ELLIPTIKUS GÖRBÉK

Definíció. Legyen P egy pont egy elliptikus görbén. Azt a legkisebb N számot, melyre $NP = 0$ a P pont *rendjének* nevezzük.

Megjegyzés.

(1) Gyakori kérdés, hogy találjunk egy véges rendű pontot egy elliptikus görbén.

(2) A továbbiakban legyen F_q egy véges test, ahol $q = p^r$. Legyen E egy elliptikus görbe F_q fölött. Belátható, hogy a görbén legfeljebb $2q + 1$ F_q pont létezik.

Tétel. (Hasse) Legyen N az F_q pontok száma egy F_q fölötti E elliptikus görbén. Ekkor

$$|N - (q + 1)| \leq 2\sqrt{q}.$$

Tétel. Legyen E az F_q test fölött értelmezett elliptikus görbe (Weierstrass egyenletével adott). Adott $P \in E$ esetén a kP pont koordinátáinak a kiszámításához $O(\log k \log^3 q)$ bitoperáció szükséges.

Definíció. Legyen E egy F_q test feletti elliptikus görbe és B egy pont a görbén. Ekkor az E-n értelmezett *diszkrét logaritmusos* problémáról beszélünk (a B alapra vonatkozóan), ha adott egy $P \in E$ pont és keressük azt az x egész számot, melyre $xB = P$ egyenlőség teljesül (ha ilyen x létezik).

Diffie-Helman kulcsmegosztás

(1) A és B nyilvánosan választ egy F_q testet és egy a test felett értelmezett E elliptikus görbét.

(2) Nyilvánosan választanak egy $B \in E$ pontot (ez szolgál alapul).

(3) A választ egy a egészet és kiszámolja $aB \in E$ pontot, amely publikus.

(4) B választ egy b egészet és kiszámolja $bB \in E$ pontot, amely publikus.

(5) A közös titkos kulcs, amelyet használnak $abB \in E$ pont, melyet mindketten ki tudnak számolni.

ElGamal kulcsmegosztás

(1) A és B nyilvánosan választ egy F_q testet és egy a test felett értelmezett E elliptikus görbét.

(2) Nyilvánosan választanak egy $B \in E$ pontot (ez szolgál alapul).

(3) Mindketten választanak egy a egész számot, legyenek ezek rendre a_A,illetve a_B, majd az aB szorzatot publikálják.

(4) A választ egy tetszőleges k egész számot és elküldi B-nek a

$$(kB, P_m + k(a_B B))$$

párt, ahol P_m az üzenet, a_B a B kulcsa.

(5) B olvassa az üzenetet:

$$P_m + k(a_B B) - a_B(kB) = P_m.$$

ELLIPTIKUS GÖRBE FAKTORIZÁCIÓ

Tétel. Legyen adva egy E elliptikus görbe az $y^2 = x^3 + ax + b$ egyenlettel, ahol a és b egészek és $(4a^3 + 27b^2, n) = 1$. Legyen P_1 és P_2 két olyan pont az elliptikus görbén, melynek a nevezői relatív prímek n-el és $P_1 \neq -P_2$. Ekkor a $P_1 + P_2 \in E$ pont koordinátáinak nevezői akkor és csak akkor relatív prímek n-el ha nem létezik olyan p prím, melyre $p|n$ és teljesül rá, hogy a $P_1 \, mod \, p$ és $P_2 \, mod \, p$ pontok összege az $E \, mod \, p$ elliptikus görbén az $O \, mod \, p \in E \, mod \, p$ végtelen távoli pontot adja.