

RSA

L'ubomíra Balková

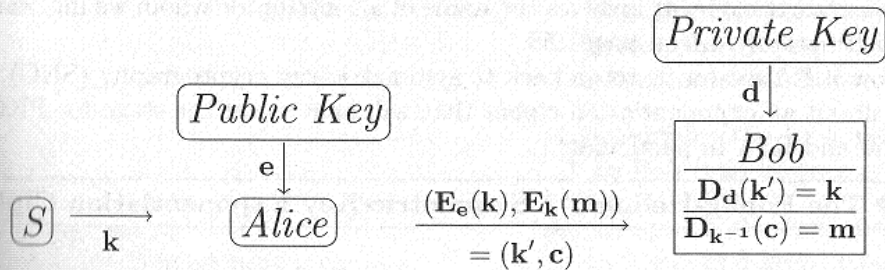
Úvod do kryptologie

15. dubna 2010

PKC Public Key Cryptography × SKC Secret Key Cryptography

- jen příjemce tajný soukromý klíč × příjemce a odesílatel sdílí tajný klíč
- pro komunikaci n osob stačí n klíčů × každý odesílatel $n - 1$ klíčů
- výpočetní náročnost: RSA 1000krát pomalejší než DES
- velikost klíčů RSA 1024 bitů, DES 64 bitů
- délka života klíčů: RSA opakované užití, DES jednorázové
- užití pro výměnu tajných klíčů symetrické kryptografie: *hybridní kryptosystémy*

Diagram 4.2 Digital Envelope — Hybrid Cryptosystem



- 1978 - Rivest, Shamir, Adleman: *A method for obtaining digital signatures and public-key cryptosystems*

- 1978 - Rivest, Shamir, Adleman: *A method for obtaining digital signatures and public-key cryptosystems*
- šifra založena na Eulerově-Fermatově větě: Necht' $a, n \in \mathbb{N}$, pak

$$a^{\varphi(n)} \equiv 1 \pmod{n} \Leftrightarrow \gcd(a, n) = 1.$$

- 1978 - Rivest, Shamir, Adleman: *A method for obtaining digital signatures and public-key cryptosystems*
- šifra založena na Eulerově-Fermatově větě: Necht' $a, n \in \mathbb{N}$, pak

$$a^{\varphi(n)} \equiv 1 \pmod{n} \Leftrightarrow \gcd(a, n) = 1.$$

- Alice a Bob

- 1978 - Rivest, Shamir, Adleman: *A method for obtaining digital signatures and public-key cryptosystems*
- šifra založena na Eulerově-Fermatově větě: Necht' $a, n \in \mathbb{N}$, pak

$$a^{\varphi(n)} \equiv 1 \pmod{n} \Leftrightarrow \gcd(a, n) = 1.$$

- Alice a Bob
- princip asymetrické kryptografie: Bob vlastní trezor, který je otevřený,

- 1978 - Rivest, Shamir, Adleman: *A method for obtaining digital signatures and public-key cryptosystems*
- šifra založena na Eulerově-Fermatově větě: Necht' $a, n \in \mathbb{N}$, pak

$$a^{\varphi(n)} \equiv 1 \pmod{n} \Leftrightarrow \gcd(a, n) = 1.$$

- Alice a Bob
- princip asymetrické kryptografie: Bob vlastní trezor, který je otevřený, Alice (stejně jako každý jiný) v něm může nechat zprávu a zaklapnout dvířka,

- 1978 - Rivest, Shamir, Adleman: *A method for obtaining digital signatures and public-key cryptosystems*
- šifra založena na Eulerově-Fermatově větě: Necht' $a, n \in \mathbb{N}$, pak

$$a^{\varphi(n)} \equiv 1 \pmod{n} \iff \gcd(a, n) = 1.$$

- Alice a Bob
- princip asymetrické kryptografie: Bob vlastní trezor, který je otevřený, Alice (stejně jako každý jiný) v něm může nechat zprávu a zaklapnout dvířka, ta otevře jen Bob - jediný vlastník klíče

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*

$$ed \equiv 1 \pmod{\varphi(n)}$$

- ▶ zveřejní (n, e) ... *veřejný klíč*

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*

$$ed \equiv 1 \pmod{\varphi(n)}$$

- ▶ zveřejní (n, e) ... *veřejný klíč*

2 šifrování

- ▶ Alice odesílá $m < n$ a $\gcd(m, n) = 1$
- ▶ vyhledá v databázi Bobův klíč (n, e) a odešle

$$c \equiv m^e \pmod{n}$$

(spočte pomocí “square and multiply”)

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*

$$ed \equiv 1 \pmod{\varphi(n)}$$

- ▶ zveřejní (n, e) ... *veřejný klíč*

2 šifrování

- ▶ Alice odesílá $m < n$ a $\gcd(m, n) = 1$
- ▶ vyhledá v databázi Bobův klíč (n, e) a odešle

$$c \equiv m^e \pmod{n}$$

(spočte pomocí “square and multiply”)

3 dešifrování

- ▶ Bob spočte

$$m \equiv c^d \pmod{n}$$

Kryptoanalýza je stejně obtížná jako prvočíselná faktorizace, tj. výpočet d je stejně obtížný jako faktorizace $n = pq$.

- ze znalosti $n = pq$ lze spočítat d
- jediný známý algoritmus pro hledání d z $ed \equiv 1 \pmod{\varphi(n)}$ je Eukleidův, a k tomu je třeba znát $\varphi(n) = (p-1)(q-1)$, a tedy $n = pq$
- ze znalosti n a $\varphi(n)$ lze určit p, q

$$p + q = n - \varphi(n) + 1, \quad p - q = \sqrt{(p + q)^2 - 4n}$$

- délka bloku
 - ▶ $m < n$ (jinak ztracena info mod n)
 - ▶ najdeme l : $2^l < n < 2^{l+1}$
 - ▶ sekáme m na bloky délky l , poslední případně doplníme nulami
- velikost modulu 1024 až 4096 bitů
 - ▶ RSA challenge number - moduly, na jejichž faktorizaci vypsána odměna
 - ▶ challenge-rsa-list@rsa.com

Čeho se vyvarovat:

- p, q blízko sebe, tj. $\frac{p+q}{2}$ o málo $> \sqrt{n}$



$$\left(\frac{p+q}{2}\right)^2 - n = \left(\frac{p-q}{2}\right)^2$$

- ▶ $x > \sqrt{n}, x \in \mathbb{N}$, dokud neplatí $x^2 - n = y^2$
- ▶ pak $n = (x - y)(x + y)$

Example

$n = 14755801$, pak $\lfloor \sqrt{n} \rfloor = 3841$, testujeme 3842, 3843, 3844, pro 3845 máme $3845^2 - 14755801 = 168^2$, a tedy $n = (3845 - 168)(3845 + 168) = 3677 \cdot 4013$.

Čeho se vyvarovat:

- velký $\gcd(p - 1, q - 1)$
 - ▶ stačí najít d tak, že $ed \equiv 1 \pmod{\text{lcm}(p - 1, q - 1)}$

Example

$p = 23, q = 67, e = 5$, pak $22 = \gcd(p - 1, q - 1)$, stačí najít d tak, že

$$5d \equiv 1 \pmod{66},$$

a tedy $d = 53$.

Řešení problému: volit p, q tak, aby $\frac{p-1}{2}, \frac{q-1}{2} \in \mathbb{P}$ (tzv. *safe primes*)

Čeho se vyvarovat:

- $e = \varphi(n)/2 + 1$

Čeho se vyvarovat:

- $e = \varphi(n)/2 + 1$

Běžná volba: $e = 65537$, elektronické platební karty $e = 3$

- výhoda - rychlé šifrování a ověřování podpisu
- nevýhoda - útok na zprávy bez formátování

- útočník zachytí $c_1 \equiv m^3 \pmod{n_1}$, $c_2 \equiv m^3 \pmod{n_2}$, $c_3 \equiv m^3 \pmod{n_3}$, z čínské zbytkové věty spočte

$$c \equiv m^3 \pmod{n_1 n_2 n_3} = m^3$$

- útočník zachytí $c_1 \equiv m^3 \pmod{n_1}$, $c_2 \equiv m^3 \pmod{n_2}$, $c_3 \equiv m^3 \pmod{n_3}$, z čínské zbytkové věty spočte

$$c \equiv m^3 \pmod{n_1 n_2 n_3 = m^3}$$

- Coppersmithův algoritmus: umí najít kořeny $m < n^{1/3}$ pro

$$p(x) = (x^3 - c) \pmod{n},$$

tedy pro $n = 1024$ bitů lze luštit zprávy délky 341 bitů

- kódovací a dekódovací transformace ψ a ψ^{-1}
- šifrování: $m = \psi(M)$, $c \equiv m^e \pmod n$
- dešifrování: $m \equiv c^d \pmod n$, $M = \psi^{-1}(m)$
- mezinárodní standard *PKCS#1*
 - ▶ pro šifrování: EME-PKCS1-v1.5 ($\psi(M) = 00\|02\|PS\|00\|M$), EME-OAEP
 - ▶ pro podpis: EMSA-PKCS1-v1.5 ($\psi(M) = 00\|01\|FF \dots FF\|00\|ID_h\|h(M)$), EMSA-PSS

Mallory "hraje" Boba

- Bob posílá veřejný klíč (n, e) Alici
- zachytí jej Mallory a pošle Alici klíč (n', e')
- Alice pošle Bobovi $c' = m^{e'} \pmod{n'}$
- Mallory přečte $m = c'^{d'} \pmod{n'}$
- Bobovi pošle $m^e \pmod{n}$
- Bob ani Alice nic netuší

Alice podepíše m a Bob podpis ověří:

- podepisovací fáze
 - ▶ Alice spočte $s \equiv m^d \pmod n$ a pošle Bobovi
- ověřovací fáze
 - ▶ Bob obdrží veřejný klíč Alice (n, e) a podpis s
 - ▶ spočte $m \equiv s^e \pmod n$