	62750	3500	14
277	76452	828	3
311	96410	5890	19
317	100172	1580	5
337	113232	1344	4

مبرهنة (٤-٢) :-

ليكن E المنحنى الاهليلجي المعرف على الحقل F_p بالمعادلة :-

$$E(F_p): y^2 = x^3 + ax + b$$

فيمكن تمييز بعض المنحنيات المفردة المفرطة وكآلاتي:-

١. إذا كان $p \equiv 1 \pmod{12}$ فان كل المنحنيات المفردة المفرطة يكون فيها $a \neq 0$ و $b \neq 0$ ، أو بعبارة أخرى كل المنحنيات التي فيها $a=0$ أو $b=0$ تكون من النوع المفرد المفرط (*supersingular*) .

٢. إذا كان $p \equiv 5 \pmod{12}$ فان:-

كل المنحنيات التي فيها $a = 0$ تكون مفردة مفرطة (*supersingular*)، أو بعبارة أخرى كل المنحنيات التي فيها $b = 0$ لاتكون منحنيات مفردة مفرطة (*non supersingular*).

٣. إذا كان $p \equiv 7 \pmod{12}$ فان:-

كل المنحنيات التي فيها $b = 0$ تكون مفردة مفرطة (*Supersingular*) وبعبارة أخرى كل المنحنيات التي فيها $a = 0$ لاتكون منحنيات مفردة مفرطة (*non supersingular*).

٤. إذا كان $p \equiv 11 \pmod{12}$ فان كل المنحنيات التي يكون فيها $a = 0$ أو $b = 0$ تكون منحنيات مفردة مفرطة (*Supersingular*).

والمبرهنة أعلاه تمكننا من التعرف على عدد نقاط بعض المنحنيات بدون الحاجة إلى حسابها.

مبرهنة (٤-٣):-

إذا كان E_1 منحنى معرف على الحقل F_p بالمعادلة:-

$$E_1(F_p): \ y^2 = x^3 + ax + b$$

وكان :

$$E_2(F_p): y^2 = x^3 + ax + b$$

بحيث أن $\# E_1 = p + 1 - t$ فأن:-

١. $\# E_1 = \# E_2$ عندما $p \equiv 1 \pmod{4}$.

٢. $\# E_2 = p + 1 + t$ إذا كان $p \equiv 3 \pmod{4}$.

البرهان :-

بما أن (-1) هو باقي تربيعي في الحقل F_p عندما يكون $p \equiv 1 \pmod{4}$ فان:-

$$y^2 = x^3 + (-1)^2 * ax + (-1)^3 b$$
$$y^2 = x^3 + ax - b$$

هو تماثل زمري (*Isomorphism group*) وبذلك تمتلك المنحنيات العدد نفسه من النقاط.

أما في الحقل F_p عندما $p \equiv 3 \pmod{4}$ فان (-1) هو باقي غير تربيعي ومنه نحصل على :-

$\# E_1 + \# E_2 = 2p + 2$ ((مبرهنة (٢-٣١))

$\rightarrow p + 1 - t + \# E_2 = 2p + 2$

$\rightarrow \# E_2 = P + 1 + t$.

وقد تم استخدام المبرهنة (٤-٣) في خوارزمية البحث العشوائي عن منحنٍ بعدد نقاط معلوم ، فكان هناك اختزال في الوقت كما يوضحه الجدول (٤-٢).

جدول (٤-٢) مقارنة بين الخوارزمية الاعتيادية وخوارزمية البحث عن منحنيين

p	N	باستخدام الطريقة الاعتيادية		باستخدام طريقة البحث عن منحنيين	
		a,b	الزمن بالثانية	a,b	الزمن بالثانية
11	17	2,4	0.050000000000007	2,4	0.06
11	7	2,7	0.049999999999972	2,7	0.049999999999972
13	11	7,6	0.110000000000001	7,6	0.109999999999999
13	16	0,5	0.050000000000043	0,5	0.050000000000043
17	11	2,6	0.11	2,6	0.050000000000007
17	25	1,8	0.1	1,8	0.050000000000007
19	14	0,10	0	0,10	0.050000000000072
19	21	0,4	0.050000000000007	1,0	0.049000000000072
23	29	1,4	0.060000000000023	1,4	0.060000000000023
23	19	1,19	0.110000000000001	1,19	0.060000000000023
29	37	4,9	0.160000000000004	4,9	0.219999999999999
29	23	1,12	0.049999999999972	1,12	0.109999999999999
31	41	1,3	0.109999999999999	1,3	0.049999999999999
31	33	1,15	0.109999999999999	1,15	0.049999999999999
37	47	3,15	0.219999999	3,15	0.219999999999999
37	28	0,6	0.060000002	0,6	0
41	34	6,15	0.4900000	6,15	0.490000000000002
41	41	3,8	0.220000	3,8	0.27
43	35	1,12	0.11	1,12	0.109999999999999
43	44	1,0	0.19999	1,0	0.599999999999987
47	37	1,43	0.219999999999999	1,43	0.22
47	57	5,1	0.44	5,1	0.5
53	43	1,18	0.219999999999999	1,18	0.159999999999999
53	63	1,11	0.17	1,11	0.159999999999997
59	53	1,46	0.27	1,46	0.27
59	66	1,7	0.160000000000004	1,7	0.159999999999997
61	61	0,2	0	0,2	0
61	63	0,5	0	0,5	0.059999999999952
67	53	2,53	0.490000000000002	2,53	0.490000000000002
67	78	1,10	0.219999999999999	1,10	0.219999999999999
71	73	1,17	0.220000000000006	1,7	0.220000000000001
71	87	1,34	0.33	1,34	0.280000000000001
73	79	3,13	0.66	3,13	0.659999999999997
73	69	1,6	0.219999999999999	1,6	0.219000000000009
79	65	3,20	0.770000000000003	3,20	0.770000000000003
79	95	3,6	0.76	3,6	0.72
83	67	2,55	0.66	2,55	0.66
83	100	1,23	0.329999999999998	1,23	0.329999999999998
89	103	3,18	0.88	3,18	0.940000000000005
89	77	13,4	0.36	13,4	3.74
97	97	1,1	0.39	1,1	0.380000000000003
97	98	1,22	0.439999999999998	1,22	0.390000000000001

٤-٣ خوارزميات الضرب بعدد صحيح

كما لاحظنا في الفصل الثاني البند (٢-٣-٥) وجود عدة خوارزميات لضرب النقاط بعدد صحيح (*scalar multiplication*) .

سنقدم الان برنامجا مقترحا يجمع خوارزميتي الضرب بعدد صحيح باستخدام عمليتي الجمع والمضاعفة وخوارزمية الضرب باستخدام دالة الاتزان، واستخدام حساب نظير النقطة لاختزال العمليات الحسابية ، ويتطلب هذا معرفة عدد نقاط المنحني .

يتم في هذا البرنامج تمثيل العدد k بالحالات المختلفة له ،التمثيل الثنائي ،والتمثيل الثنائي بتطبيق دالة الاتزان ومن ثم إيجاد t = (#E-k) حيث E عدد نقاط المنحنى واخذ التمثيل الثنائي لـ t والتمثيل الثنائي بدالة الاتزان أيضا ، وتعريف ميزان لحساب أي من الحالات الأربع تكون ذات عدد عمليات اقل، ومن ثم اختيارها وتطبيق الدالة المناسبة عليها و إجراء عملية الضرب بعدد صحيح .

وبالنظر لكون عملية ضرب النقطة بعدد صحيح عملية سريعة جداً فقد تم تطبيق برنامج إيجاد كل نقاط منحنٍ ما باستخدام خوارزمية ضرب النقطة بعدد صحيح أي أن، بإدخال P وحساب k*P عن طريق ضرب النقطة بالعدد k واخذ قيم k من 2 إلى عدد نقاط المنحنى، وذلك لتسهيل ملاحظة اختلاف الوقت.

والجدول (٤-٣) يوضح مقارنة بالوقت لخوارزميات الضرب بعدد صحيح بين الخوارزمية الاعتيادية باستخدام عمليتي الجمع والمضاعفة وخوارزمية الجمع والمضاعفة باستخدام دالة الاتزان ، والبرنامج المقترح الذي يجمع الخوارزميات ونظير النقطة.

جدول (٤-٣) خوارزميا ت ضرب النقطة بعدد صحيح

a,b,p	النقطة المولدة	عدد نقاط المنحنى	خوارزمية الجمع والمضاعفة	خوارزمية دالة الاتزان	الخوارزميات ونظير النقطة
12,8,17	(1,2)	15	0.21999999999999	0.05000000000007	0
1,1,23	(0,1)	28	0.5	0.0	0
1,4,23	(0,2)	29	0.55000000000001	0.05000000000007	0
1,13,31	(9,10)	34	0.66666666666664	0.0599999999987	0
49,41,151	(118,122)	150	5.22	0.22000000000002	0.0599999999987
2,1,3023	(1,2)	3054	222.22	2.41	2.17
2,1,3023	(1877,371)	3054	224.2	4.12	3.46

ومن الجدول (٤-٣) نلاحظ ان البرنامج الذي يجمع الخوارزميتين ونظير النقطة يكاد يكون وقت تنفيذه معدوماً، بينما في الحقول العددية المتوسطة F_{151} مثلاً فأن الوقت اللازم يكون مساو إلى 1.15% منه في حالة خوارزمية والمضاعفة وحوالي 27.27% من الوقت اللازم في خوارزمية الاتزان ، أما في الحقول العددية الكبيرة فان الوقت اللازم لتنفيذ البرنامج يكون حوالي 25.5% في خوارزمية الجمع والمضاعفة الاعتيادية وحوالي 90.05% مقارنة بخوارزمية الاتزان .

٤-٤ تصميم المخططات الانسيابية للخوارزميات والعمليات الحسابية في زمرة نقاط المنحنى

يقدم هذا البند المخططات الانسيابية للبرمجيات التي تم بناءها لتنفيذ أنظمة تشفير المنحنيات الاهليلجية وما يتعلق بها من عمليات حسابية باستخدام تطبيق الـ MATLAB R12 [48] وفيما يلي المخططات مرتبة حسب أسبقيات التنفيذ وكالآتي:

آ-**نظام تشفير الجمال باستخدام المنحنيات الاهليلجية** :- يوضح المخطط (٤-١) عمل برنامج للتشفير باستخدام خوارزمية الجمال ، ويشمل بناء مفتاح معلن وتشفير نص واضح واسترجاعه، ويحوي على دوال إغمار الرسالة كنقطة في المنحنى (*embedded plain text*) وخوارزمية الضرب بعدد صحيح *Scalar multiplication*

ب-**نظام تشفير منسيز –فنستون** :- يوضح المخطط (٤-٢) برنامجاً لنظام منسيز–فنستون يشتمل على خوارزميات بناء المفتاح المعلن وتشفير النص واسترجاعه ويحوي دالة الضرب بعدد صحيح ولا يحتاج إلى دالة اغمار .

جـ-**اغمار الرسالة** :-يقدم المخطط (٤-٣) برنامجاً لاغمار الرسالة الواضحة كنقطة في المنحنى المستخدم في التشفير ، ويعد هذا البرنامج مطلبا أساسيا في أنظمة تشفير الجمال وميسي اومورا.

د-**ضرب النقطة بعدد صحيح** :- يقدم المخطط (٤-٤) خوارزمية ضرب النقطة بعدد صحيح باستخدام عمليتي الجمع والمضاعفة .

هـ- **ضرب النقطة بعدد صحيح باستخدام طريقة الاتزان** :-يوضحها المخطط (٤-٥).

و-**إيجاد عدد نقاط منحنى**:- يقدم المخطط(٤-٦) برنامجاً لإيجاد عدد نقاط منحنٍ اهليلجي معرف بالمعادلة (6) باستخدام حساب رمز ليجندر.

ز-**حساب جميع المنحنيات في الحقل F_p:**- يقدم المخطط (٤-٧) برنامجا لحساب كل المنحنيات الاهليلجية في الحقل F_p وترتيبها تصاعديا حسب عدد نقاطها.

حـ-**البحث العشوائي عن منحنى** :- يقدم المخطط (٤-٨) الخوارزمية الاعتيادية للبحث العشوائي عن منحنٍ اهليلجياً بعدد نقاط معلوم.

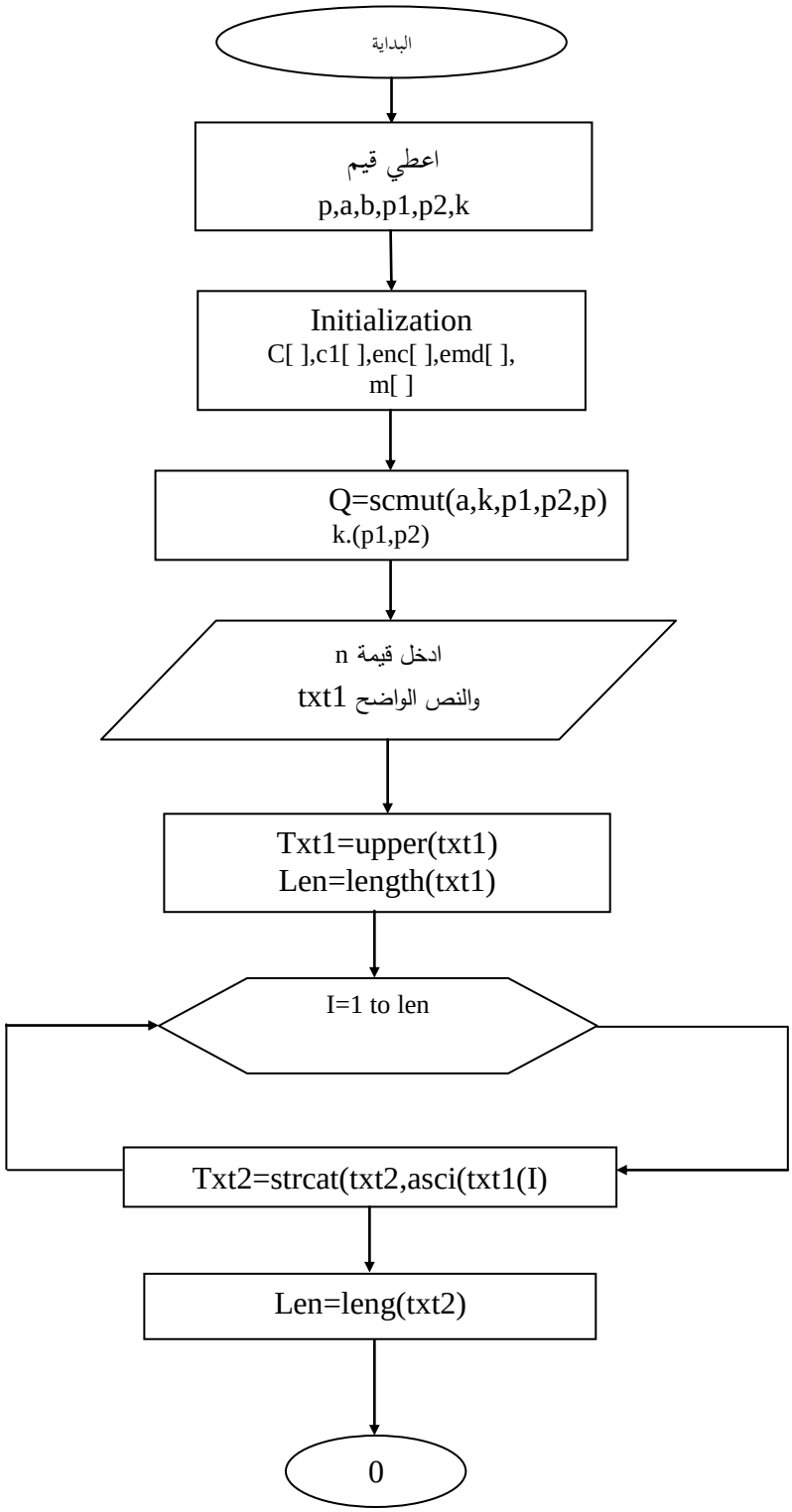
ط-**الخوارزمية المقترحة للبحث:**-يقدم المخطط (٤-٩) الخوارزمية المقترحة للبحث العشوائي عن منحنٍ اهليلجياً بعدد نقاط معلوم باستخدام المبرهنة (٤-٣).

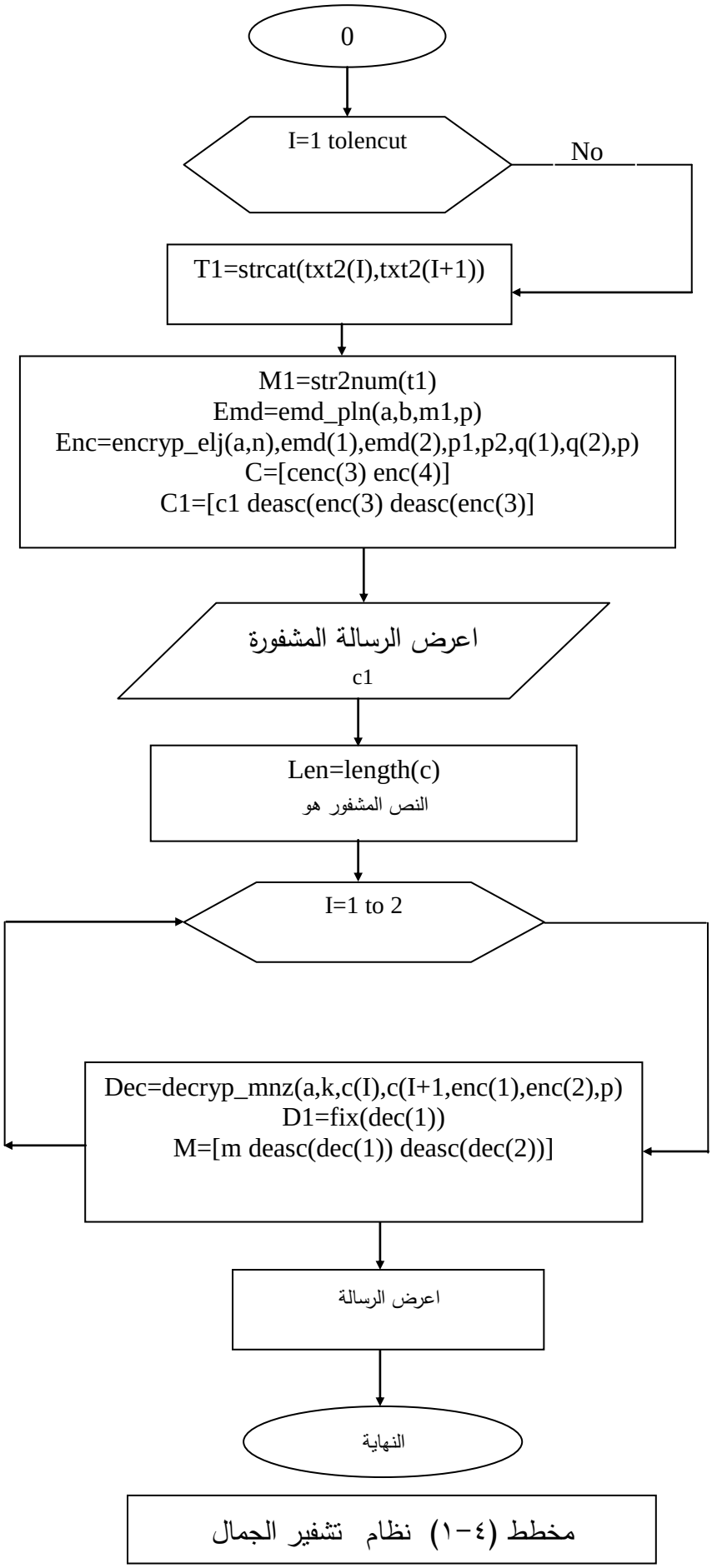
ي-**الخوارزمية المقترحة للضرب:**- يوضح المخطط (٤-١٠) الخوارزمية المقترحة لضرب النقطة بعدد صحيح ، تم فيها جمع كل من الخوارزميتين في (جـ) و (د) أعلاه وإيجاد نظير النقطة ، والتي تم مناقشتها في البند (٤-٣).

ك- **خوارزمية جمع نقطتين** :- يوضح المخطط (٤-١١) خوارزمية جمع نقطتين في منحنى أهليلجي كما يتضمن حالة مضاعفة النقطة أيضاً .

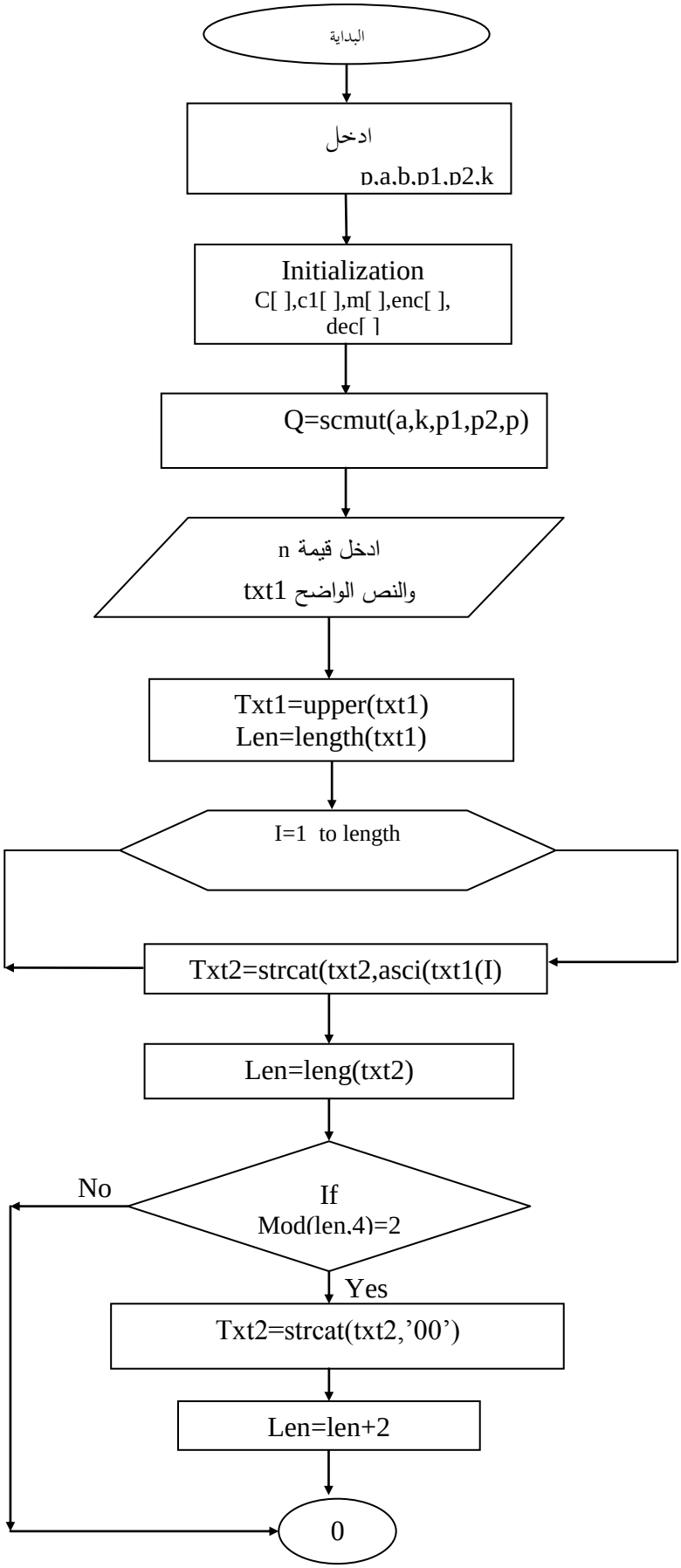
ل- **خوارزمية المضاعفة** :- يبين المخطط (٤-١٢) خوارزمية مضاعفة النقطة في المنحنى الأهليلجي .

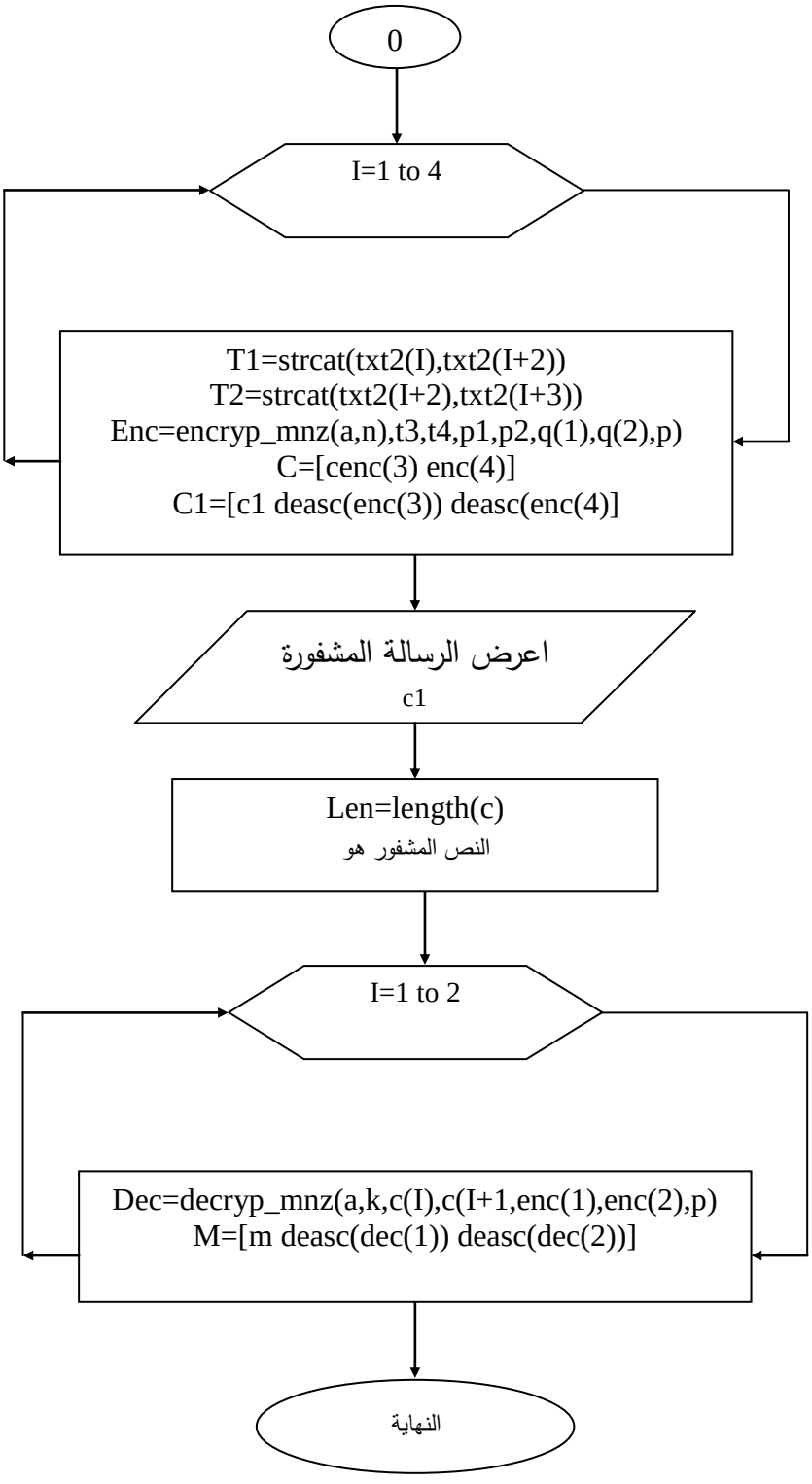
م- **مخططات تمثل برامج ساندة متعلقة بعناصر الحقل المعرف عليه المنحنى:**- حيث يوضح المخطط (٤-١٣) دالة الإتزان للعدد الصحيح ، والمخطط (٤-١٤) يبين عملية إيجاد معكوس عدد صحيح وأخيراً المخطط (٤-١٥) يبين عملية إيجاد الجذر التربيعي لعدد صحيح في حقل منته .


البداية
اعطي قيم
p,a,b,p1,p2,k
Initialization
C[ ],c1[ ],enc[ ],emd[ ],
m[ ]
Q=scmut(a,k,p1,p2,p)
k.(p1,p2)
ادخل قيمة n
والنص الواضح txt1
Txt1=upper(txt1)
Len=length(txt1)
I=1 to len
Txt2=strcat(txt2,asci(txt1(I)
Len=leng(txt2)
0

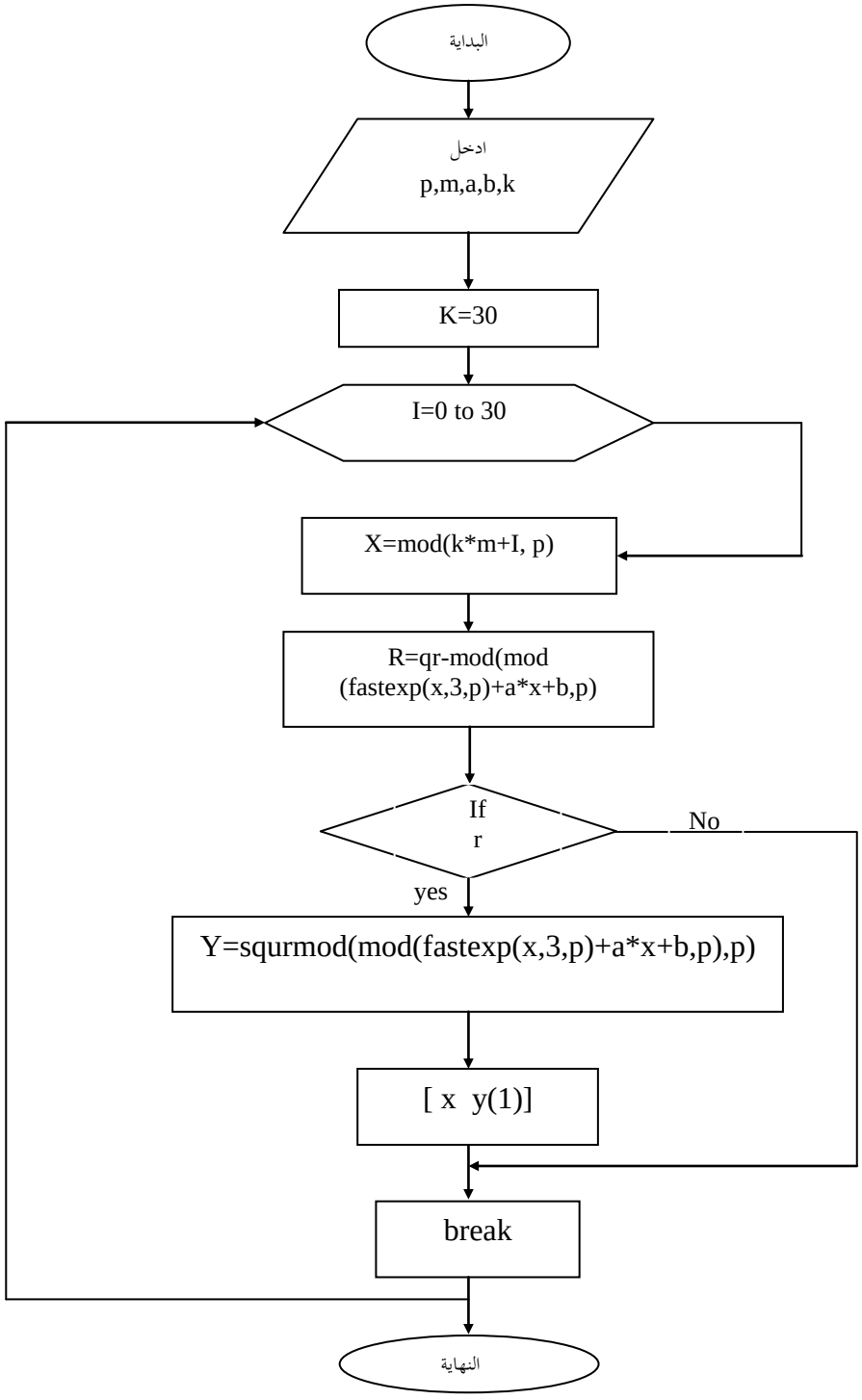


مخطط (٤-١) نظام تشفير الجمال

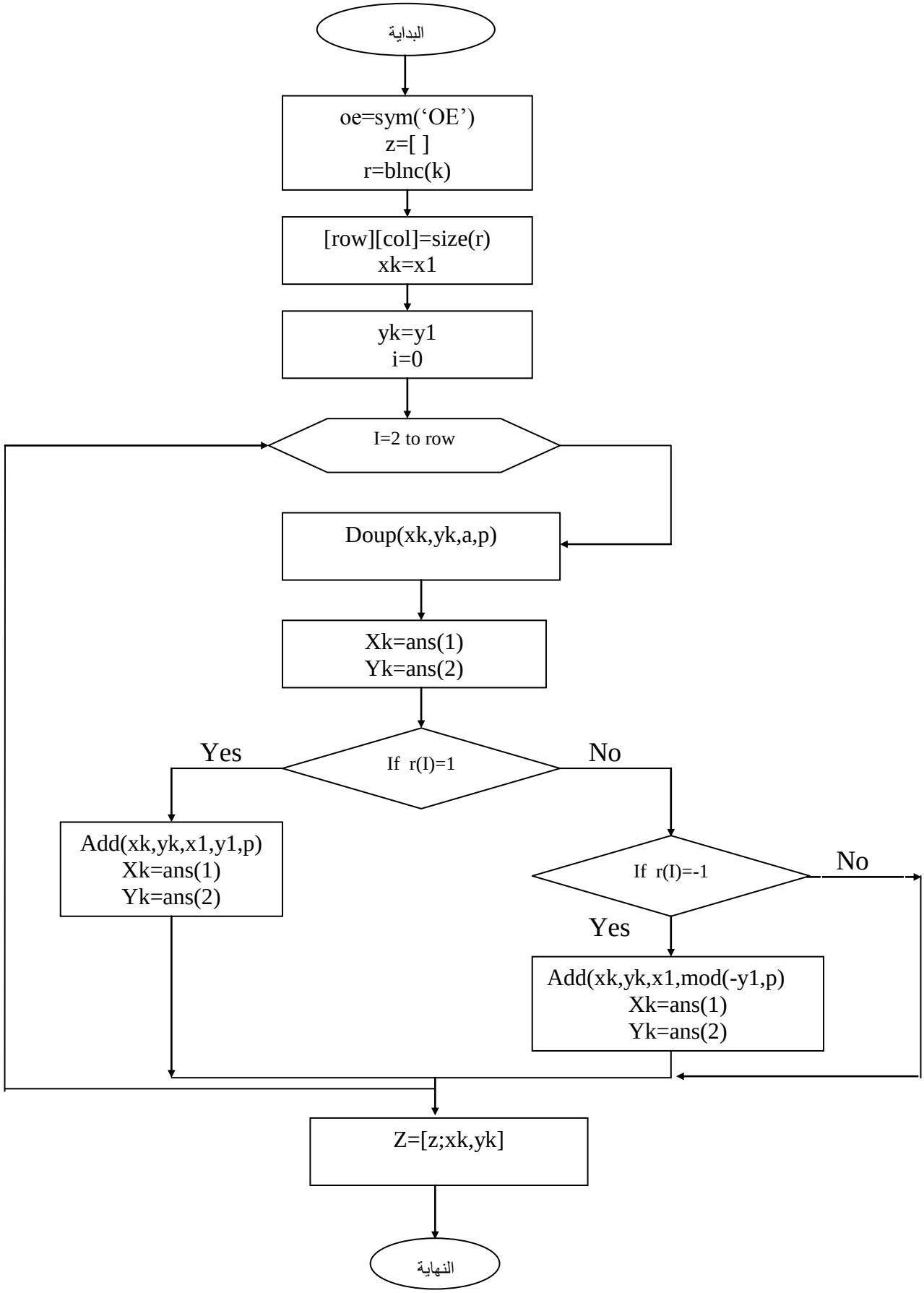

البداية
ادخل
p,a,b,p1,p2,k
Initialization
C[ ],c1[ ],m[ ],enc[ ],
dec[ ]
Q=scmut(a,k,p1,p2,p)
ادخل قيمة n
والنص الواضح txt1
Txt1=upper(txt1)
Len=length(txt1)
I=1 to length
Txt2=strcat(txt2,asci(txt1(I)
Len=leng(txt2)
If
Mod(len,4)=2
No
Yes
Txt2=strcat(txt2,'00')
Len=len+2
0



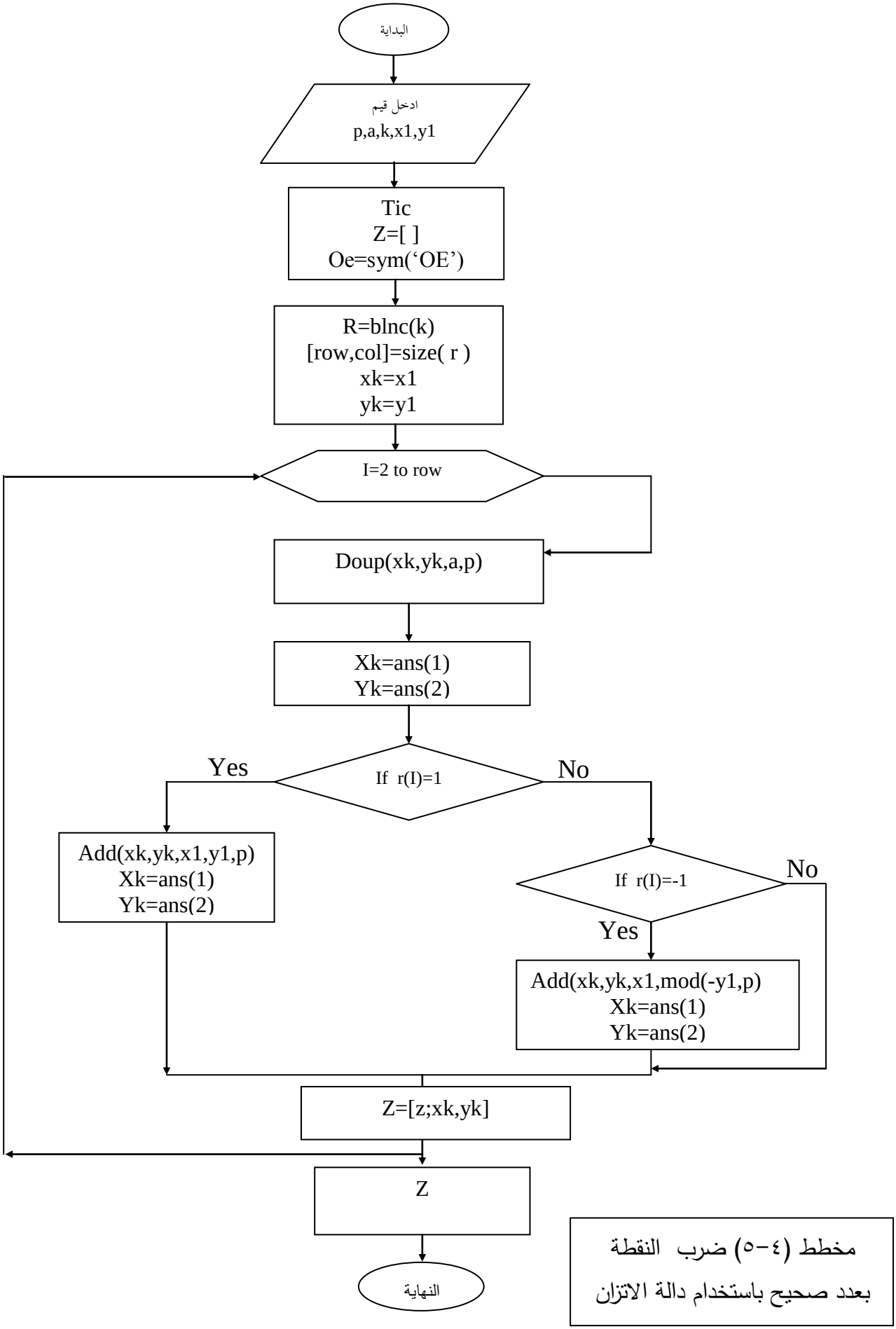
مخطط (٤-٢) نظام منسيز- فنستون



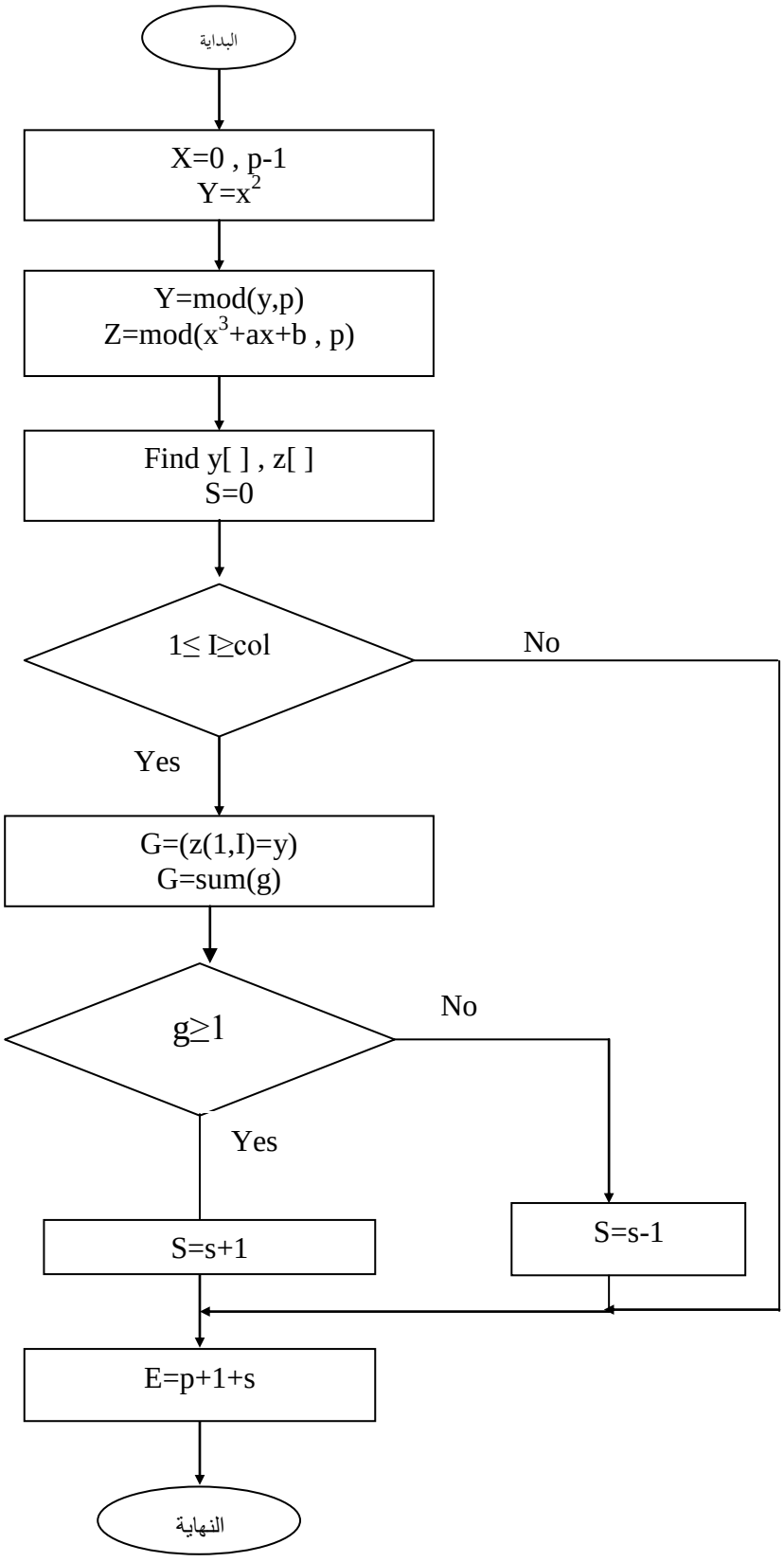
مخطط (٤-٣) اغمار الرسالة الواضحة كنقطة في المنحني



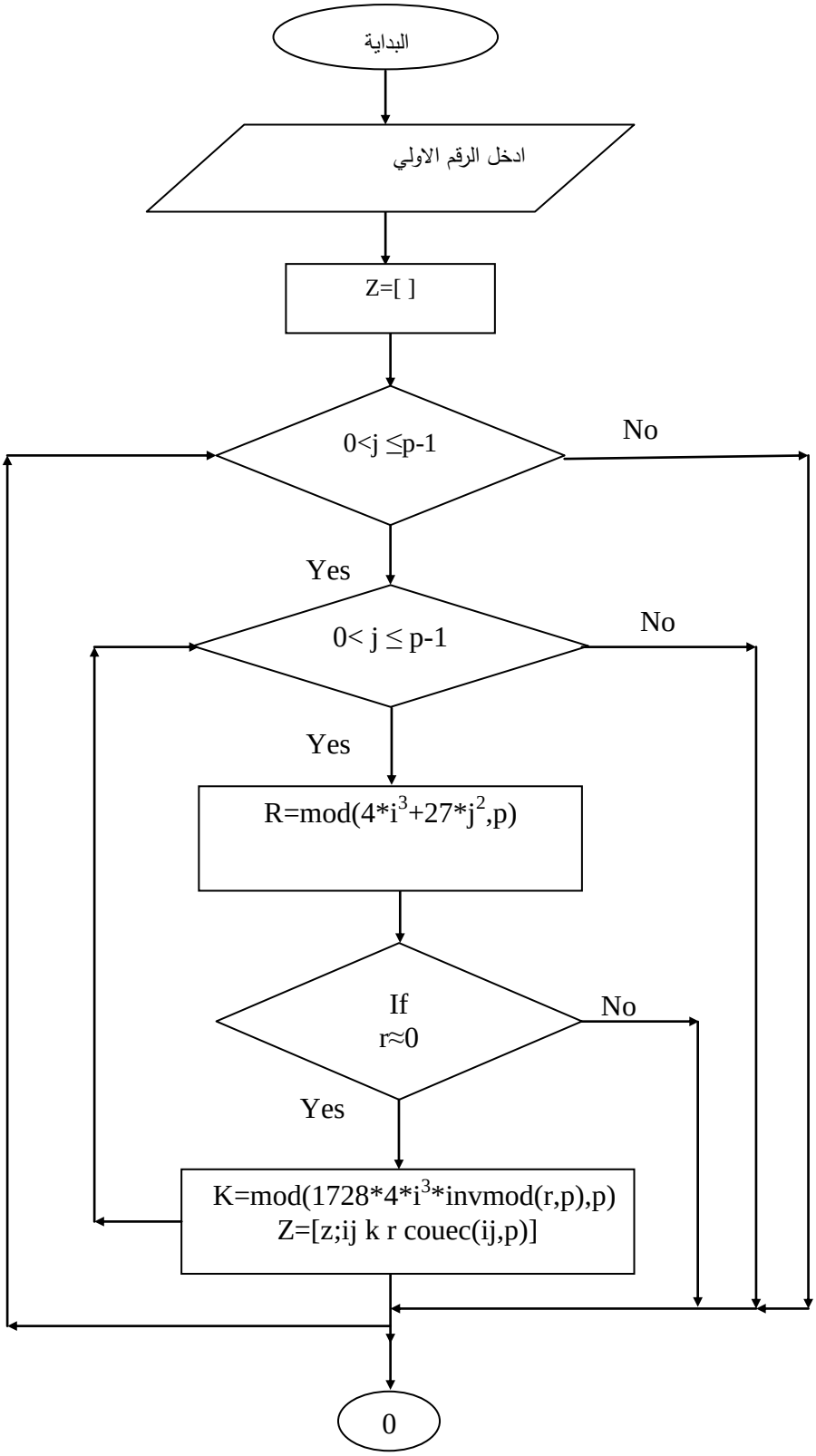
مخطط (٤-٤) خوارزمية ضرب النقطة بعدد صحيح باستخدام دالة الجمع و

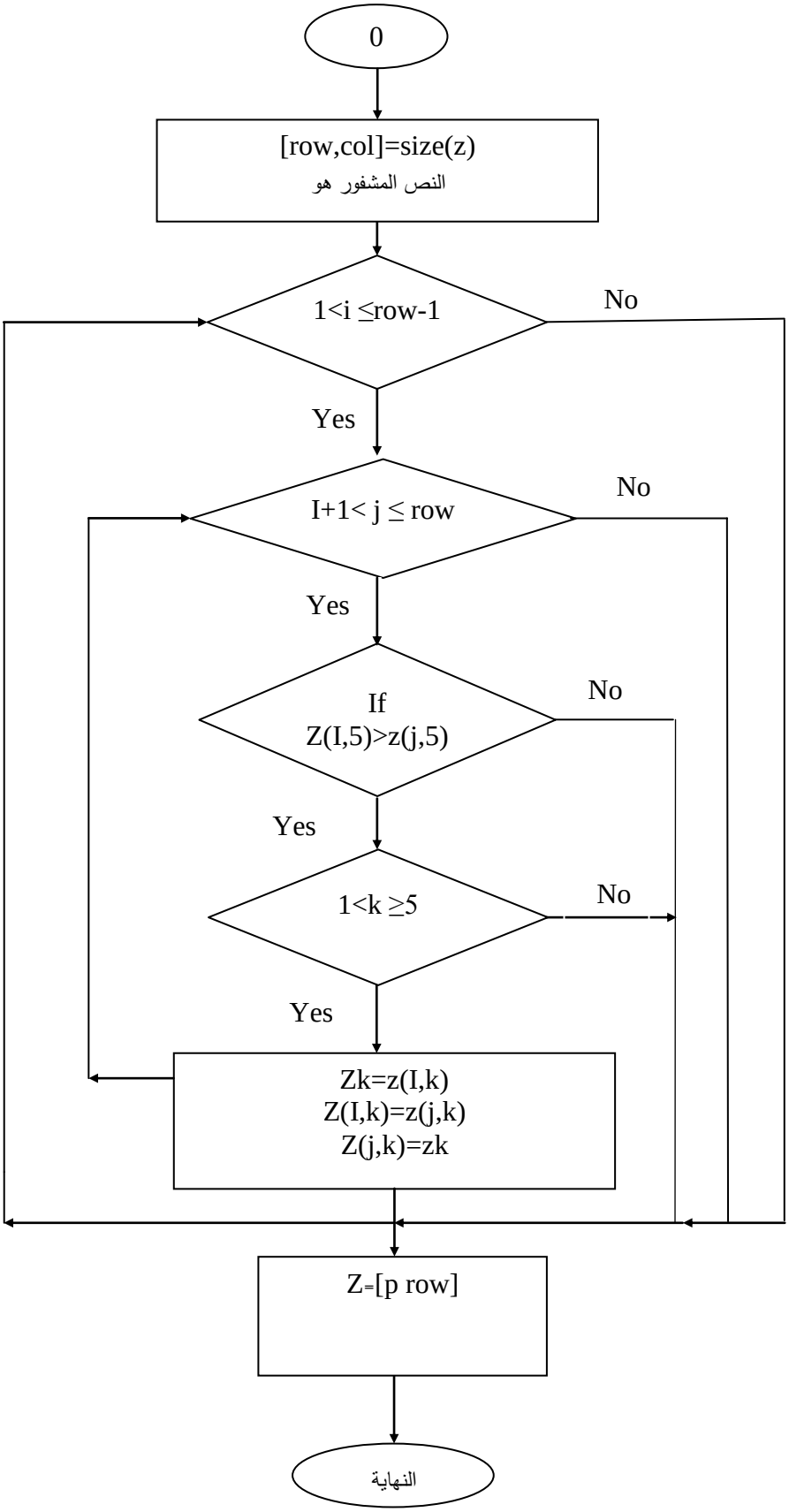


مخطط (٤-٥) ضرب النقطة بعدد صحيح باستخدام دالة الاتزان

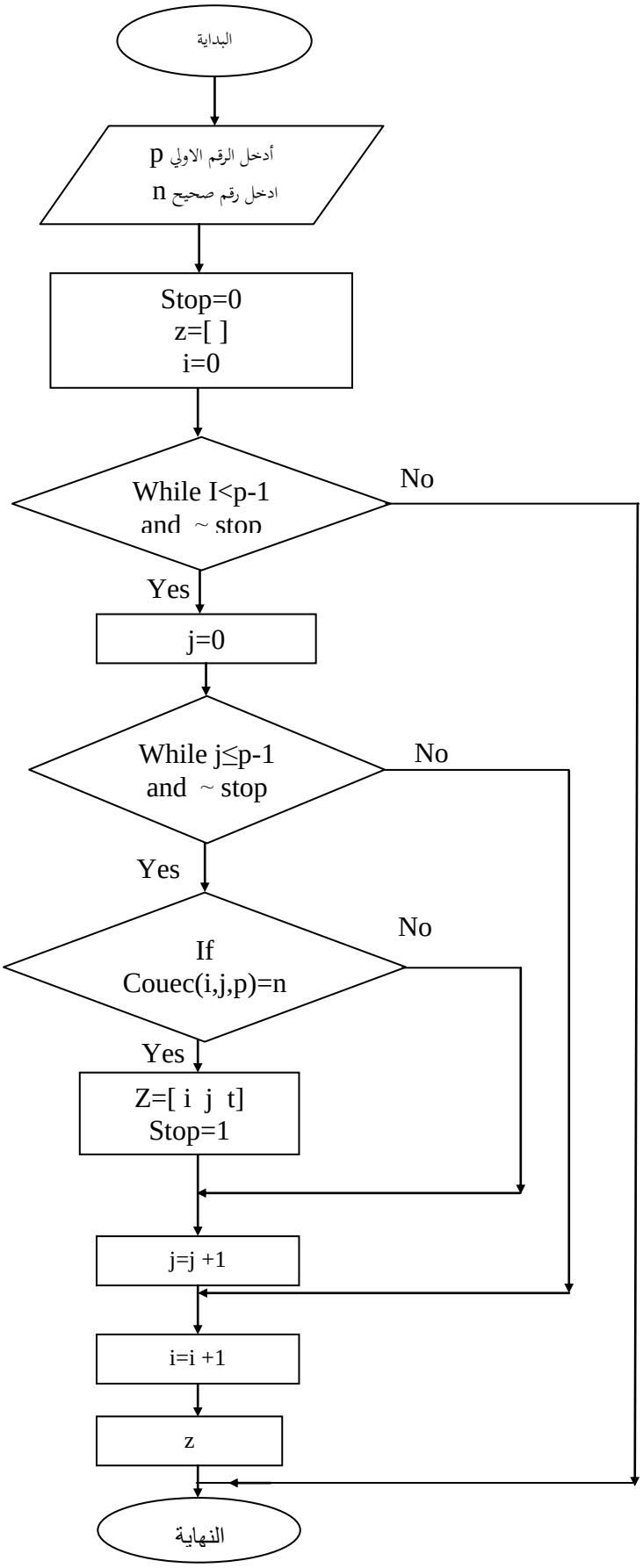


مخطط (٤- ٦) مخطط ايجاد عدد نقاط المنحني

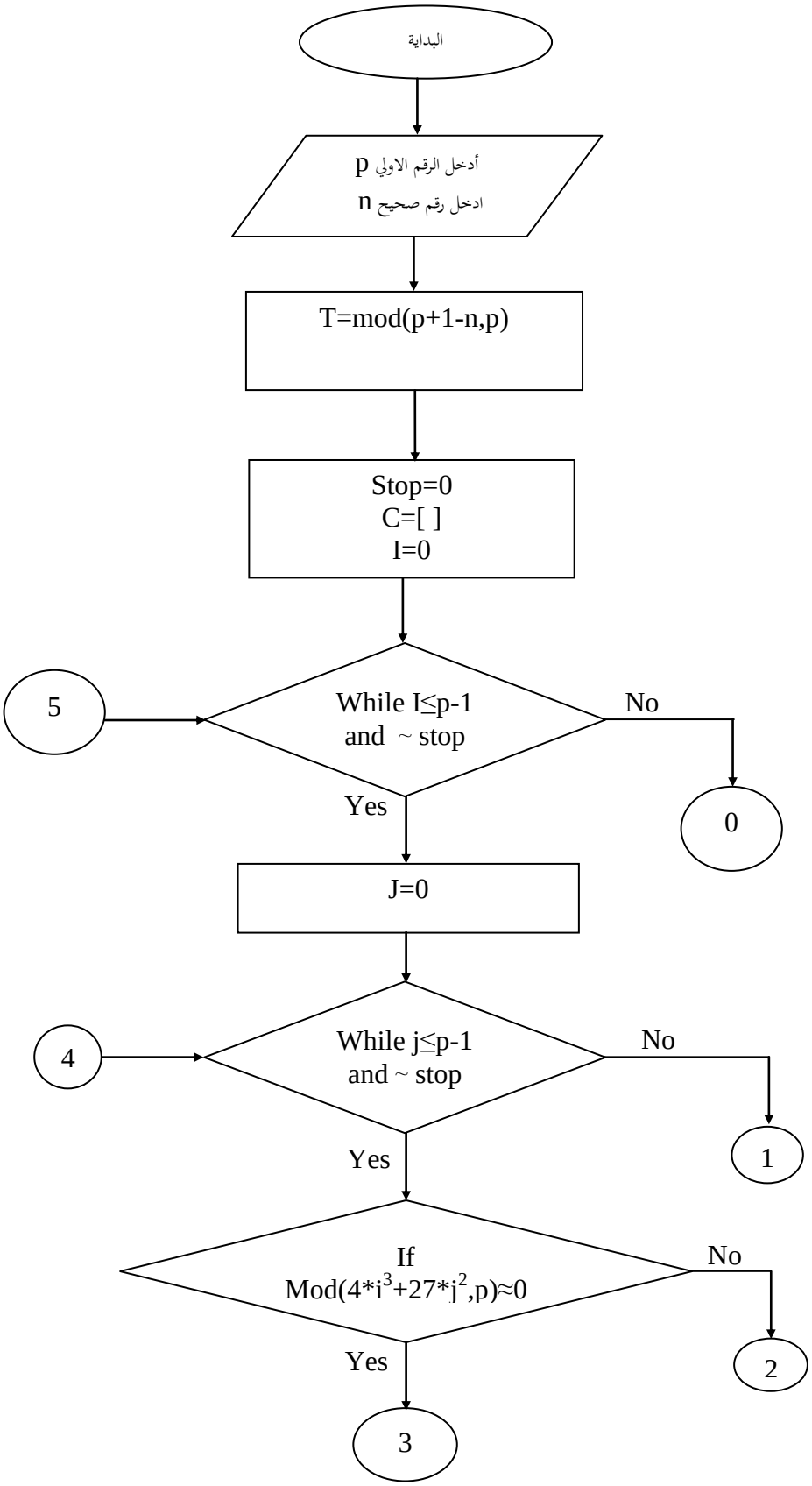

البداية
ادخل الرقم الاولي
Z=[ ]
0<j ≤p-1
No
Yes
0< j ≤ p-1
No
Yes
R=mod(4*i^3+27*j^2,p)
If
r≈0
No
Yes
K=mod(1728*4*i^3*invmod(r,p),p)
Z=[z;ij k r couec(ij,p)]
0

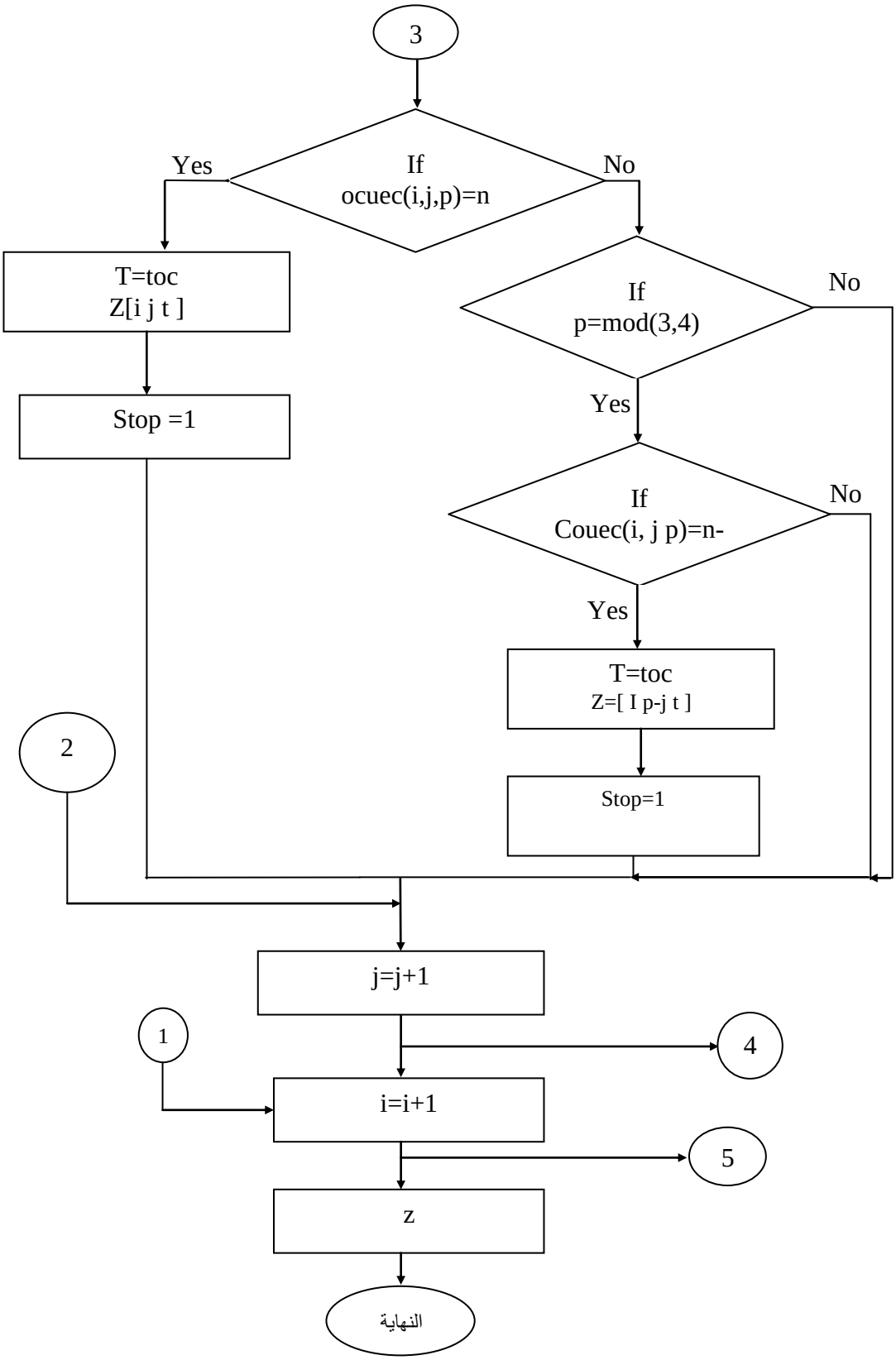


مخطط (٤- ٧) حساب كل المنحنيات وترتيبها في الحقل F_p

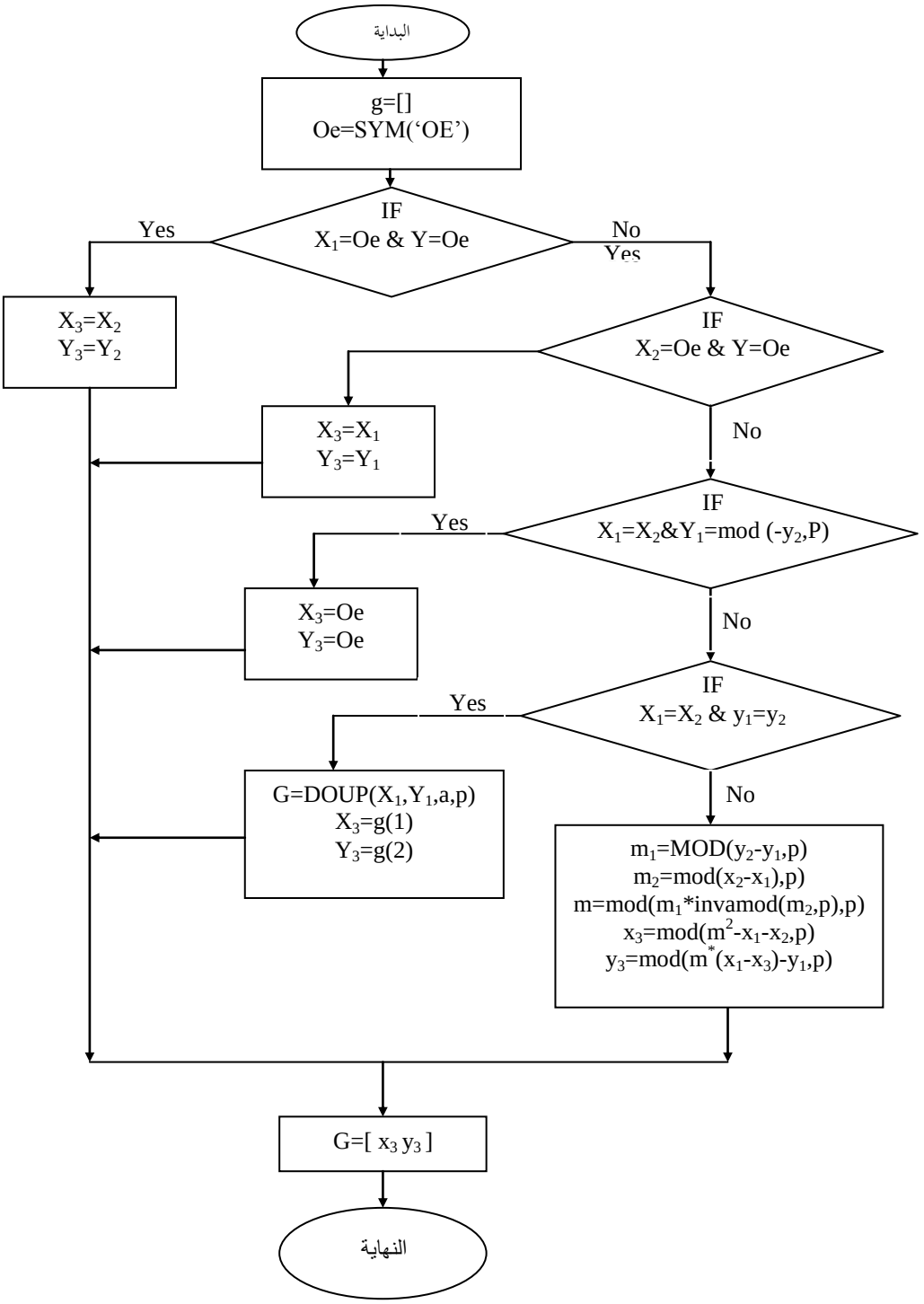


مخطط (٤-٨) الخوارزمية الاعتيادية للبحث

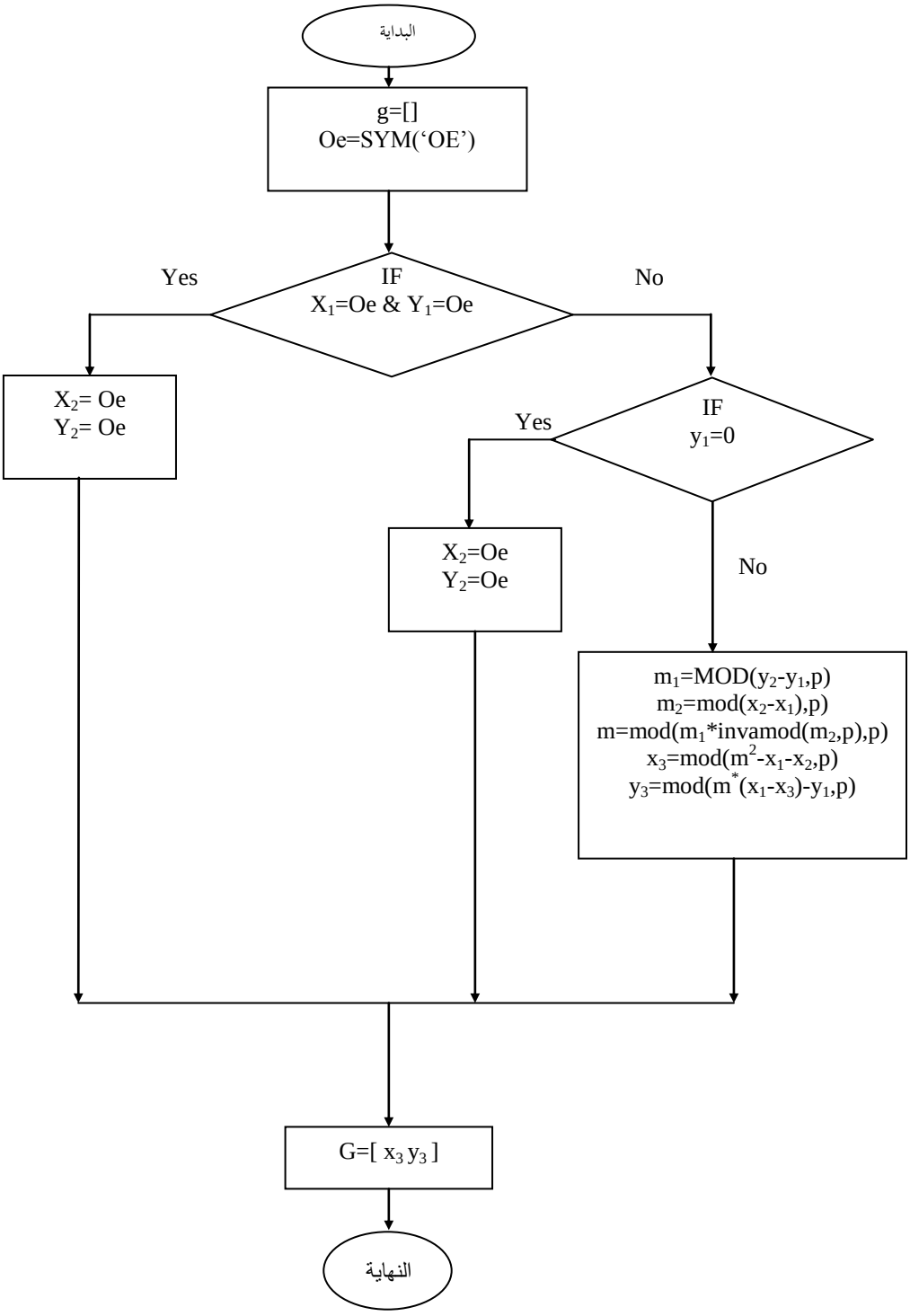

البداية
أدخل الرقم الاولي p
ادخل رقم صحيح n
T=mod(p+1-n,p)
Stop=0
C=[ ]
I=0
5
While I≤p-1
and ~ stop
No
Yes
0
J=0
4
While j≤p-1
and ~ stop
No
Yes
1
If
Mod(4*i^3+27*j^2,p)≈0
No
Yes
2
3



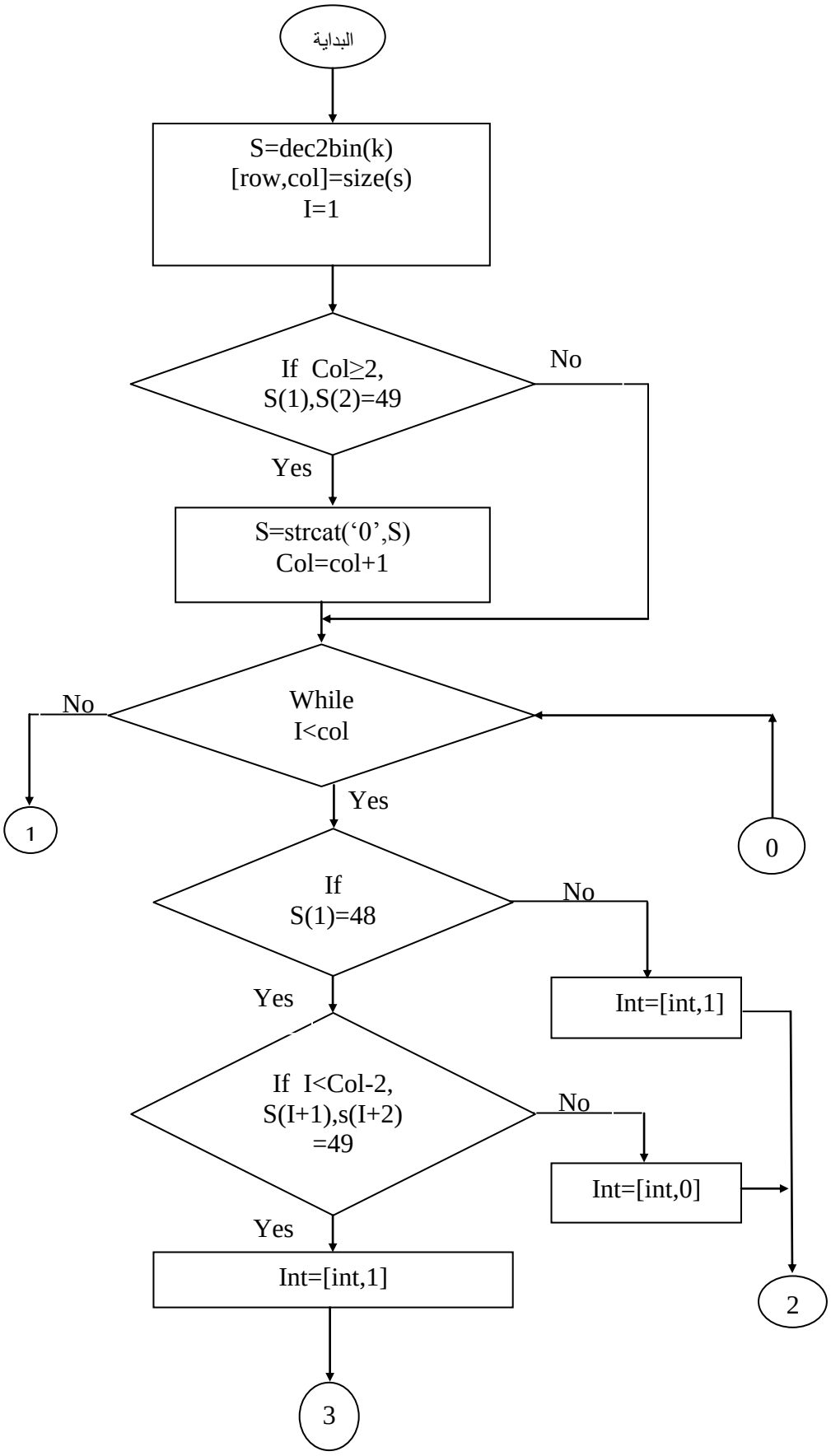
شكل (٤– ٩) الخوارزمية المقترحة للبحث العشوائي عن منحني باستخدام

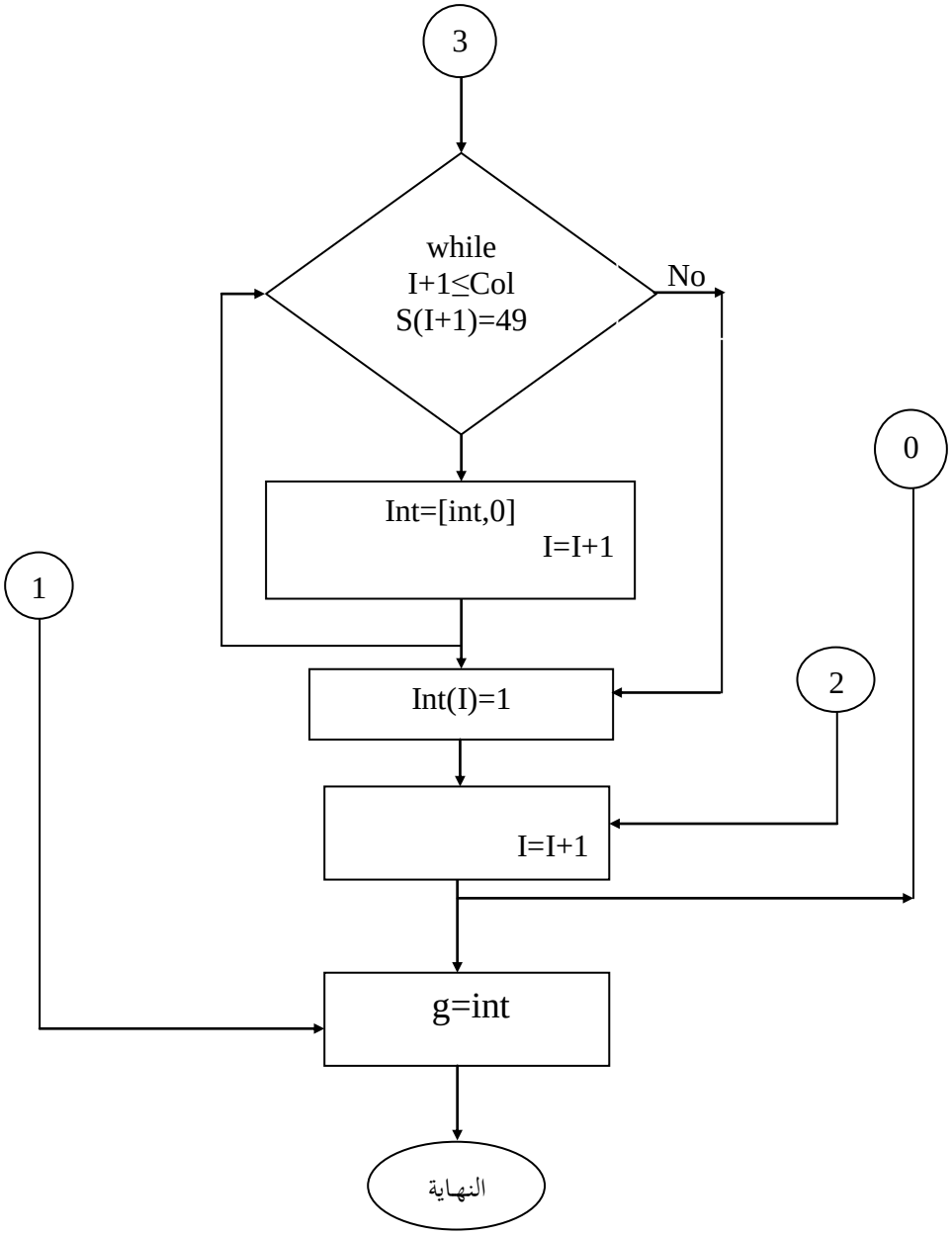


مخطط (٤-١١) خوارزمية جمع نقطتين

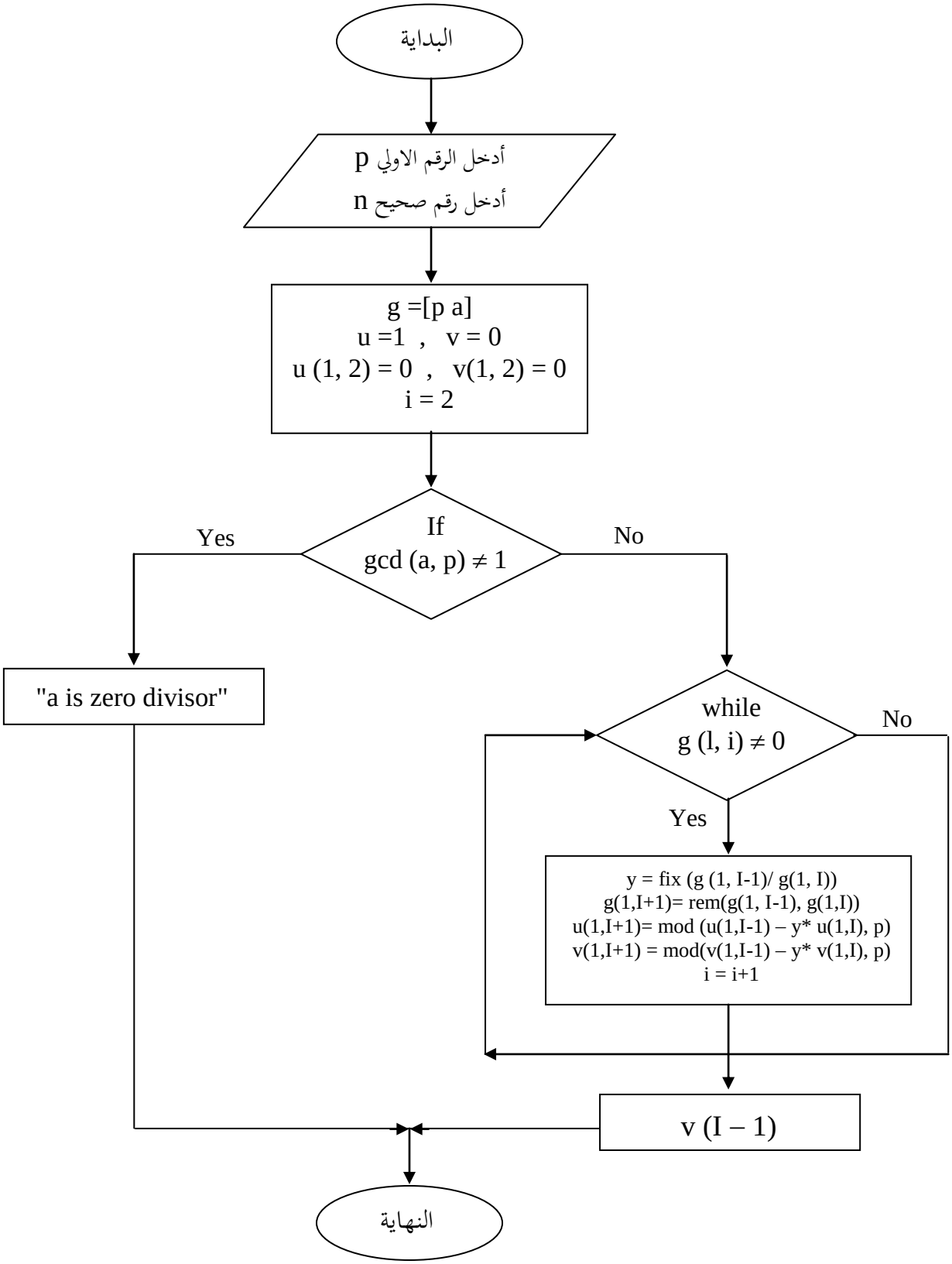


مخطط (٤-١٢) خوارزمية المضاعفة

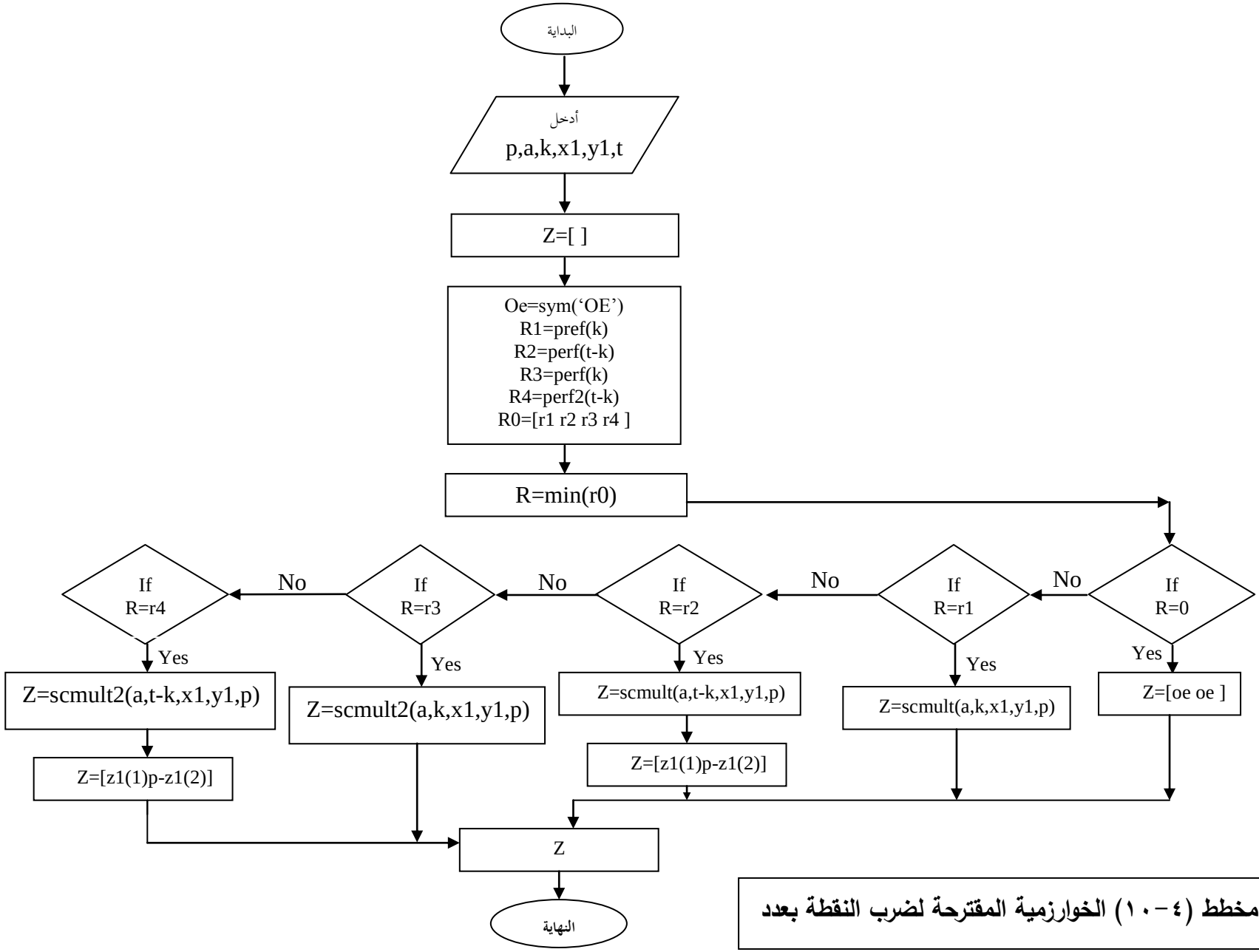

البداية
S=dec2bin(k)
[row,col]=size(s)
I=1
If Col≥2,
S(1),S(2)=49
No
Yes
S=strcat('0',S)
Col=col+1
While
I<col
No
Yes
1
0
If
S(1)=48
No
Yes
Int=[int,1]
If I<Col-2,
S(I+1),s(I+2)
=49
No
Yes
Int=[int,0]
Int=[int,1]
2
3



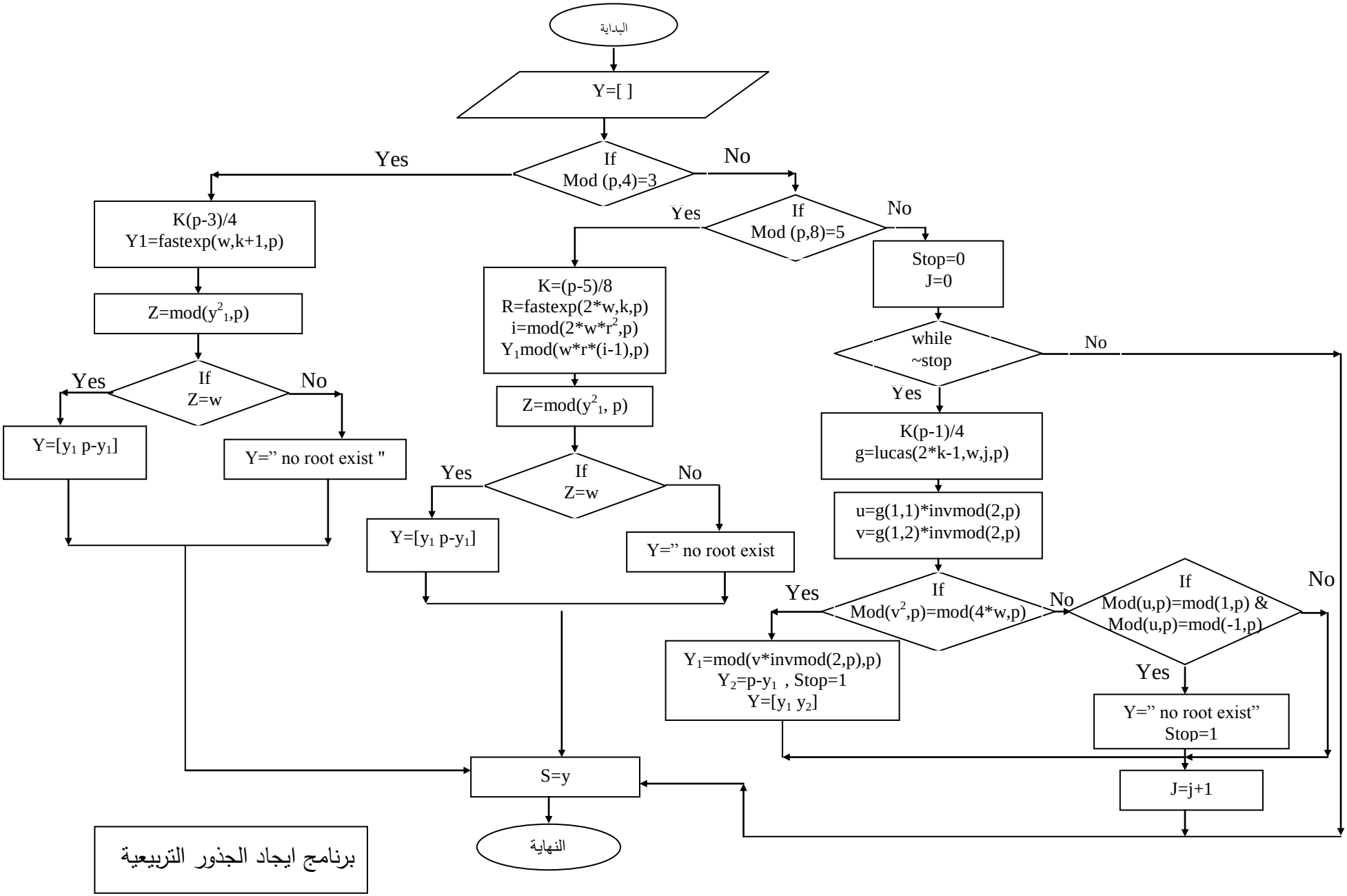
مخطط (٤-١٣) دالة الاتزان



مخطط (٤–١٤) برنامج ايجاد معكوس عدد صحيح في الحقل المنهي F_p .



مخطط (٤-١٠) الخوارزمية المقترحة لضرب النقطة بعدد


البداية
Y=[ ]
If
Mod (p,4)=3
Yes
No
K(p-3)/4
Y1=fastexp(w,k+1,p)
Z=mod(y^2_1,p)
If
Z=w
Yes
No
Y=[y1 p-y1]
Y=" no root exist "
If
Mod (p,8)=5
Yes
No
K=(p-5)/8
R=fastexp(2*w,k,p)
i=mod(2*w*r^2,p)
Y1mod(w*r*(i-1),p)
Z=mod(y^2_1, p)
If
Z=w
Yes
No
Y=[y1 p-y1]
Y=" no root exist
Stop=0
J=0
while
~stop
No
Yes
K(p-1)/4
g=lucas(2*k-1,w,j,p)
u=g(1,1)*invmod(2,p)
v=g(1,2)*invmod(2,p)
If
Mod(v^2,p)=mod(4*w,p)
Yes
No
Y1=mod(v*invmod(2,p),p)
Y2=p-y1 , Stop=1
Y=[y1 y2]
If
Mod(u,p)=mod(1,p) &
Mod(u,p)=mod(-1,p)
No
Yes
Y=" no root exist"
Stop=1
J=j+1
S=y
النهاية
برنامج ايجاد الجذور التربيعية

٥-١ المقدمـة

لقد تضمن البحث دراسة تحليلية لبعض الجوانب الرياضياتية للمنحنيات الاهليلجية وما توفره هذه الجوانب من نقاط قوة وضعف يمكن أن تحسب لها أو عليها وتم التوصل إلى عدد من الاستنتاجات وتصور لبعض من الأعمال المستقبلية.

٥-٢ الاستنتاجات

آ- تصور مقبول لبدايات استخدام المنحنيات الاهليلجية (*Elliptic curves*) في التطبيقات الرياضياتية والمجالات التي تم فيها هذا التطبيق .

ب-التعرف على الخواص الحسابية للمنحنيات الاهليلجية التي ساعدت على توظيف هذه الأنواع من المنحنيات في أنظمة التشفير .

جـ- دراسة تحليلية لأنظمة تشفير المنحنيات الاهليلجية وشملت :-

أولا- نظام تشفير دايف – هيلمان (*Dieffe – Hellman*) باستخدام المنحنيات الاهليلجية وهو نظام لتبادل المفاتيح بين طرفين باستخدام قناة عامة .

ثانياً- نظام تشفير ميسي – اومورا (*Massy-Omura*) ويعتمد على المبدأ نفسه الذي تم على اساسه تصميم نظام دايف-هيلمان، ولكن في هذا النظام يتم تبادل الرسائل بدلا من المفاتيح . وهنا يجب أن تكون وحدة النص الواضح نقطة في المنحنى.

ثالثاً- خوارزمية تشفير الجمال باستخدام المنحنيات الاهليلجية وفيها يجب أن تكون وحدات الرسالة نقطة في المنحنى .

رابعاً- نظام منسيز- فنستون (*Menzese-Vanstone*) وهو من الأنظمة التي توظف المنحنيات الاهليلجية ولا يوجد مشابه له في الأنظمة الاعتيادية، ولا يشترط فيه أن تكون الرسالة نقطة في المنحنى الاهليلجي.

د – دراسة بعض الطرائق المستخدمة لمهاجمة أنظمة تشفير المنحنيات الاهليلجية (ECC) باختلاف أنواعها. التي تعتمد على تحليل رتبة المنحنى أو التي تختزل (ECDLP) إلى (DLP) الاعتيادي أو التي تعتمد على القنوات الجانبية أو نوعية الحسابات المستخدمة .

هـ- مسألة اللوغاريتم المنفصل في المنحنيات الاهليلجية (*ECDLP*) لم يثبت إنها غير قابلة للحل ، وفي الوقت نفسه لا توجد خوارزمية لحل هذه المسألة في اقل من وقت مستغرق بـ (*Exponential time*).

و- نوع المنحنى له دور كبير في أمنية أنظمة (*ECC*) وفي الوقت نفسه لا يمكن الإقرار فيما إذا كان المنحنى يحقق الأمنية ، أي أن يقال عن منحنٍ يحقق ألامنية كما لم يتم التوصل إلى شروط للمنحنيات التي لا تحقق الأمنية المطلوبة أمام طرائق المهاجمة المعروفة .

ز-(*ECDLP*) يعتمد على دالة الأثر للمنحنى (*Trace of curve*) وعلى نوع الحقل المعرف عليه المنحنى، بينما لا يوجد مثل ذلك في (*DLP*).

ح-العدد الكلي للمنحنيات في الحقل F_p يكون $p(p-1)$.

ط-العدد الكلي للمنحنيات المفردة المفرطة في الحقل F_p يكون أحد مضاعفات $(p-1)$.

ي- يمكن تمييز صفوف بعض المنحنيات (*Classes of curve*) في الحقل F_p من خلال :-

أولاً- إذا كان $p \equiv 1 \pmod{12}$ فان كل المنحنيات المفردة المفرطة يكون فيها $b \neq 0$, $a \neq 0$.

ثانياً- إذا كان $p \equiv 5 \pmod{12}$ فان كل المنحنيات التي فيها $a=0$ تكون مفردة مفرطة.

ثالثاً- إذا كان $p \equiv 7 \pmod{12}$ فان كل المنحنيات التي فيها $b=0$ تكون مفردة مفرطة.

رابعاً- إذا كان $p \equiv 11 \pmod{12}$ فان كل المنحنيات التي يكون فيها $a=0$ أو $b=0$ تكون مفردة مفرطة .

ك- المنحنيان $E_1: y^2 = x^3 + ax + b$ و $E_2: y^2 = x^3 + ax - b$ المعرفان على الحقل F_p يمتلكان العدد نفسه من النقاط إذا كان $p \equiv 1 \pmod 4$ ويكون $\#E_2 = p+1+t$ إذا كان $p \equiv 3 \pmod 4$ حيث أن t هي دالة الأثر للمنحنى E_1.

ل- حساب عدد نقاط المنحنى باستخدام الطريقة العامة (طريقة حساب رمز ليجندر لمتعددة الحدود التكعيبية) يكون مكافئاً لحل (*ECDLP*).

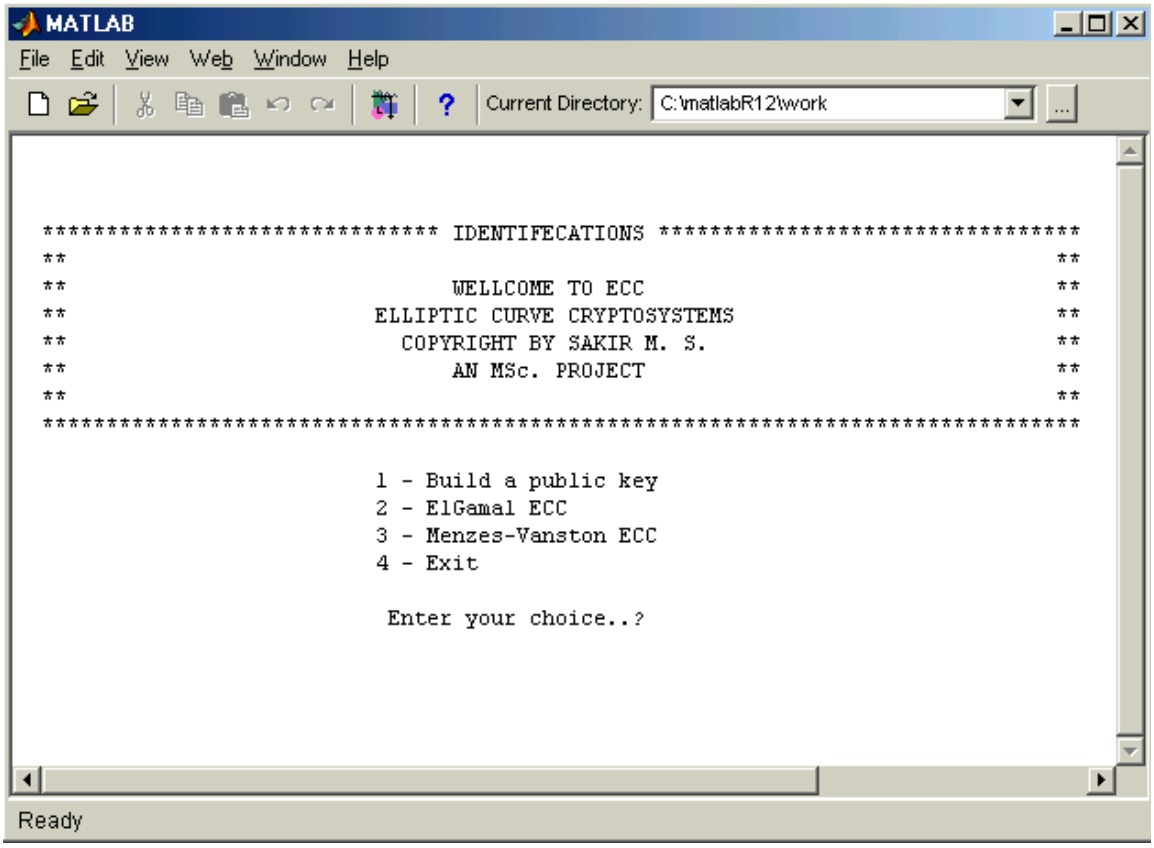
٥-٣ الأعمال المستقبلية

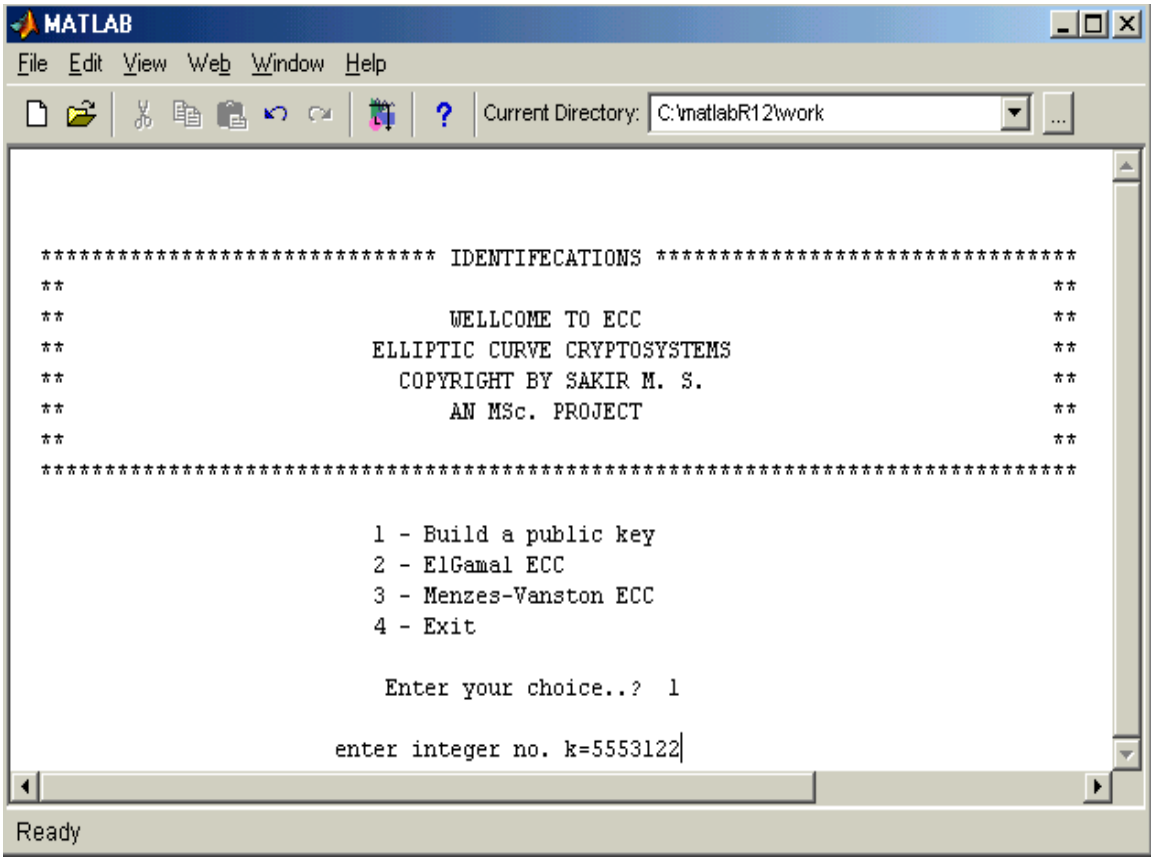
آ-محاولة تطوير البرامج التي تم إنشاؤها وصولا بها إلى أعداد كبيرة بحيث يمكن إنشاء أنظمة تشفير عملية قابلة للتطبيق تقريبا بحجم مفتاح (160 *bits*) أو اكثر حتى وان تطلب الأمر تغيير اللغة التي كتبت بها .

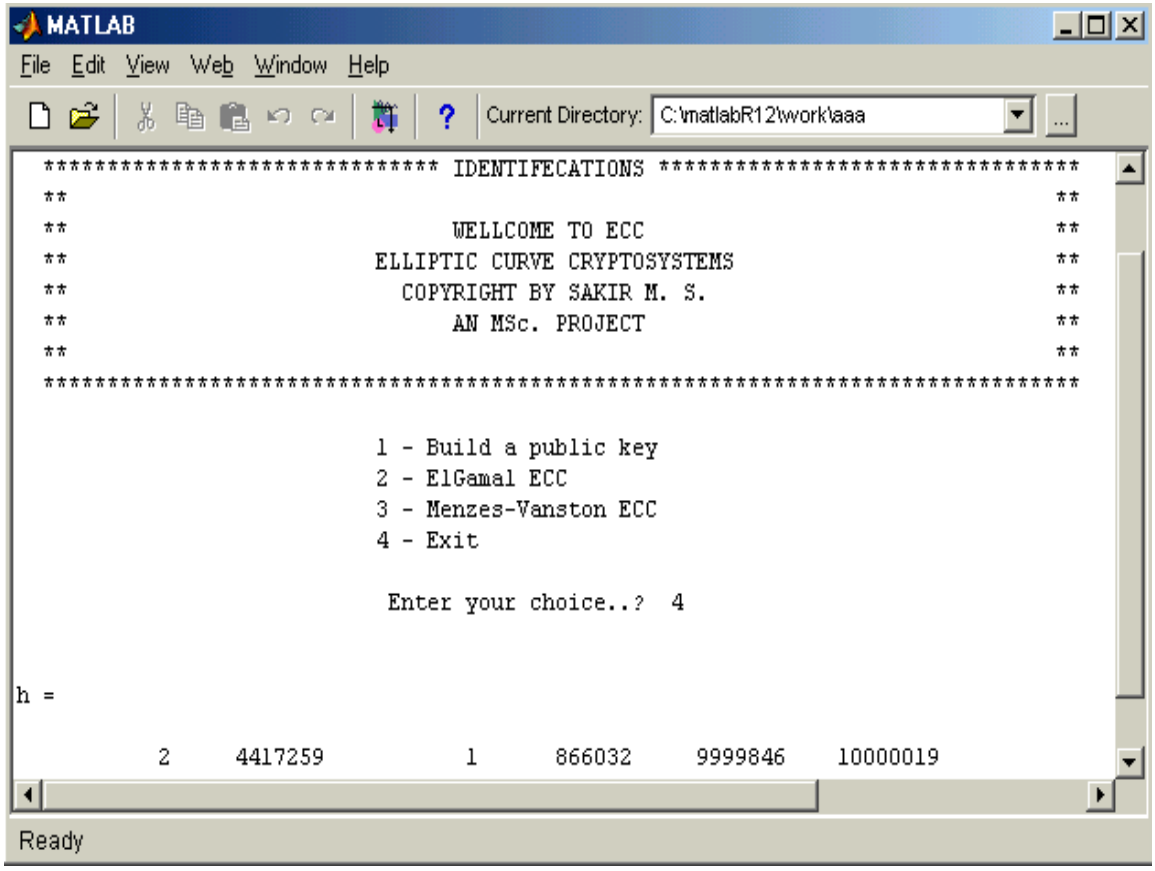
ب-دراسة مواضيع أخرى مقاربة أو لها علاقة بالمنحنيات الاهليلجية مثل منحنيات *hyper Elliptic curve*) و (*Super Elliptic curve*)وكذلك المواضيع المتعلقة بالكومبيوتر الكمي والحسابات الكمية .

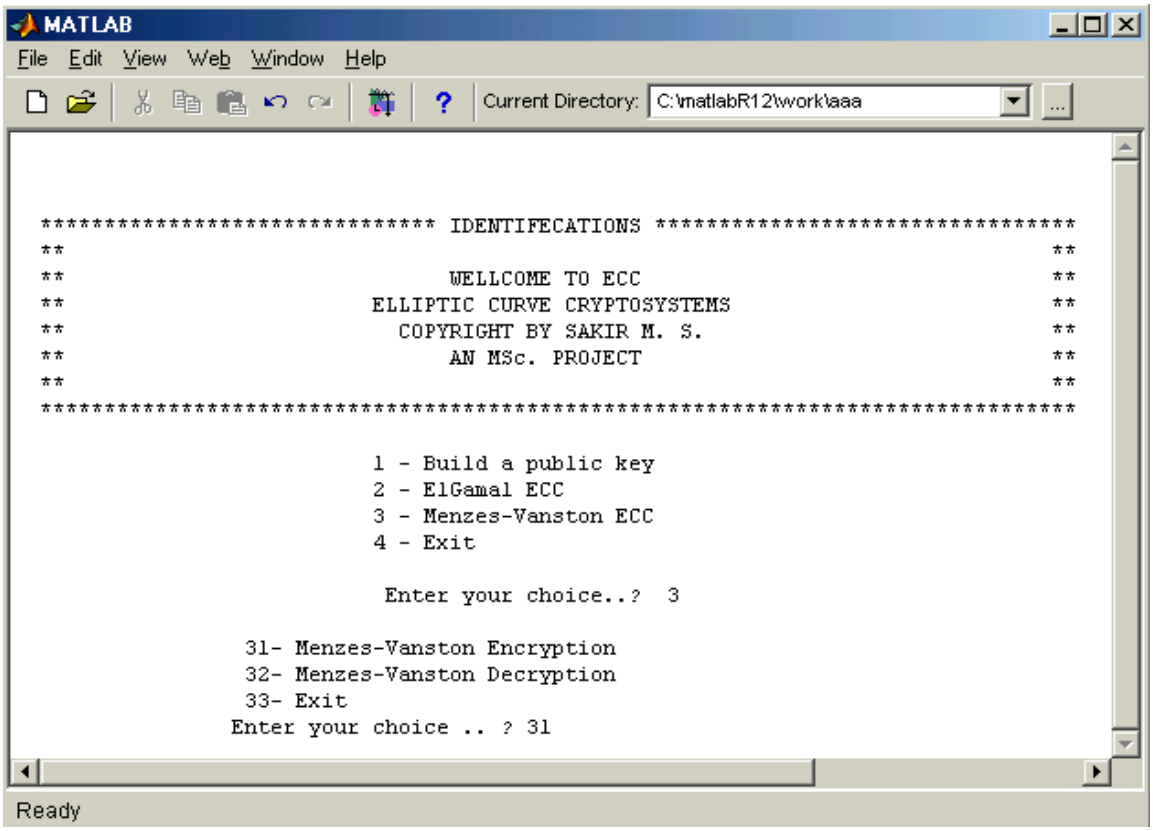
جـ- تلعب التماثلات (*Isomorphism*) دورا مهما في المنحنيات الاهليلجية ويمكن استغلال هذا الدور لإعطاء أمنية اكبر أو لمهاجمة أنظمة تشفير المنحنيات الاهليلجية بل ويمكن استغلال هذه الخاصية حتى في بناء أنظمة تشفير جديدة .

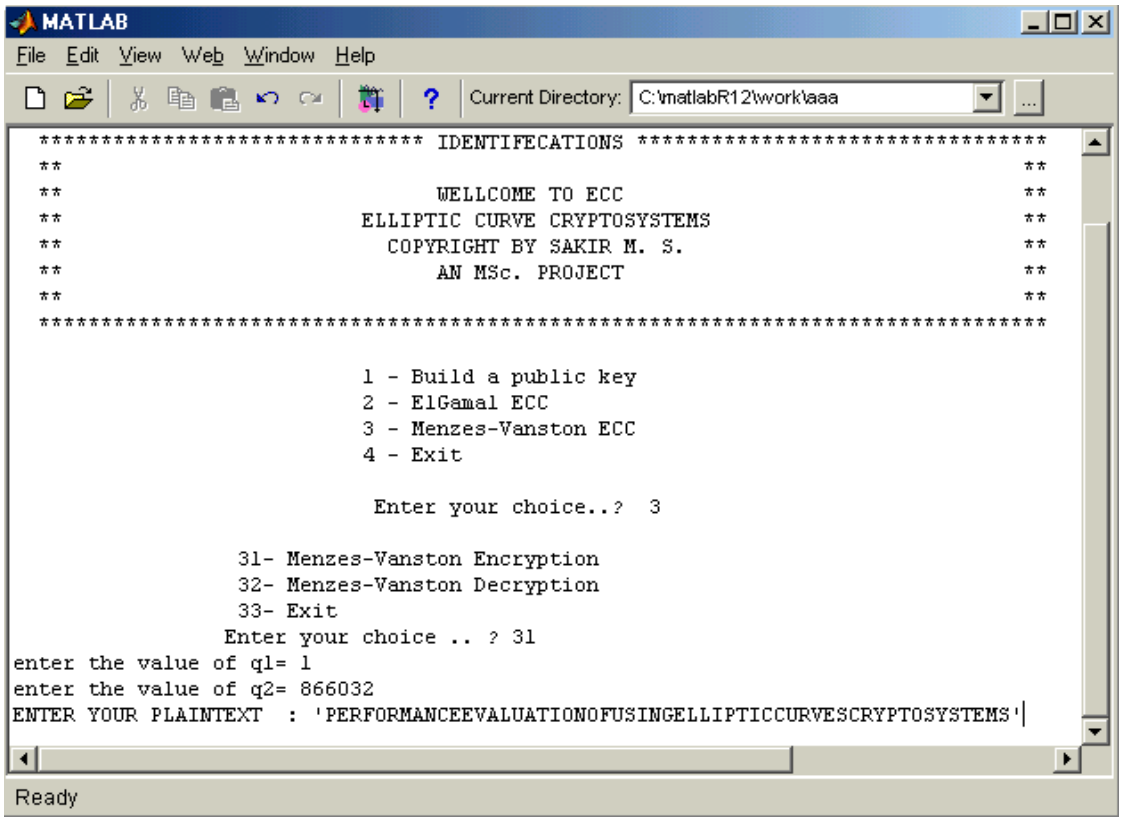
د -الصلة الوثيقة بين حساب البواقي التربيعية ورمز ليجندر من جهة وحساب عدد نقاط المنحنيات من جهة أخرى فإذا ما كان هناك خوارزميات اكثر كفاءة لحسابها فيمكن إيجاد طرائق اكفأ لحساب عدد نقاط المنحنيات .

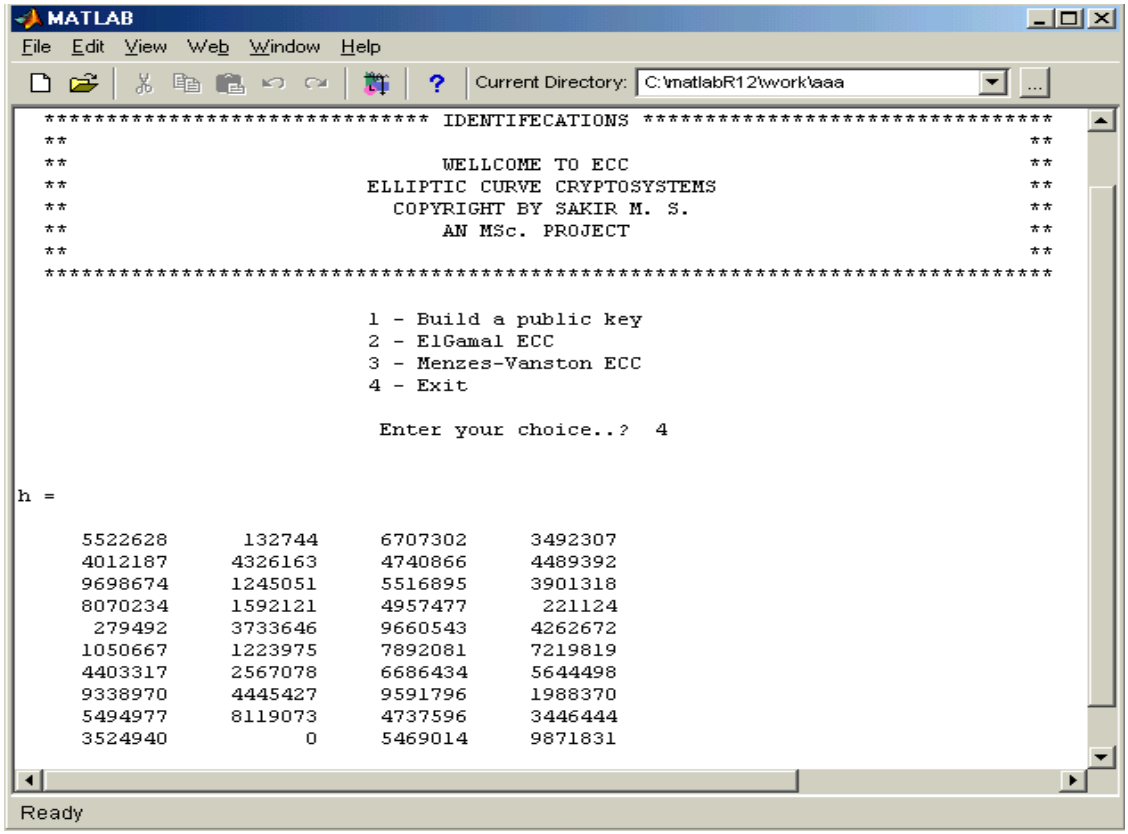

MATLAB
File Edit View Web Window Help
Current Directory: C:\matlabR12\work
********** IDENTIFECATIONS **********
WELLCOME TO ECC
ELLIPTIC CURVE CRYPTOSYSTEMS
COPYRIGHT BY SAKIR M. S.
AN MSc. PROJECT
1 - Build a public key
2 - ElGamal ECC
3 - Menzes-Vanston ECC
4 - Exit
Enter your choice..?
Ready

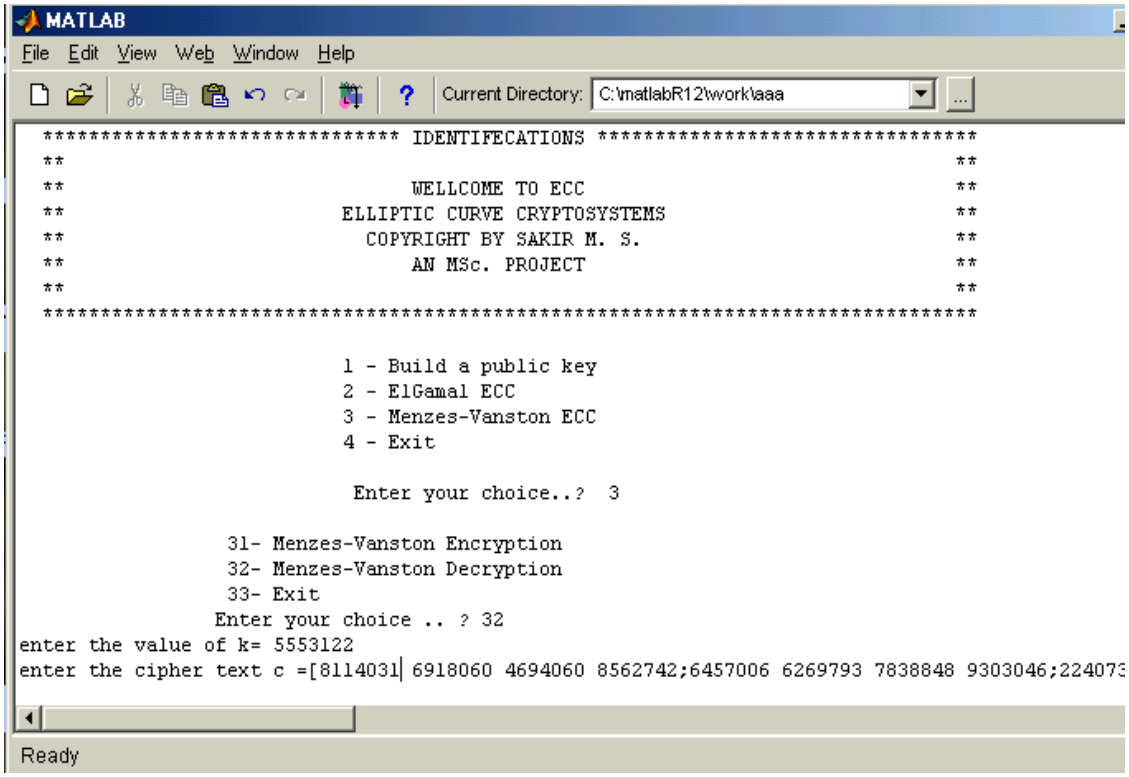

MATLAB
File Edit View Web Window Help
Current Directory: C:\matlabR12\work
********** IDENTIFECATIONS **********
WELLCOME TO ECC
ELLIPTIC CURVE CRYPTOSYSTEMS
COPYRIGHT BY SAKIR M. S.
AN MSc. PROJECT
1 - Build a public key
2 - ElGamal ECC
3 - Menzes-Vanston ECC
4 - Exit
Enter your choice..? 1
enter integer no. k=5553122
Ready

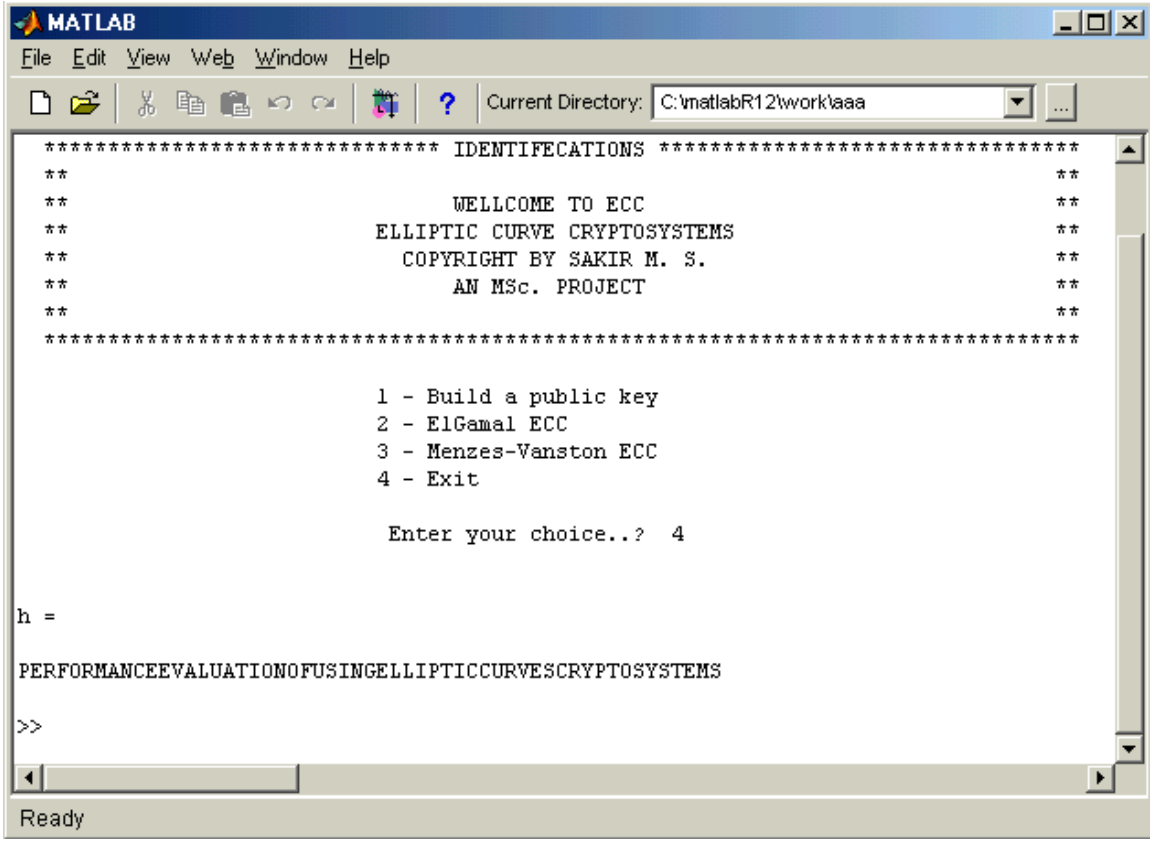

MATLAB
File Edit View Web Window Help
Current Directory: C:\matlabR12\work\aaa
********** IDENTIFECATIONS **********
**
**
WELLCOME TO ECC
ELLIPTIC CURVE CRYPTOSYSTEMS
COPYRIGHT BY SAKIR M. S.
AN MSc. PROJECT
**
**
****
1 - Build a public key
2 - ElGamal ECC
3 - Menzes-Vanston ECC
4 - Exit
Enter your choice..? 4
h =
2 4417259 1 866032 9999846 10000019
Ready


MATLAB
File Edit View Web Window Help
Current Directory: C:\matlabR12\work\aaa
********** IDENTIFECATIONS **********
**
**
WELLCOME TO ECC
ELLIPTIC CURVE CRYPTOSYSTEMS
COPYRIGHT BY SAKIR M. S.
AN MSc. PROJECT
**
**
****
1 - Build a public key
2 - ElGamal ECC
3 - Menzes-Vanston ECC
4 - Exit
Enter your choice..? 3
31- Menzes-Vanston Encryption
32- Menzes-Vanston Decryption
33- Exit
Enter your choice .. ? 31
Ready


MATLAB
File Edit View Web Window Help
Current Directory: C:\matlabR12\work\aaa
********** IDENTIFECATIONS **********
** **
** WELLCOME TO ECC **
** ELLIPTIC CURVE CRYPTOSYSTEMS **
** COPYRIGHT BY SAKIR M. S. **
** AN MSc. PROJECT **
** **
1 - Build a public key
2 - ElGamal ECC
3 - Menzes-Vanston ECC
4 - Exit
Enter your choice..? 3
31- Menzes-Vanston Encryption
32- Menzes-Vanston Decryption
33- Exit
Enter your choice .. ? 31
enter the value of q1= 1
enter the value of q2= 866032
ENTER YOUR PLAINTEXT : 'PERFORMANCEEVALUATIONOFUSINGELLIPTICCURVESCRYPTOSYSTEMS'
Ready


MATLAB
File Edit View Web Window Help
Current Directory: C:\matlabR12\work\aaa
********** IDENTIFECATIONS **********
** **
** WELLCOME TO ECC **
** ELLIPTIC CURVE CRYPTOSYSTEMS **
** COPYRIGHT BY SAKIR M. S. **
** AN MSc. PROJECT **
** **
1 - Build a public key
2 - ElGamal ECC
3 - Menzes-Vanston ECC
4 - Exit
Enter your choice..? 4
h =
5522628 132744 6707302 3492307
4012187 4326163 4740866 4489392
9698674 1245051 5516895 3901318
8070234 1592121 4957477 221124
279492 3733646 9660543 4262672
1050667 1223975 7892081 7219819
4403317 2567078 6686434 5644498
9338970 4445427 9591796 1988370
5494977 8119073 4737596 3446444
3524940 0 5469014 9871831
Ready


MATLAB
File Edit View Web Window Help
Current Directory: C:\matlabR12\work\aaa
********** IDENTIFECATIONS **********
WELLCOME TO ECC
ELLIPTIC CURVE CRYPTOSYSTEMS
COPYRIGHT BY SAKIR M. S.
AN MSc. PROJECT
1 - Build a public key
2 - ElGamal ECC
3 - Menzes-Vanston ECC
4 - Exit
Enter your choice..? 3
31- Menzes-Vanston Encryption
32- Menzes-Vanston Decryption
33- Exit
Enter your choice .. ? 32
enter the value of k= 5553122
enter the cipher text c =[8114031 6918060 4694060 8562742;6457006 6269793 7838848 9303046;224073
Ready


MATLAB
File Edit View Web Window Help
Current Directory: C:\matlabR12\work\aaa
********** IDENTIFECATIONS **********
WELLCOME TO ECC
ELLIPTIC CURVE CRYPTOSYSTEMS
COPYRIGHT BY SAKIR M. S.
AN MSc. PROJECT
1 - Build a public key
2 - ElGamal ECC
3 - Menzes-Vanston ECC
4 - Exit
Enter your choice..? 4
h =
PERFORMANCEEVALUATIONOFUSINGELLIPTICCURVESCRYPTOSYSTEMS
>>
Ready

ABSTRACT

The Group of elliptic curve points is considered as suitable choice for constructing a ciphering system based on the concept of difficult solution of discrete logarithm problem in elliptic curve, that great's a clear change in the cryptography, and open a new widows for treatment with the special groups and abnormal operation .

This thesis provide the definition and mathematical properties of these curves, gives a strong for the properties of constricted group with it's points , gives how it is possible to be implemented in the cryptography and analyzing the weak points for such group .

This thesis proved a new theorem and corollary that can contribute in facilitating the computation process and give methods to conclude the n points of the curves without there calculation and using one of these theorem to propose the algorithm for random search about a curve with specified number of points, as well as design a program for implementing process of multiplying a point with a constant number , this program contains the combination of conventional addition and duplication and addition and duplication using the balancing function and calculating of inverse of points .a great reduction in calculation time is resulted .

Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Technology
Department of Applied Science

Performance Evaluation of Using Elliptic Curves Cryptosystems

A thesis
Submitted to Department of Applied Science in University of Technology as a Partial Fulfillment for the Requirement of M.Sc. Degree in Applied Mathematics Science

By
Shakir Mahmoud Salman Al- Azzawy

Supervised by
Prof. Dr. Sattar Badder Sadkhan Al- Malki

Thu Al-kidh 1423 January 2003