ECDH Diffie-Hellman

Připomínka

A zná x —(pošle x-násobek)→ } Oba znají

B zná y —(pošle y-násobek)→ } xy-násobek

Násobek se uskutečňuje v nějaké grupě G

grupa G je vybavená generátorem g nebo P (α)

multiplikativní notace g^x

aditivní notace $[x]P$ $[x]\alpha$

Vel. kryptografie je DLP otázka efektivní „dělení"

$Q = [x]P \xrightarrow{?}$ urči x ze znalosti Q a P

A i B mají společné (C, P)

A si vybere křivku d_A $\quad A \xrightarrow{[d_A]P} B : [d_B][d_A]P$

B si vybere křivku d_B $\quad B \xrightarrow{[d_B]P} A : [d_A][d_B]P$

Oba mají $d_A d_B P$, což je součet

$d_A d_B = d_B d_A$ regulární

$[d_A d_B](P) = (\xi, \eta)$ ZA KLÍČ SE BERE POUZE ξ

Symetrické	RSA a Diffie-Hellman	ECC	
80	1024	160	dobrá
112	2048	224	
128	3072	256	
192	7680	384	
256	15360	521	

Elgamal kryptosystém

Alice (C, P, Q) $\quad Q = [x]P$ $\quad x$ tajemství

Bob zvolí y náhodně a pošle $[y]Q$

Dva zprávy $[xy]P$, a to se používá pro dešifrování

Vložíme zprávu m pošle Bob jako

$P_m \oplus [y]Q$, kde P_m bod který odpovídá m

Dešifrování $\quad P_m \oplus [y]Q = P_m \oplus [xy]P$

$P_m = (P_m + [y]Q) \ominus [y]Q$

Alice zná $[xy]P$

$= [x][y]P$

Alice zná

ECDSA Elliptic curve digital signature algorithm

Alice zveřejňuje (C, p, P, Q, g) $g: C \to \mathbb{Z}$

p řád cyklické grupy generované P

$Q = [x]P$ x tajemství Alice

Alice podepisuje, Bob ověřuje

$m \in \mathbb{Z}$ vygeneruje náhodné y, $1 \leq y < p$

počítá se $(m, [y]P, y^{-1}(m + x g([y]P)) \bmod p)$

Ověření: (a) $= m(y^{-1}(m + x g([y]P))^{-1} \bmod p$

$y \cdot \frac{m}{m + x g([y]P)}$ (b) $= g([y]P)(y^{-1}(m + x g([y]P))^{-1} = y \frac{g([y]P)}{m + x(g([y]P))}$

$[a + xb]P = [c]P$

$[a]P + [b][x]P = [a]P + [b]Q$