المنحنيات الاهليجية

1.1 مقدمة

- ذكرنا في الفصول السابقة عدة تطبيقات لمسألة حساب اللوغاريتم المتقطع في زمر دورية منتهية $\mathbb{G}$.
- كان مثالنا الاساسي هو الزمرة الضربية $\mathbb{Z}_p^*$ للاعداد الصحيحة في حالة mod لعدد اولي كبير نسبيا p.
- مما يعيب هذه الزمرة هو ان مسألة اللوغاريتم المتقطع **لها ليست صعبة بما فيه الكفاية**. $y = g^x \ mod \ p$
  - حيث تم حساب مسألة اللوغاريتم المتقطع بخوارزمية general number field sieve (GNFS) عام 2016 في حالة mod لعدد اولي p بطول 768 ثنائية.
  - تعتبر هذه الخوارزمية هي السبب الذي يتطلب ان يكون طول العدد الاولي 2048 ثنائية على الاقل.
    - يكون اجراء العمليات الرياضية لهكذا اعداد كبيرة بطيئًا ويزيد كلفة استخدام مناهج التشفير التي تتعامل مع هذه الزمر.
- لحل هذه المشكلة ، نستخدم "**زمرة نقاط**" **المنحنى الاهليجي** elliptic curve الذي يعرّف فوق زمرة منتهية.
- يعتبر هذا الحل مناسبا من الناحية العملية وهو شائع الاستخدام في شبكة الانترنت حاليا.
- تعمل افضل خوارزمية لحل مسألة اللوغاريتم المتقطع "الزمرة نقط المنحى الاهليجي" التي عدد عناصرها q بوقت مقداره $\mathcal{O}(\sqrt{q})$.
- وهذا يعني انه لتوفير أمنية مقاربة لامنية AES-128 ، فأنه يكفي استخدام زمرة بحجم $q \approx 2^{256}$ وبذلك فإن وقت حساب اللوغاريتم المتقطع هو $\sqrt{q} = 2^{128}$.
- تستخدم هذه الزمرة اعداد اولية بطول 256 ثنائية ، وهي اسرع من التعامل مع اعداد اولية بطول 2048 ثنائية.
- توصف المنحنيات الاهليجية بكونها مجموعة **الحلول** (النقاط) لمعادلات معيّنة ذات متغيرين.
- يمكن ان تعرّف المنحنيات الاهليجية فوق الزمر $\mathbb{Z}_p$ وتعتبر هذه المنحنيات بالغة الاهمية في التشفير معلن المفتاح.
- نبتدأ بعرض المنحنيات الاهليجية المعرّفة على اعداد حقيقية $\mathbb{R}$ ، لأنه يسهل تقديم المفاهيم الاساسية في هذه الحالة.

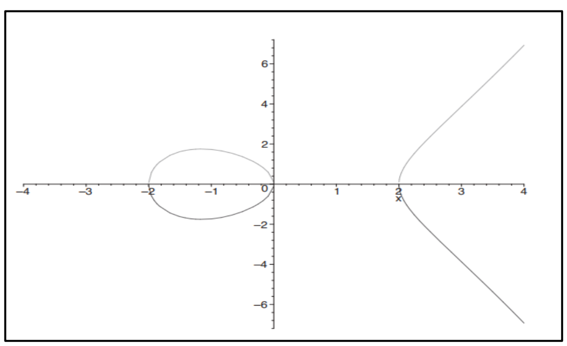
1.2 المنحنيات الاهليجية فوق الاعداد الحقيقية

تعريف(12.1): ليكن لدينا $a, b \in \mathbb{R}$ ثوابت تحقق $4a^3 + 27b^2 \neq 0$. يعرف المنحنى الاهليجي $\mathcal{E}$ بكونه مجموعة الحلول $(x, y) \in \mathbb{R} \times \mathbb{R}$ للمعادلة

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

بالاضافة الى نقطة خاصة $\mathcal{O}$ تعرف **بنقطة اللانهاية** point at infinity.

يوضّح الشكل(12.1) المنحنى الاهليجي $y^2 = x^3 - 4x$



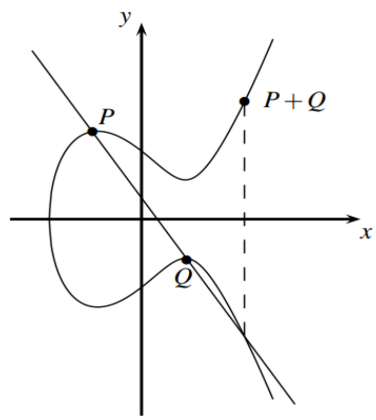
شكل (12.1): منحنى اهليجي فوق اعداد حقيقية

- يضمن الشرط $4a^3 + 27b^2 \neq 0$ ان المعادلة $x^3 + ax + b = 0$ تمتلك ثلاث جذور مختلفة.
- نقوم الأن بتعريف عملية ثنائية على $\mathcal{E}$ لتشكيل زمرة تبادلية (abelian group).
- تعرف هذه العملية عادة بعملية الجمع (+).
- تعتبر النقطة $\mathcal{O}$ هي العنصر المحايد ، وبذلك $P + \mathcal{O} = \mathcal{O} + P = P$ لجميع $P \in \mathcal{E}$.

ليكن لدينا $P, Q \in \mathcal{E}$ ، بحيث $P = (x_1, y_1)$ و $Q = (x_2, y_2)$. نفترض الأن ثلاث حالات:

1. $x_1 \neq x_2$
2. $x_1 = x_2$ و $y_1 = -y_2$
3. $x_1 = x_2$ و $y_1 = y_2$

الحالة الأولى. في هذه الحالة ، نعرّف $\mathcal{L}$ بكونه الخط الذي يمر خلال P و Q. يتقاطع $\mathcal{L}$ مع $\mathcal{E}$ في النقطتين P و Q ، ومن السهولة ملاحظة ان $\mathcal{L}$ يقطع نقطة اخرى ، ندعوها R'. عندما نعكس R' حول المحور السيني ، نحصل على النقطة R. نعرّف $P + Q = R$. لاحظ الشكل (12.2).



شكل (12.2): جمع نقطتين في منحنى اهليجي فوق الاعداد الحقيقية.

لنرى الصيغة الجبرية لحساب R. معادلة $\mathcal{L}$ هي $y = \lambda x + v$ ، حيث ان ميل $\mathcal{L}$ هو

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

و

$$v = y_1 - \lambda x_1 = y_2 - \lambda x_2$$

لايجاد النقاط في $\mathcal{L} \cap \mathcal{E}$ ، نعوّض $y = \lambda x + v$ في معادلة $\mathcal{E}$ لنحصل على

$$(\lambda x + v)^2 = x^3 + ax + b$$

وهي

$$x^3 - \lambda^2 x^2 + (a - 2\lambda v)x + b - v^2 = 0$$

بحيث ان جذور هذه المعادلة هي قيم المحور السيني للنقاط الموجودة في $\mathcal{L} \cap \mathcal{E}$. عرفنا للتو ان النقطتين P و Q ينتميان الى $\mathcal{L} \cap \mathcal{E}$ وبالتالي فإن x_1 و x_2 هما جذران للمعادلة اعلاه. وبما انها معادلة تكعيبية فانها تمتلك جذر حقيقي ثالث ، ليكن x_3. مجموع الجذور الثلاثة يجب ان يكون مساوٍ لنفي معامل λ^2. لذلك

$$x_3 = \lambda^2 - x_1 - x_2$$

وبذلك فإن x_3 هو المحور السيني للنقطة R'. نرمز للمحور الصادي لـR' بالرمز $-y_3$ ، وبالتالي فإن المحور الصادي لـ R هو y_3. نحسب y_3 عن طريق الميل λ وبذلك نحصل

$$\lambda = \frac{-y_3 - y_1}{x_3 - x_1}$$

وبالتالي

$$y_3 = \lambda(x_1 - x_3) - y_1$$

وبذلك اشتققنا معادلة $P + Q$ للحالة الأولى: اذا كان $x_1 \neq x_2$ ، فإن $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ بحيث

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

و

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

الحالة الثانية. عندما $x_1 = x_2$ و $y_1 = -y_2$: نعرّف في هذه الحالة $(x,y) + (x,-y) = \mathcal{O}$ لجميع النقاط $(x,y) \in \mathcal{E}$. وبذلك فإن (x,y) و $(x,-y)$ هما معكوسان في المنحنيات الاهليجية فيما يخص عملية الجمع.

الحالة الثالثة. هنا يتم جمع النقطة $P = (x_1, y_1)$ مع نفسها. نفترض ان $y_1 \neq 0$. سوف نعالج هذه الحالة كما فعلنا في الحالة الأولى، باستثناء ان الخط $\mathcal{L}$ هو المماس للنقطة P. يحسب ميل الخط $\mathcal{L}$ باشتقاق المعادلة بالنسبة الى $\mathcal{E}$:

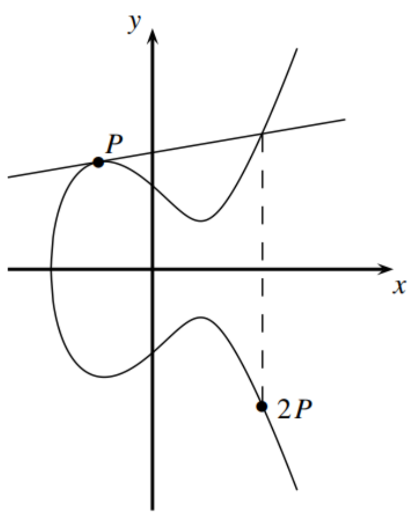
$$2y\frac{dy}{dx} = 3x^2 + a$$

بتعويض $x = x_1$ و $y = y_1$، نرى ان ميل المماس هو

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

بقية التفاصيل تشبه الحالة الأولى باستثناء التغيير في حساب λ.

يوضّح الشكل(13.3) جمع النقطة مع نفسها في المنحنى الاهليجي فوق القيم الحقيقية.



شكل (12.3): جمع النقطة مع نفسها في المنحنى الاهليجي

لحد الأن وصلنا الى تعريف خصائص عملية الجمع:

1. عملية الجمع تكون مغلقة في الزمرة $\mathcal{E}$.
2. عملية الجمع هي عملية تبادلية.
3. تمثل النقطة $\mathcal{O}$ العنصر المحايد لعملية الجمع.
4. لكل نقطة في $\mathcal{E}$ يوجد معكوس فيما يخص عملية الجمع.

- لغرض اظهار ان $(\mathcal{E}, +)$ هي زمرة تبادلية ، يجب اثبات ان عملية الجمع هي عملية تجميعية. اثبات هذا الشئ خارج نطاق الكتاب.

1.3 المنحنيات الاهليجية فوق الزمر $\mathbb{Z}_p$

- نهتم في تطبيقات التشفير بالمنحنيات الاهليجية فوق الحقول المنتهية Finite fields.
- لغرض التبسيط سوف نتعامل مع منحنيات فوق زمر اولية prime groups فقط $\mathbb{Z}_p$.
- نستخدم الرمز $\mathcal{E}\backslash\mathbb{Z}_p$ للاشارة الى ان المنحنى الاهليجي معرّف فوق الزمرة الاولية.

تعريف(12.2)**:** ليكن $p > 3$ عدد اولي. يعرف المنحنى الاهليجي $y^2 = x^3 + ax + b$ فوق الزمرة $\mathbb{Z}_p$ بأنها مجموعة الحلول $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ للتطابق

$$y^2 = x^3 + ax + b \bmod p \qquad (12.1)$$

بحيث ان $a, b \in \mathbb{Z}_p$ بشرط $4a^3 + 27b^2 \bmod p = 0$ ، بالاضافة الى النقطة $\mathcal{O}$ التي تعرف بنقطة اللانهاية.

نقاط المنحنى. ليكن $\mathcal{E}/\mathbb{Z}_p$ منحنى اهليجي. سوف نركّز على النقاط (x_1, y_1) الموجودة في $\mathcal{E}$ بحيث ان x_1 و y_1 هي قيم من $\mathbb{Z}_p$. نستخدم الرمز $\mathcal{E}(\mathbb{Z}_p)$ ليمثل مجموعة النقاط الموجودة على المنحنى التي تحقق (12.1) بالاضافة الى نقطة $\mathcal{O}$.

قانون الجمع. تعرّف عملية الجمع على $\mathcal{E}/\mathbb{Z}_p$ بالشكل التالي (مع ملاحظة ان جميع العمليات هي في الزمرة $\mathbb{Z}_p$): افترض $P = (x_1, y_1)$ ، و $Q = (x_2, y_2)$ هي نقاط في $\mathcal{E}/\mathbb{Z}_p$. عندما $x_1 = x_2$ و $y_2 = -y_1$ ، فأنه $P + Q = \mathcal{O}$ ، ما عدا ذلك $P + Q = (x_3, y_3)$ ، حيث

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

و

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, \text{if } P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1}, \text{if } P = Q \end{cases}$$

واخيرا ، نعرّف

$$P + \mathcal{O} = \mathcal{O} + P = P$$

لجميع قيم $P \in \mathcal{E}/\mathbb{Z}_p$.

- لاحظ ان عملية الجمع على $\mathcal{E}/\mathbb{Z}_p$ لايمكن رسمها وتوضيحها كما هو الحال في المنحنيات الاهليجية فوق الاعداد الحقيقية.
- على كل حال ، تعتبر $(\mathcal{E}, +)$ زمرة تبادلية.
- يتطلب الحل في المنحنيات الاهليجية حساب الجذور التربيعية.
- سوف نقدّم خوارزمية كفوءة لحساب الجذر التربيعي mod p

1.3.1 حساب الجذر التربيعي

- ليكن p هو عدد اولي فردي. يكون حساب الجذور التربيعية mod p بسيطا عندما يكون $p = 3 \bmod 4$.
- في هذه الحالة نحتاج ان نحسب الجذور التربيعية للبقية التربيعية $z \in \mathbb{Z}_p^*$. في هذه الحالة يمكن كتابة $p = 4i + 3$ لبعض قيم i.
- بما ان $z \in \mathbb{Z}_p^*$ هو بقية تربيعية ، اذن يكون لدينا $\mathcal{J}_p(z) = 1 = z^{p-1/2} \bmod p$ (راجع فرضية 11.2). عند ضرب الطرفين بـ z نحصل على

$$z = z^{\frac{p-1}{2}+1} = z^{2i+2} = (z^{i+1})^2 \bmod p$$

- وبذلك فإن $z^{i+1} = z^{p+1/4} \bmod p$ هو الجذر التربيعي الى z.
- مما يعني انه لحساب الجذور التربيعية لـ z mod p فأنه نحسب $x = z^{p+1/4} \bmod p$ ، والجذر الاخر هو $[-x \bmod p] = [p - x]$.
- **مثال**(12.1)**:** ليكن $\mathcal{E}/\mathbb{Z}_{11}$ منحنى اهليجي $y^2 = x^3 + x + 6$ فوق $\mathbb{Z}_{11}$.
- دعنا في البداية نحدد نقاط المنحنى.
- يتم هذا الامر عن طريق النظر لكل قيمة $x \in \mathbb{Z}_{11}$ وحساب $x^3 + x + 6 \bmod 11$ ، ومن ثم حل المعادلة (12.1) بالنسبة لقيمة y.

- لاي قيمة x نختبر فيما اذا كان $z = x^3 + x + 6 \bmod 11$ هو بقية تربيعية وذلك بأستخدام فرضية (11.1)، والتي تنص على انه يمكن اختبار كون العدد z بقية تربيعية في حالة mod p وذلك بحساب $\mathcal{J}_p(z)$ فإن كانت النتيجة 1 فهو بقية تربيعية.
- ذكرنا قبل قليل طريقة لحساب الجذور التربيعية للبقية التربيعية z ، فعند تطبيقها نحصل على الجذرين

$$\mp z^{\frac{11+1}{4}} \bmod 11 = \mp z^3 \bmod 11$$

يوضّح الجدول(12.1) نتائج الحسابات.

جدول (12.1): المنحنى الاهليجي $y^2 = x^3 + x + 6$ فوق $\mathbb{Z}_{11}$

x	$x^3 + x + 6 \bmod 11$	بقية تربيعية؟	y
0	6	كلا	
1	8	كلا	
2	5	نعم	4,7
3	3	نعم	5,6
4	8	كلا	
5	4	نعم	2,9
6	8	كلا	
7	4	نعم	2,9
8	9	نعم	3,8
9	7	كلا	
10	4	نعم	2,9

- تكون الزمرة $\mathcal{E}(\mathbb{Z}_{13})$ هي نقاط المنحنى الاهليجي $\mathcal{E}/\mathbb{Z}_{13}$ ، حيث ان $\left|\mathcal{E}(\mathbb{Z}_{13})\right| = 13$.
- بما ان اي الزمرة $\mathcal{E}(\mathbb{Z}_{13})$ لها رتبه اولية (عدد عناصرها اولي)، اذن تكون هذه الزمرة دورية ، وبالتالي فإن اي نقطة (ماعدا نقطة اللانهاية) هي عنصر بدائي (مولّد) للمنحنى $\mathcal{E}/\mathbb{Z}_{13}$.
- افترض اننا اخذنا المولّد $g = (2,7)$.
  - عندها سوف نحسب "قوى" هذا المولّد (وهي هنا مضاعفات g ، لان عملية الزمرة هي الجمع).
  - لحساب $2g = (2,7) + (2,7)$ ، نحسب اولا

$$\lambda = (3 \times 2^2 + 1)(2 \times 7)^{-1} \bmod 11$$

$$= 2.3^{-1} \bmod 11$$

$$= 2.4 \bmod 11$$

$$= 8.$$

وبذلك فإن $x_3 = 8^2 - 2 - 2 \bmod 11$

$$= 5$$

و $y_3 = 8(2-5) - 7 \bmod 11$

$$= 2$$

وبذلك فإن $2g = (5,2)$.

عند حساب $3g = 2g + g = (5,2) + (2,7) = (8,3)$

بقية المضاعفات نحصل عليها بتكرار نفس النمط ، حيث

$g = (2,7)$	$2g = (5,2)$	$3g = (8,3)$
$4g = (10,2)$	$5g = (3,6)$	$6g = (7,9)$
$7g = (7,2)$	$8g = (3,5)$	$9g = (10,9)$
$12g = (8,8)$	$11g = (5,9)$	$10g = (8,8)$

$$13g = \mathcal{O}$$

وبذلك نعرف بأن $g = (2,7)$ هو بالفعل مولّد (عنصر بدائي).

1.4 خصائص المنحنيات الاهليجية

نصّت نظرية Hasse على ان عدد نقاط $\left|\mathcal{E}(\mathbb{Z}_p)\right|$ تحقق ما يلي

$$p + 1 - 2\sqrt{p} \le \left|\mathcal{E}(\mathbb{Z}_p)\right| \le p + 1 + 2\sqrt{p}$$

نلاحظ ان عدد النقاط في المثال (12.1) هو تماما $p + 1$.

- هناك خوارزمية تعود الى Schoof تحسب عدد نقاط $\left|\mathcal{E}(\mathbb{Z}_p)\right|$ بصورة مضبوطة وبوقت $\log(p)$.
- من خلال نظرية Hasse نلاحظ انه للحصول على منحنى اهليجي ذو 2^{256} نقطة ، فأننا نختار عدد اولي p بطول 256 ثنائية فقط.
- عند محاولة استخدام المنحنيات الاهليجية في التشفير فأننا نحتاج الى افتراض وجود مسألة صعبة.
  - تعتبر مسألة **اللوغاريتم المتقطع** هي المسألة الصعبة في المنحنيات الاهليجية وبذلك تكون هي الافتراض الذي بصعوبته يمكن إثبات أمنية مناهج التشفير التي تعتمد على زمرة نقاط المنحنيات الاهليجية.
- ليكن لدينا النقطة P في $\mathcal{E}(\mathbb{Z}_p)$ بحيث ان رتبة هذه النقطة هي q بمعنى $qP = \mathcal{O}$.
- تعرّف مسألة اللوغاريتم المتقطع في $\mathcal{E}(\mathbb{Z}_p)$ بحساب $m \in \mathbb{Z}_p$ عند اعطاء الزوج P و $Q = mP$.

$$\underbrace{P + P + \cdots P}_{\text{m times}} = mP = Q$$

- تمثل m المفتاح الخاص.
- اما النقطة Q فهي تمثل المفتاح المعلن.
- وكما ذكرنا في بداية الفصل ، في اغلب المنحنيات الاهليجية تحتاج افضل خوارزمية لحل هذه المسألة الى وقت $\mathcal{O}(\sqrt{q})$.
- هناك استثناء وهو عندما يكون $\left|\mathcal{E}(\mathbb{Z}_p)\right| = p$ حيث تحل مسألة اللوغاريتم المتقطع بوقت ابسط.
- وللتخلص من هذه المشكلة تستخدم الكثير من التطبيقات مجموعة جاهزة من المنحنيات.
  - وهذا الاجراء يعتبر اكثر امان من توليد عدد عشوائي p وتوليد المنحنى الاهليجي فوق الزمرة $\mathbb{Z}_p$.
  - سنذكر احد تلك المنحنيات الامنة في نهاية الفصل.

بعد ان تم تأسيس صعوبة مسألة اللوغاريتم المتقطع في الزمرة $\mathcal{E}(\mathbb{Z}_p)$، فأنه من الممكن اعادة صياغة جميع مناهج التشفير التي تعتمد على صعوبة مسألة اللوغاريتم المتقطع وذلك باستخدام تلك الزمرة.

1.5 الاتفاق على المفاتيح باستخدام المنحنيات الاهليجية

في هذا الجزء سوف نرى كيفية تصميم بروتوكول الاتفاق على المفتاح اعتمادا على زمر المنحنيات الاهليجية. يعتبر هذا البروتوكول مناظرا لطريقة Diffie-Hellman.

- نحتاج في البداية الى تعريف المعلمات العامة والتي تمثل المنحنى الاهليجي والعنصر الابتدائي لذلك المنحنى.
- نختار في لبداية العدد الاولي p ونّعرف المنحنى الاهليجي

$$\mathcal{E}: y^2 = x^3 + ax + b \bmod p$$

ثم نختار العنصر البدائي $P = (x_p, y_p)$. يتم الأن وصف البروتوكول.

1. تختار Alice $a \in \{2, \dots, |\mathcal{E}(\mathbb{Z}_p)|\}$، وتحسب $A = aP$، اخيرا ترسل A الى Bob.
2. يختار Bob $b \in \{2, \dots, |\mathcal{E}(\mathbb{Z}_p)|\}$، ويحسب $B = bP$، اخيرا يرسل B الى Alice.
3. تحسب Alice المفتاح $T = aB$، وبنفس الوقت يحسب Bob نفس المفتاح $T = bA$

ويمكن اثبات صحة هذا البروتوكول بسهولة لان Alice تحسب $aB = a(bP)$، اما Bob فيحسب $bA = b(aP)$، وبما ان عملية الجمع هي عملية تجميعية فإن كلا الطرفين يحصلون على نفس المفتاح $T = abP$. دعنا نأخذ مثال بأرقام صغيرة.

مثال(12.3): افترض بروتوكول الاتفاق على المفاتيح بالمنحنيات الاهليجية بالمعلمات التالية: المنحنى الاهليجي هو

$$\mathcal{E}: y^2 = x^3 + 2x + 2 \bmod 17$$

حيث عدد نقاطه هو $|\mathcal{E}(\mathbb{Z}_{17})| = 19$. المولّد هو $P = (5,1)$. يعمل البروتوكول بالشكل التالي.

1. افترض ان Alice اختارت $a = 3$، اذن $A = 3P = (10,6)$. ترسل قيمة A الى Bob.
2. افترض ان Bob اختار $b = 10$، اذن $B = 10P = (7,11)$. يرسل قيمة B الىAlice.
3. تحسب Alice المفتاح $T = aB = 3(7,11) = (13,10)$، في نفس الوقت يحسب Bob المفتاح $T = bA = 10(10,6) = (13,10)$

- يتم عادة استخدام احد احداثيات النقطة T كمفتاح.
- في التطبيقات العملية يُنحت محور x من النقطة T باستخدام دالة نحت للحصول على المفتاح.
- على سبيل المثال ، نحت الاحداثي x باستخدام SHA3-224 يولّد مفتاح بطول 224 ثنائية.

1.6 منحنى P256

اعلنت مؤسسة NIST عام 1999 قائمة بالمنحنيات الاهليجية للاستخدامات الحكومية.

- يعتبر المنحنى P256 واحدا من اشهر هذه المنحنيات.
- ويعتبر هذا المنحنى شرط اجباري لتبادل المفاتيح ببروتوكول Difie-Hellman.
- يعرّف هذا المنحنى على العدد الاولي $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$.
- تكون صيغة المنحنى هي $y^2 = x^3 - 3x + b$ بحيث ان قيمة b بالنظام السداسي عشر هي:

$$b = \text{5ac635d8 aa3a93e7 b3ebbd55 769886bc}$$

$$\text{651d06b0 cc53b0f6 3bce3c3e 27d2604b}$$

- عدد نقاط هذا المنحنى هو العدد الاولي q. تستخدم النقطة G لتوليد الزمرة باكملها. بما ان العدد الاولي p قريب من 2^{256}، فإن عدد النقاط q يكون قريب من 2^{256}. وبالتالي فإن الحسابات المطلوبة لحل مسألة اللوغاريتم المتقطع هي تقريبا $\sqrt{q}$ وهو حوالي 2^{128}.
- يكون الهدف هنا هو ان تكون صعوبة مسألة اللوغاريتم المتقطع هي على الاقل بصعوبة AES-128. وبالتالي ، فأنه عند استخدام AES-128 لتشفير النص الصريح ، فإن P256 يمكن ان يستخدم لبروتوكول Diffie-Hellman لتبادل المفاتيح ، التشفير معلن المفتاح ، والتوقيع الرقمي.

تمارين

1. بيّن ان الشرط $4a^3 + 27b^2 \neq 0 \bmod p$ متحقق في المنحنى $y^2 = x^3 + a2 + 2 \bmod 17$.
2. اجمع كل من $(5,2) + (2,7)$ في زمرة المنحنى الاهليجي $y^2 = x^3 + 2x + 2 \bmod 17$.
3. ليكن لديك المنحنى الاهليجي $y^2 = x^3 - 2x + 4$ ولتكن $P = (0,2)$ و $Q = (3,-5)$.
   أ. اختبر ان P و Q تنتميان للمنحنى.
   ب. احسب $P + Q$ ، $P + P$ ، $Q + Q$ ، $P + P + P$ ، $Q + Q + Q$
4. هل يمثّل المنحنى الاهليجي $y^2 = x^3 + 10x + 5$ زمرة فوق $\mathbb{Z}_{17}$؟
5. اختبر صحة نظرية Hasse للمنحنى $y^2 = x^3 + 2x + 2 \bmod 17$ الذي لديه 19 نقطة.
6. ليكن لديك المنحنى الاهليجي $y^2 = x^3 + 2x + 2 \bmod 7$ على الزمرة $\mathbb{Z}_7$.
   أ. احسب جميع نقاط المنحنى.
   ب. ماهي رتبة الزمرة؟(لاتنسى نقطة الانهاية).
   ت. عندما $g = (0,3)$ ما هي رتبة g؟ وهل هو مولّد(عنصر ابتدائي)؟
7. احسب المفتاح الخاص باستخدام طريقة Diffie-Hellman للمنحنيات الاهليجية. افترض $a = 6$. مفتاح Bob المعلن هو $B = (5,9)$. يعرف المنحنى الاهليجي بالشكل $y^2 = x^3 + x + 6 \bmod 11$.