Verschlüsseln mit elliptischen Kurven

ETH unterwegs an Mittelschulen

L. Halbeisen

Cäsar Verschlüsselung

Modulorechnen (oder Rechnen mit Rest)

Modulorechnen (oder Rechnen mit Rest)

Sei q eine fest gewählte natürliche Zahl, z.B. $q = 26$.

Modulorechnen (oder Rechnen mit Rest)

Sei q eine fest gewählte natürliche Zahl, z.B. $q = 26$.
Sei a eine beliebige Zahl, z.B. $a = 60$.

Modulorechnen (oder Rechnen mit Rest)

Sei q eine fest gewählte natürliche Zahl, z.B. $q = 26$.
Sei a eine beliebige Zahl, z.B. $a = 60$.

Dann ist 60 **modulo** 26, $60 \pmod{26}$, gleich dem **Rest** der Division von $60 : 26$. Wir schreiben

$$60 \pmod{26} = 8\,.$$

Modulorechnen (oder Rechnen mit Rest)

Sei q eine fest gewählte natürliche Zahl, z.B. $q = 26$.
Sei a eine beliebige Zahl, z.B. $a = 60$.

Dann ist 60 **modulo** 26, $60 \pmod{26}$, gleich dem **Rest** der Division von $60 : 26$. Wir schreiben

$$60 \pmod{26} = 8\,.$$

Zum Beispiel ist $26 \pmod{26} = 0$ und $5 \cdot 9 \pmod{26} = 19$.

Modulorechnen (oder Rechnen mit Rest)

Sei q eine fest gewählte natürliche Zahl, z.B. $q = 26$.
Sei a eine beliebige Zahl, z.B. $a = 60$.

Dann ist 60 **modulo** 26, $60 \pmod{26}$, gleich dem **Rest** der Division von $60 : 26$. Wir schreiben

$$60 \pmod{26} = 8\,.$$

Zum Beispiel ist $26 \pmod{26} = 0$ und $5 \cdot 9 \pmod{26} = 19$.

Weiter ist

$$20 + 9 \pmod{26} = 3,$$

Modulorechnen (oder Rechnen mit Rest)

Sei q eine fest gewählte natürliche Zahl, z.B. $q = 26$.
Sei a eine beliebige Zahl, z.B. $a = 60$.

Dann ist 60 **modulo** 26, $60 \pmod{26}$, gleich dem **Rest** der Division von $60 : 26$. Wir schreiben

$$60 \pmod{26} = 8\,.$$

Zum Beispiel ist $26 \pmod{26} = 0$ und $5 \cdot 9 \pmod{26} = 19$.

Weiter ist

$$20 + 9 \pmod{26} = 3,$$

und wenn wir auf beiden Seiten 9 subtrahieren, erhalten wir

$$20 = -6 \pmod{26}.$$

Modulorechnen (oder Rechnen mit Rest)

Sei q eine fest gewählte natürliche Zahl, z.B. $q = 26$.
Sei a eine beliebige Zahl, z.B. $a = 60$.

Dann ist 60 **modulo** 26, $60 \pmod{26}$, gleich dem **Rest** der Division von $60 : 26$. Wir schreiben

$$60 \pmod{26} = 8\,.$$

Zum Beispiel ist $26 \pmod{26} = 0$ und $5 \cdot 9 \pmod{26} = 19$.

Weiter ist

$$20 + 9 \pmod{26} = 3,$$

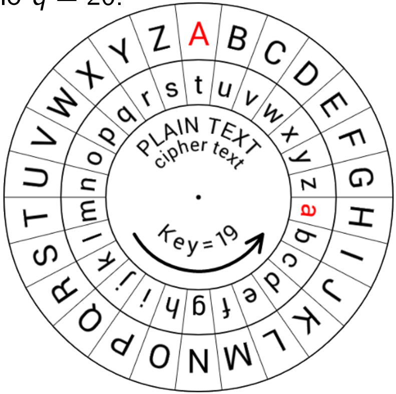
und wenn wir auf beiden Seiten 9 subtrahieren, erhalten wir

$$20 = -6 \pmod{26}.$$

Analog erhält man z.B. $-71 \pmod{26} = 7$.

Cäsarverschlüsselung

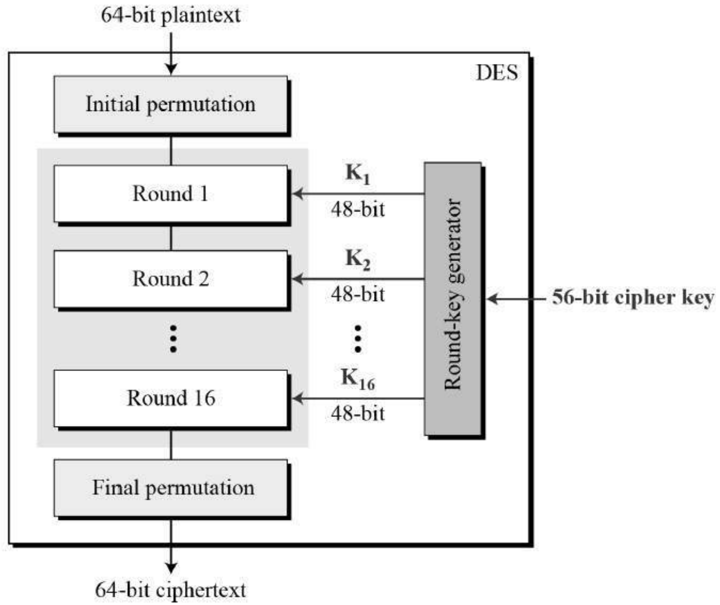
Wir nummerieren die Buchstaben A–Z mit 0–25, zählen zu jedem Buchstabenwert eine feste Zahl $s = 19$ dazu, und rechnen modulo $q = 26$.



$$H \to 7, \qquad 7 + 19 \pmod{26} = 0, \qquad \text{also } H \Rightarrow a$$
$$N \to 13, \qquad 13 + 19 \pmod{26} = 6, \qquad \text{also } N \Rightarrow g$$

Enigma

Data Encryption Standard (DES)



Diskreter Logarithmus

Diskreter Logarithmus

Für positive Zahlen a, b, n gilt:

$$a^n = b \quad \Rightarrow \quad n = \log_a(b)$$

Diskreter Logarithmus

Für positive Zahlen a, b, n gilt:

$$a^n = b \quad \Rightarrow \quad n = \log_a(b)$$

Wir können also aus a und b die Zahl n berechnen.

Diskreter Logarithmus

Für positive Zahlen a, b, n gilt:

$$a^n = b \quad \Rightarrow \quad n = \log_a(b)$$

Wir können also aus a und b die Zahl n berechnen.

Ist q irgendeine positive Zahl, zum Beispiel $q = 137$, und gilt zum Beispiel

$$2^n \pmod{137} = 101,$$

können wir dann n immer noch berechnen?

Diskreter Logarithmus

Für positive Zahlen a, b, n gilt:

$$a^n = b \quad \Rightarrow \quad n = \log_a(b)$$

Wir können also aus a und b die Zahl n berechnen.

Ist q irgendeine positive Zahl, zum Beispiel $q = 137$, und gilt zum Beispiel

$$2^n \pmod{137} = 101,$$

können wir dann n immer noch berechnen?

NEIN!

Diskreter Logarithmus

Durch ausprobieren erhält man

$$2^{77} \pmod{137} = 101.$$

Wir sagen 77 ist ein **diskreter Logarithmus** von 101.

Diskreter Logarithmus

Durch ausprobieren erhält man

$$2^{77} \pmod{137} = 101.$$

Wir sagen 77 ist ein **diskreter Logarithmus** von 101.

Modulo 137 gilt:

$$2^{77} = 101 \qquad 2^{33} = 68 \qquad 2^{33\cdot 77} = 118$$

Diskreter Logarithmus

Durch ausprobieren erhält man

$$2^{77} \pmod{137} = 101.$$

Wir sagen 77 ist ein **diskreter Logarithmus** von 101.

Modulo 137 gilt:

$$2^{77} = 101 \qquad 2^{33} = 68 \qquad 2^{33\cdot 77} = 118$$

Weil $(2^{77})^{33} = (2^{33})^{77} = 2^{33\cdot 77}$, gilt modulo 137:

$$101^{33} = 68^{77} = 2^{33\cdot 77} = 118$$

Diffie-Hellman Schlüsselaustausch

Alice und Bob wählen öffentlich

$$q = 1111111111111911111111111197$$

und eine Basis $a = 2$ für das Potenzieren.

Diffie-Hellman Schlüsselaustausch

Alice und Bob wählen öffentlich

$$q = 111111111111191111111111197$$

und eine Basis $a = 2$ für das Potenzieren.

Alice wählt geheim: $n = 77777777777777777777777$

Bob wählt geheim: $m = 33333333333333333333$

Diffie-Hellman Schlüsselaustausch

Alice und Bob wählen öffentlich

$$q = 1111111111119111111111197$$

und eine Basis $a = 2$ für das Potenzieren.

Alice wählt geheim: $n = 7777777777777777777777$

Bob wählt geheim: $m = 3333333333333333333$

Alice sendet Bob die Zahl

$$2^n \pmod{q} = 1792160008654009846128881$$

Diffie-Hellman Schlüsselaustausch

Alice und Bob wählen öffentlich

$$q = 111111111111191111111111197$$

und eine Basis $a = 2$ für das Potenzieren.

Alice wählt geheim: $n = 77777777777777777777777$

Bob wählt geheim: $m = 33333333333333333333$

Alice sendet Bob die Zahl

$$2^n \pmod{q} = 1792160008654009846128881$$

Bob sendet Alice die Zahl

$$2^m \pmod{q} = 61898758397207174475737915$$

Diffie-Hellman Schlüsselaustausch

Alice berechnet $(2^m)^n$ modulo q, also

$$61898758397207174475737915^{77777777777777777777777} \pmod{q},$$

und Bob berechnet $(2^n)^m$ modulo q, also

$$1792160008654009846128881^{33333333333333333333} \pmod{q},$$

Diffie-Hellman Schlüsselaustausch

Alice berechnet $(2^{m})^{n}$ modulo q, also

$$61898758397207174475737915^{77777777777777777777777} \pmod{q},$$

und Bob berechnet $(2^{n})^{m}$ modulo q, also

$$17921600086540098461288881^{33333333333333333333} \pmod{q},$$

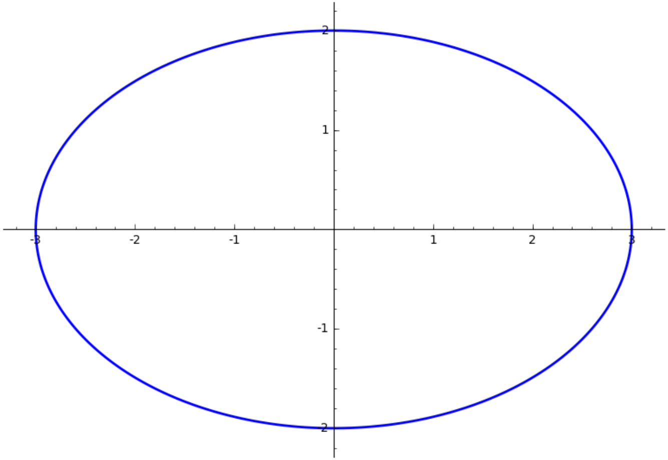
Der gemeinsame Schluessel von Alice und Bob ist:

$$(2^{m})^{n} \pmod{q} = (2^{n})^{m} \pmod{q},$$

also

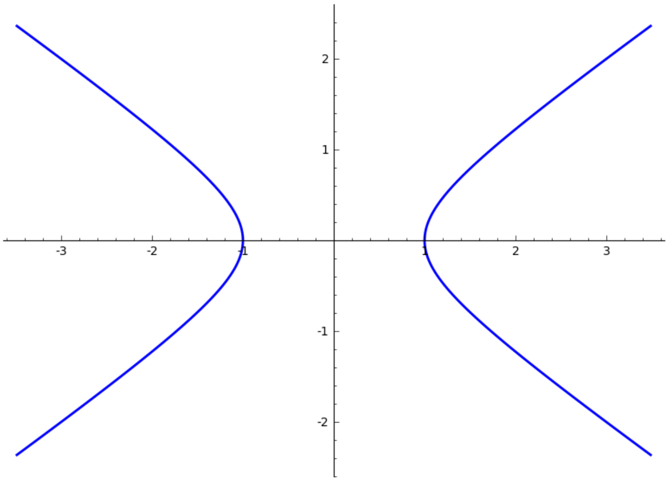
$$2^{n \cdot m} \pmod{q} = 42406702470360552326107761.$$

Ellipse



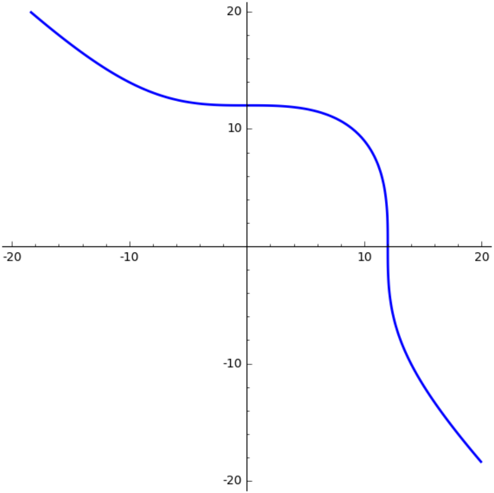
$$4x^2 + 9y^2 = 36$$

Hyperbel



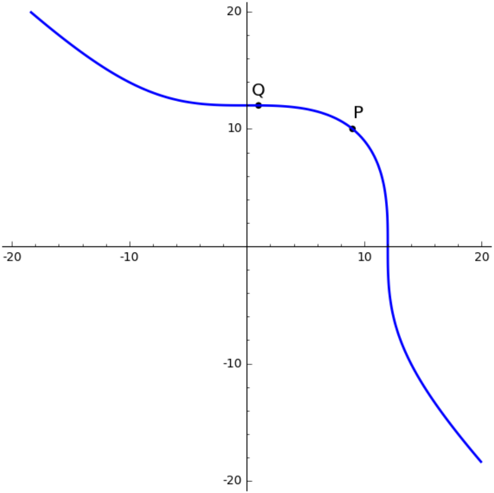
$$x^2 - 2y^2 = 1$$

Cubische oder elliptische Kurve



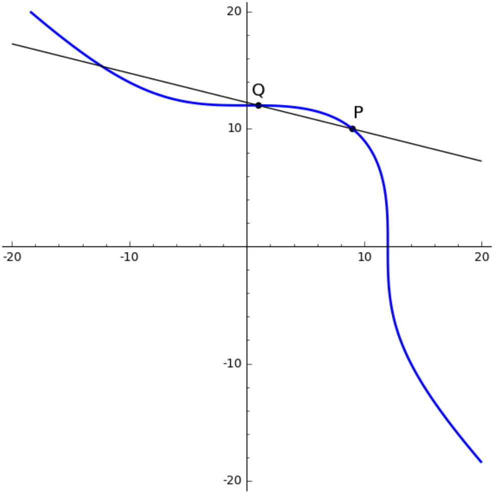
$$x^3 + y^3 = 1729$$

Addition von Punkten



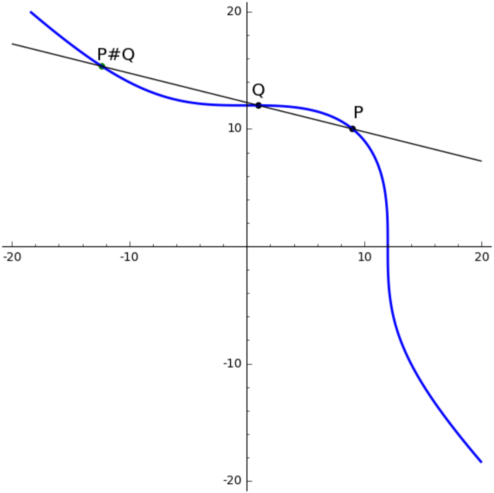
$$x^3 + y^3 = 1729$$

Addition von Punkten



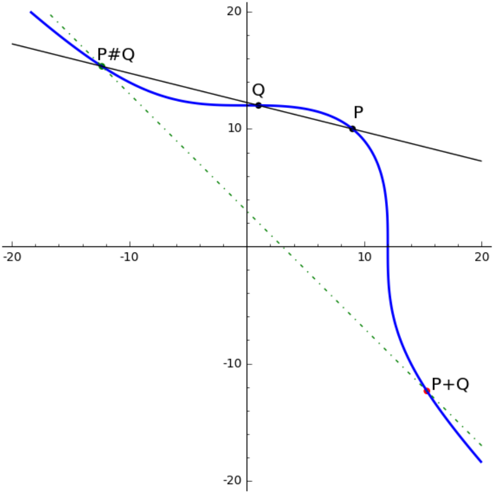
$$x^3 + y^3 = 1729$$

Addition von Punkten



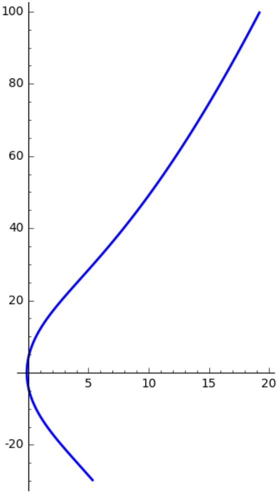
$$x^3 + y^3 = 1729$$

Addition von Punkten



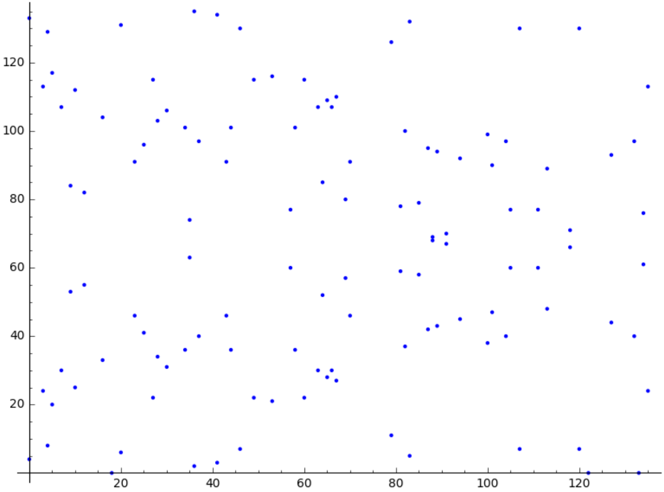
$$x^3 + y^3 = 1729$$

Elliptische Kurve

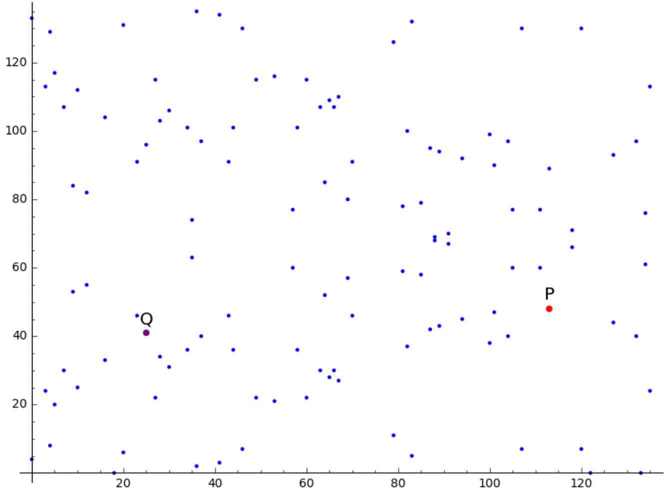


$$y^2 = x^3 + x^2 + 129x + 16$$

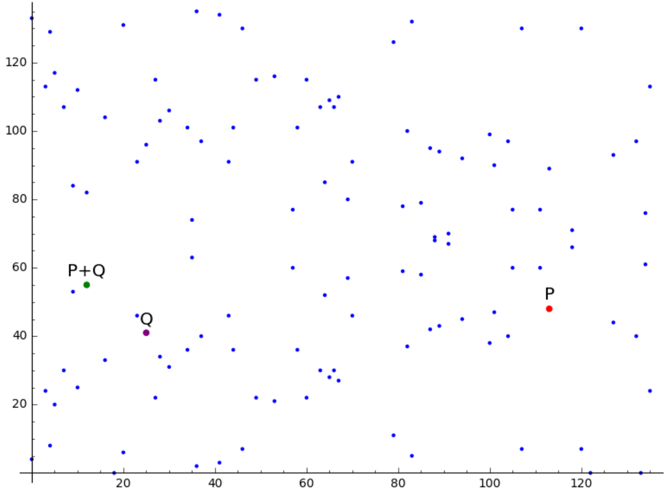
Dieselbe elliptische Kurve modulo $q = 137$



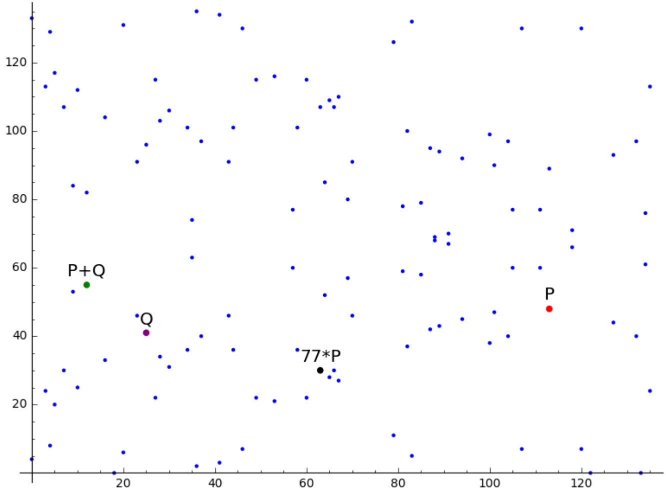
$$y^2 = x^3 + x^2 + 129x + 16 \pmod{137}$$



$$y^2 = x^3 + x^2 + 129x + 16 \pmod{137}$$



$$y^2 = x^3 + x^2 + 129x + 16 \pmod{137}$$



$$y^2 = x^3 + x^2 + 129x + 16 \pmod{137}$$

Diffie-Hellman mit elliptischen Kurven

Alice und Bob wählen öffentlich

Diffie-Hellman mit elliptischen Kurven

Alice und Bob wählen öffentlich

- eine Primzahl q,

Diffie-Hellman mit elliptischen Kurven

Alice und Bob wählen öffentlich

- eine Primzahl q,
- eine elliptische Kurve $E \pmod{q}$,

Diffie-Hellman mit elliptischen Kurven

Alice und Bob wählen öffentlich

- eine Primzahl q,
- eine elliptische Kurve $E \pmod{q}$,
- und einen Punkt $P = (x, y)$ auf der Kurve E.

Diffie-Hellman mit elliptischen Kurven

Alice und Bob wählen öffentlich

- eine Primzahl q,
- eine elliptische Kurve $E \pmod{q}$,
- und einen Punkt $P = (x, y)$ auf der Kurve E.

Geheim wählt

- Alice eine Zahl n,
- und Bob eine Zahl m.

Diffie-Hellman mit elliptischen Kurven

Alice und Bob wählen öffentlich

- eine Primzahl q,
- eine elliptische Kurve $E \pmod{q}$,
- und einen Punkt $P = (x, y)$ auf der Kurve E.

Geheim wählt

- Alice eine Zahl n,
- und Bob eine Zahl m.

Anschliessend sendet Alice an Bob den Punkt

$$n \cdot P = (x_n, y_n),$$

und Bob sendet Alice den Punkt

$$m \cdot P = (x_m, y_m).$$

Diffie-Hellman mit elliptischen Kurven

Nun berechnet

- Alice den Punkt

$$n \cdot (m \cdot P) = n \cdot (x_m, y_m),$$

- und Bob den Punkt

$$m \cdot (n \cdot P) = m \cdot (x_n, y_n).$$

Diffie-Hellman mit elliptischen Kurven

Nun berechnet

- Alice den Punkt

$$n \cdot (m \cdot P) = n \cdot (x_m, y_m),$$

- und Bob den Punkt

$$m \cdot (n \cdot P) = m \cdot (x_n, y_n).$$

Das heisst, beide berechnen den Punkt

$$(n \cdot m) \cdot P = (x_{nm}, y_{nm}),$$

und x_{nm} ist der gemeinsame Schlüssel von Alice und Bob.

Diffie-Hellman mit elliptischen Kurven

Alice und Bob wählen öffentlich die Primzahl

$$q = 1111111111111911111111111197,$$

die elliptische Kurve

$$E: \; y^2 = x^3 - 9x + 17 \pmod{q},$$

und den Punkt

$$P = (16, 63)$$

auf der Kurve E.

Diffie-Hellman mit elliptischen Kurven

Alice und Bob wählen öffentlich die Primzahl

$$q = 111111111111191111111111197,$$

die elliptische Kurve

$$E: \; y^2 = x^3 - 9x + 17 \pmod{q},$$

und den Punkt

$$P = (16, 63)$$

auf der Kurve E.

Alice wählt geheim: $n = 77777777777777777777777$

Bob wählt geheim: $m = 33333333333333333333$

Diffie-Hellman mit elliptischen Kurven

Alice sendet Bob den Punkt

$$n \cdot P = (407592870394917149487052227,\\ 581650276074904700847890063)$$

Bob sendet Alice den Punkt

$$m \cdot P = (125084664163780288152224951,\\ 289328246710449638814489 37)$$

Diffie-Hellman mit elliptischen Kurven

Alice sendet Bob den Punkt

$$n \cdot P = (40759287039491714948705227, 58165027607490470084789063)$$

Bob sendet Alice den Punkt

$$m \cdot P = (12508466416378028815224951, 28932824671044963881448937)$$

Alice berechnet $n \cdot (m \cdot P)$ und Bob berechnet $m \cdot (n \cdot P)$, das heisst beide berechnen

$$(n \cdot m) \cdot P = (99109872087352514342446926, 104339393474553694544327134)$$

Diffie-Hellman mit elliptischen Kurven

Die elliptische Kurve secp256k1, die für Bitcoins verwendet wird:

Alice und Bob wählen öffentlich die Primzahl

$$q = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1,$$

$(q = 115792089237316195423570985008687907853269984665640564039457584007908834671663)$

Diffie-Hellman mit elliptischen Kurven

Die elliptische Kurve secp256k1, die für Bitcoins verwendet wird:

Alice und Bob wählen öffentlich die Primzahl

$$q = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1,$$

$(q = 115792089237316195423570985008687907853269984665640564039457584007908834671663)$

die elliptische Kurve $E: \ y^2 = x^3 + 7 \pmod{q}$,

Diffie-Hellman mit elliptischen Kurven

Die elliptische Kurve secp256k1, die für Bitcoins verwendet wird:

Alice und Bob wählen öffentlich die Primzahl

$$q = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1,$$

$(q = 115792089237316195423570985008687907853269984665640564039457584007908834671663)$

die elliptische Kurve $E: \ y^2 = x^3 + 7 \pmod{q}$,
und den Punkt $P = (x_0, y_0)$ auf der Kurve E, wobei

Diffie-Hellman mit elliptischen Kurven

Die elliptische Kurve secp256k1, die für Bitcoins verwendet wird:

Alice und Bob wählen öffentlich die Primzahl

$$q = 2^{256} - 2^{32} - 2^{9} - 2^{8} - 2^{7} - 2^{6} - 2^{4} - 1,$$

$(q = 115792089237316195423570985008687907853269984665640564039457584007908834671663)$

die elliptische Kurve $E: \; y^2 = x^3 + 7 \pmod{q}$,
und den Punkt $P = (x_0, y_0)$ auf der Kurve E, wobei

$$x_0 = 55066263022277343669578718895168534326250603453777594175500187360389116729240$$

und

$$y_0 = 32670510020758816978083085130507043184471273380659243275938904335757337482424$$

obxexgwtgdynxkbakxtnyfxkdltfdxbm