Asymetrická kryptografie

Matěj Novotný

19.3.2012

Obecně

- Šifrování a dešifrování probíhá jiným klíčem
- Veřejný + soukromý klíč, dva soukromé klíče
- RSA, ElGamal, D-H, DSA

RSA

- 1978 na MIT
- Ron Rivest
- Adi Shamir
- Leonard Adleman

RSA princip

- Neexistuje algoritmus na polynomiální faktorizaci
- Veřejný klíč na šifrování
- Soukromý klíč na dešifrování

RSA tvorba klíčů

- Volíme náhodná, velká prvočísla p, q
- Modul $n = pq$
- Eulerova funkce $\phi(n) = (p-1)(q-1)$
- Volíme $1 < e < \phi(n)$, nesoudělné s $\phi(n)$
- Nalezneme d tak, že $de \bmod \phi(n) = 1$
- Veřejný klíč (n,e)
- Soukromý klíč (n,d)

RSA šifrování

- Zprávu převedeme na číslo m, $m < n$
- Šifrování $c = m^e \ mod \ n$

RSA dešifrování

- Dešifrování $m = c^d \ mod \ n$

- $c^d = (m^e)^d = m^{ed} \ (mod \ n)$

$ed = 1 \ (mod \ p\text{-}1), \ ed = 1 \ (mod \ q\text{-}1)$

z malé Fermatovy věty $m^{ed} = m \ (mod \ p), \ m^{ed} = m \ (mod \ q)$

p, q různá prvočísla $\Rightarrow m^{ed} = m \ (mod \ pq)$

$\Rightarrow c^d = m \ mod \ n$

RSA příklad

- $p = 61, q = 53$
- $n = 3233$
- $e = 17$
- $d = 2753$
- $zašifruj(117) = 2160$
- $dešifruj(855) = 123$

RSA použití

- SSH
- SLL
- digitální podpis

ElGamal

- Založený na problému diskrétního logaritmu na cyklické multiplikativní grupě
- Zašifrovaná zpráva má dvojnásobnou délku
- Taher ElGamal 1984

ElGamal tvorba klíče

- Multiplikativní cyklická grupa G řádu q, s generátorem g
- Náhodné x, $0 \leqq x \leqq q - 1$
- Vypočtené $h = g^x$
- Veřejný klíč (G, q, g, h)
- soukromý klíč x

ElGamal šifrování

- Náhodné y, $0 \leqq y \leqq q - 1$
- $c_1 = g^y$
- Sdílené tajemství $s = h^y$
- Převod zprávy m do $m' \in G$
- $c_2 = m' \,.\, s$
- Odesílá se (c_1, c_2)

ElGamal Dešifrování

- Sdílené tajemství $s = c_1^x$
- $m' = c_2 \cdot s^{-1}$
- Převod m' zpátky na m

Diffie-Hellman

- Protokol pro výměnu klíčů
- Whitefield Diffie, Martin Hellman 1976
- Umožňuje komunikaci dvou neznámých účastníků na nechráněném kanálu
- Není odolná na útok *Man in the middle*

D-H výměna klíčů

- Zveřejnění prvočísla p, grupy G s generátorem g
- První zvolí soukromý klíč a a zveřejní veřejný $A = g^a \ mod \ p$
- Druhý zvolí soukromý klíč b a zveřejní veřejný $B = g^b \ mod \ p$
- První spočte veřejné tajemství $s = B^a \ mod \ p$
- Druhý spočte veřejné tajemství $s' = A^b \ mod \ p$
- $s = s'$