Public Key Cryptography

RSA

1. generování klíče
   - Bob generuje velká $p, q \in \mathbb{P}$, $n := pq$ ... *modul RSA*
   - zvolí $1 < e < \varphi(n) = (p-1)(q-1)$ a $\gcd(e, \varphi(n)) = 1$
   - Eukleidovým algoritmem najde jediné $1 < d < \varphi(n)$... *soukromý klíč*

     $$ed \equiv 1 \mod \varphi(n)$$

   - zveřejní (n, e) ... *veřejný klíč*
2. šifrování
   - Alice vyhledá v databázi Bobův klíč (n, e)
   - zašifruje $m < n$ a $\gcd(m, n) = 1$
   - odešle

     $$c \equiv m^e \mod n$$

     (spočte pomocí "square and multiply")
3. dešifrování
   - Bob spočte

     $$m \equiv c^d \mod n$$

ElGamal

1. generování klíče
   - Bob generuje velké $p \in \mathbb{P}$ a najde g generátor $\mathbb{Z}_p^*$
   - zvolí $x \in \{1, 2, \ldots, p-2\}$... *soukromý klíč*
   - spočte

     $$y = g^x \mod p$$

   - zveřejní (p, g, y) ... *veřejný klíč*
2. šifrování
   - Alice vyhledá v databázi Bobův klíč (p, g, y)
   - zašifruje $m < p$
   - bere náhodné $k \in \mathbb{N}$, $\gcd(k, p-1) = 1$
   - odešle (a, b), kde

     $$\begin{aligned} a &\equiv g^k \mod p \\ b &\equiv my^k \mod p \end{aligned}$$

3. dešifrování
   - Bob spočte

     $$m \equiv ba^{-x} \mod p$$

Diffie-Hellmanova výměna klíčů

nechť $p \in \mathbb{P}$ a a primitivní kořen modulo p

1. generování klíče uživatelem A
   - vybere $x_A < p$ ... uchová v tajnosti
   - spočte
   $$y_A = a^{x_A} \mod p$$
2. generování klíče uživatelem B
   - vybere $x_B < p$ ... uchová v tajnosti
   - spočte
   $$y_B = a^{x_B} \mod p$$
3. výměna klíče
   - uživatel A odešle y_A a uživatel B spočte $k = y_A^{x_B} \mod p$
   - uživatel B odešle y_B a uživatel A spočte $k = y_B^{x_A} \mod p$
   - uživatelé pak sdílí klíč k a mohou používat symetrickou kryptografii (DES, AES, ...)

Baby-step-giant-step (cryptoanalysis of DLP)

nechť $p \in \mathbb{P}$, g generátor $\mathbb{Z}_p^*$ a $y = g^x \mod p$, hledáme x

1. **baby step**:
   - $M := \lceil \sqrt{p} \rceil$
   - for $j = 0$ to $M - 1$ spočti $g^j \mod p$ a ulož $(j, g^j \mod p)$
2. **giant step**
   - $A := g^{-M} \mod p$, $B := y$
   - for $i = 0$ to $M - 1$ do
     - je-li $B = g^j \mod p$ ze seznamu, pak hledané $x = iM + j$
     - jinak $B = B \cdot A \mod p$