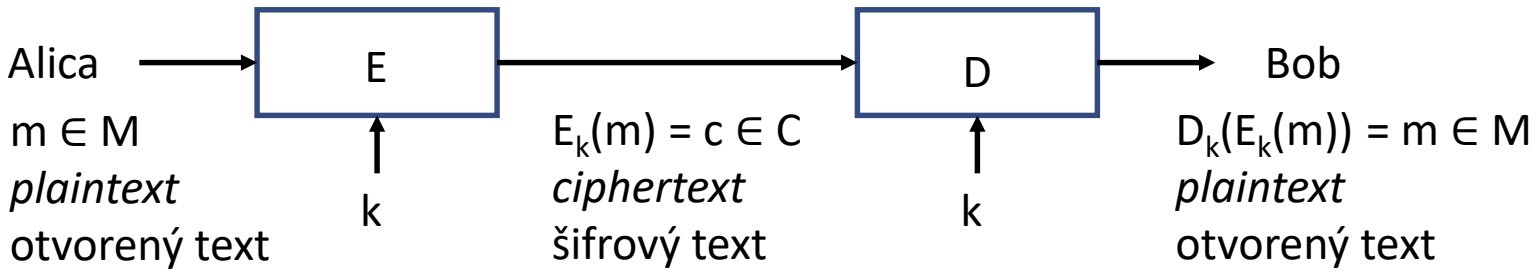
Kryptografické systémy
Asymetrická kryptografia

doc. RNDr. Jozef Jirásek, PhD.

ZS 2023

Kryptografické systémy s tajným kľúčom



k – tajný kľúč (secret key) Boba a Alice
problémy s bezpečným prenosom kľúča k adresátovi správy

rozdelenie tajného kľúča :

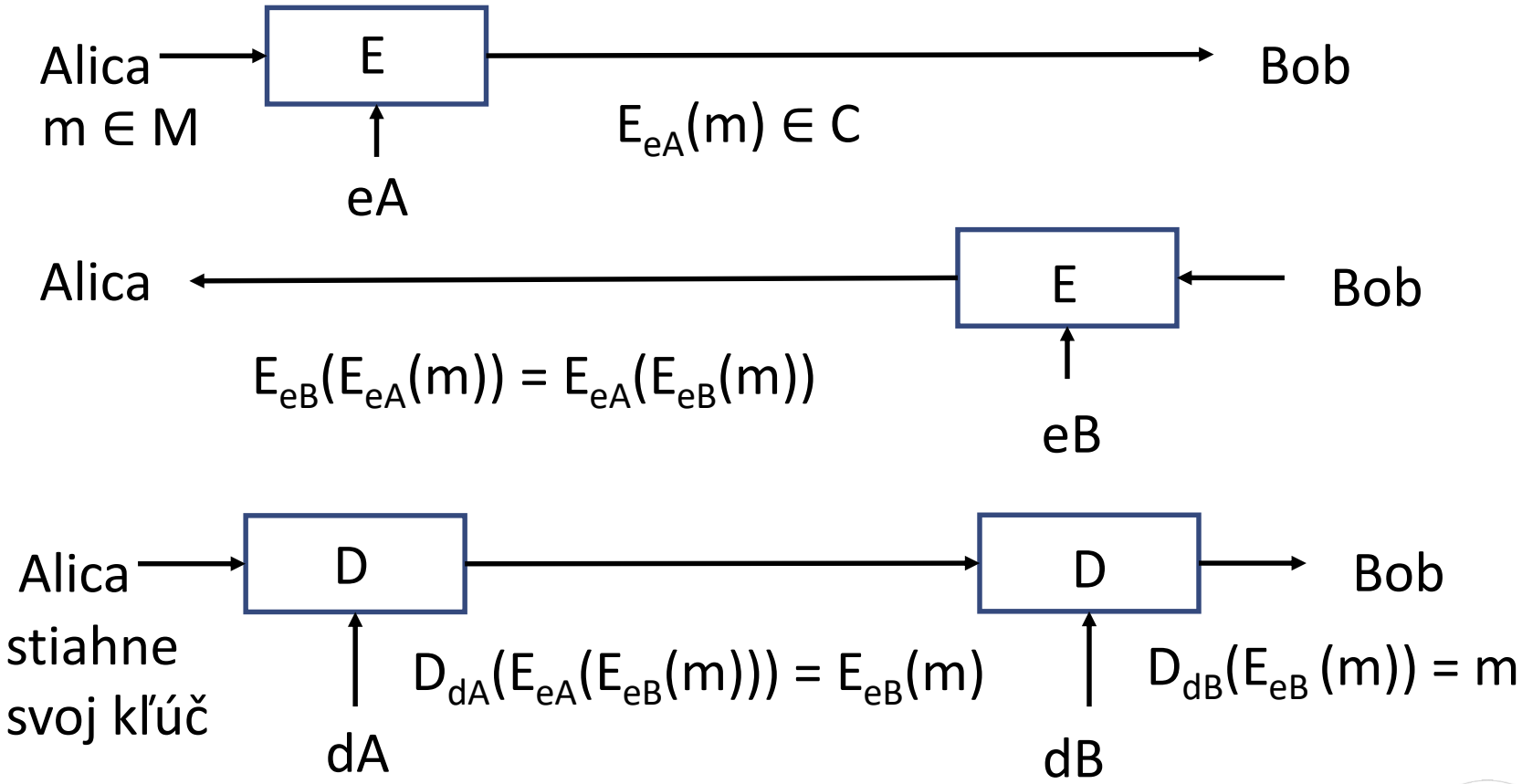
e – šifrovací kľúč

d – dešifrovací kľúč

$$D_d(E_e(m)) = m$$

Alica – eA, dA Bob – eB, dB všetky kľúče **tajné**

Utajenie správy bez prenosu tajného kľúča



predpoklady pre prenos s deleným kľúčom

- z odpočutia $E_{eA}(m)$ je ťažké zistiť m - (výpočet je dokázateľne algoritmicky zložitý) jednocestná resp. jednosmerná funkcia (one-way)
- ak poznám dA, možno vypočítať $D_{dA}(E_{eA}(m)) = m$ existujú „zadné vrátka“ (trapdoor)
- $E_{eB}(E_{eA}(m)) = E_{eA}(E_{eB}(m))$ šifrovanie je komutatívne (možno vymeniť poradie kľúčov)

Jednocestná funkcia – rýchly výpočet

- jednoducho vypočítateľná ale ťažko invertovateľná

$E: x \rightarrow x^e \bmod n \quad (x < n)$

k	$3^k \bmod 263$
2	9
$2 \cdot 2 = 4$	$9 \cdot 9 = 81$
8	$6561 \equiv 249$
16	196
32	18
64	61
128	39

$3^{165} \bmod 263$

$3^{165} = 3^{128+32+4+1}$

$\equiv 39 \cdot 18 \cdot 81 \cdot 3$

$\equiv 162 \pmod{263}$

modulárne umocňovanie

```
y = 1; while (e > 0)
    { if lsb(e) = 1 then y = (y * x) mod n endif; x = x^2 mod n; e = shr(e) };
return (y)
```

Zadné vrátka - ?

- jednoducho vypočítateľná ale ťažko invertovateľná

  E: $x \rightarrow x^e \bmod n \quad (x < n)$

  D: $x^e \bmod n \rightarrow x \quad ?$

- nájsť také d, aby $(x^e \bmod n)^d \bmod n = x$
  (postupným násobením a modulovaním sa dostať k x)

  teda $(162)^d \equiv (x^{165})^d \equiv x^{165 \cdot d} \equiv x^1 \pmod{263}$

Zadné vrátka – FLT (Fermat's little theorem)

- E: $x \rightarrow x^e \bmod n \quad (x < n) \qquad x^e \bmod n \rightarrow x$?
- nájsť také d, aby $(x^e \bmod n)^d \bmod n = x$

teda $(162)^d \equiv (x^{165})^d \equiv x^{165 \cdot d} \equiv x^1 \pmod{263}$

malá Fermatova veta: ak p je prvočíslo a gcd(a,p)=1, potom $a^{p-1} \equiv 1 \pmod p$ (resp. $a^p \equiv a \pmod p$)

D.: $(a \cdot 1)(a \cdot 2) \ldots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod p$
pretože gcd(a,p)=1 dostaneme vľavo všetky zvyšky ...
obe strany predelíme (p-1)!

Zadné vrátka – FLT – pre prvočíselné n

- E: $x \rightarrow x^e \bmod n \quad (x < n) \qquad x^e \bmod n \rightarrow x$?
- nájsť také d, aby $(x^e \bmod n)^d \bmod n = x$

teda $(162)^d \equiv (x^{165})^d \equiv x^{165 \cdot d} \equiv x^1 \pmod{263}$

FLT: ak p je prvočíslo a gcd(a,p)=1, potom $a^{p-1} \equiv 1 \pmod p$

Naše n = 263 je prvočíslo, teda hľadáme d, aby

$x^{165 \cdot d} = x^{k(263-1)+1} \equiv x^1 \pmod{263}$ {pretože $(x^{(263-1)})^k \bmod 263 = 1^k$ }

teda $165 \cdot d = k\,(263 - 1) + 1$ resp. $165 \cdot d \equiv 1 \pmod{262}$

(hľadáme d - inverznú hodnotu k 165 modulo 262)

EEA - rozšírený Euklidov algoritmus

pre a, b existujú x, y, že
$ax + by = \gcd(a, b)$

$\gcd(262,165) = 1$

$\exists x,y:\ y \cdot 262 + x \cdot 165 = 1$

z čoho
$x \cdot 165 \equiv 1 \bmod 262$

$-17 \cdot 262 + 27 \cdot 165 = 1$

$27 \cdot 165 \equiv 1 \pmod{262}$

$27 = 165^{-1} \bmod 262$

$1 \cdot 262$	+	$0 \cdot 165$	=	262	
$0 \cdot 262$	+	$1 \cdot 165$	=	165	1
$1 \cdot 262$	+	$-1 \cdot 165$	=	97	1
$-1 \cdot 262$	+	$2 \cdot 165$	=	68	1
$2 \cdot 262$	+	$-3 \cdot 165$	=	29	2
$-5 \cdot 262$	+	$8 \cdot 165$	=	10	2
$12 \cdot 262$	+	$-19 \cdot 165$	=	9	1
$-17 \cdot 262$	+	$27 \cdot 165$	=	1	

- pre prvočíselné n z FLT platí
  $a^{n-2} \equiv a^{-1} \pmod n$
- modulárne umocňovanie je rýchlejšie ako EEA (nepotrebuje deliť)

Rozšírený Euklidov algoritmus - zjednodušenie

pre a, b existujú x, y, že
$ax + by = \gcd(a, b)$

$\gcd(262,165) = 1$

$\exists x,y:\ y \cdot 262 + x \cdot 165 = 1$

z čoho
$x \cdot 165 \equiv 1 \bmod 262$

$-17 \cdot 262 + 27 \cdot 165 = 1$

$27 \cdot 165 \equiv 1 \pmod{262}$

$27 = 165^{-1} \bmod 262$

0	262	
1	165	1
-1	97	1
2	68	1
-3	29	2
8	10	2
-19	9	1
27	1	

(x,a) = (0, a); (y,b) = (1,b);
while (c>0) (z,c) = ((x-$\lfloor\frac{a}{b}\rfloor$y), (a − $\lfloor\frac{a}{b}\rfloor$b));
(x,a)=(y,b); (y,b)=(z,c);
endwhile; return (x)

Zadné vrátka – FLT + EEA – pre prvočíselné n

- E: $x \to x^e \bmod n \quad (x < n) \qquad x^e \bmod n \to x$?
- nájsť také d, aby $(x^e \bmod n)^d \bmod n = x$

  teda $(162)^d \equiv (x^{165})^d \equiv x^{165 \cdot d} \equiv x^1 \pmod n$
- ak p je prvočíslo a gcd(a,p)=1, potom $a^{p-1} \equiv 1 \pmod p$
- naše n = 263 je prvočíslo, potom pre d = 27 platí $165 \cdot 27 \equiv 1 \pmod{262}$ a z FLT $x^{165 \cdot 27} \equiv x^1 \pmod{263}$

  $x^1 \equiv x^{165 \cdot 27} \equiv 162^{27} \equiv 162^{16} \cdot 162^8 \cdot 162^2 \cdot 162 \equiv$
  $\equiv 96 \cdot 137 \cdot 207 \cdot 162 \equiv 3 \pmod{263}$
- ak n je prvočíslo, je ľahké z e vypočítať d (a naopak) (teda ani jedno z nich nemožno zverejniť !)

Three-pass protocol (bez zverejnenia kľúčov)

(Shamir) Three-pass protocol – utajený prenos správy bez zverejnenia kľúčov

p – známe prvočíslo, $m < p$, $m^{eA \cdot dA} \bmod p = m^{eB \cdot dB} \bmod p = m$

- A -> B $m^{eA} \bmod p$
- B -> A $(m^{eA} \bmod p)^{eB} \bmod p = m^{eA \cdot eB} \bmod p$
- A -> B $(m^{eA \cdot eB} \bmod p)^{dA} \bmod p = (m^{eA \cdot dA})^{eB} \bmod p = m^{eB} \bmod p$
- B spočíta $(m^{eB} \bmod p)^{dB} \bmod p = m \bmod p = m$ (pre $m < p$)

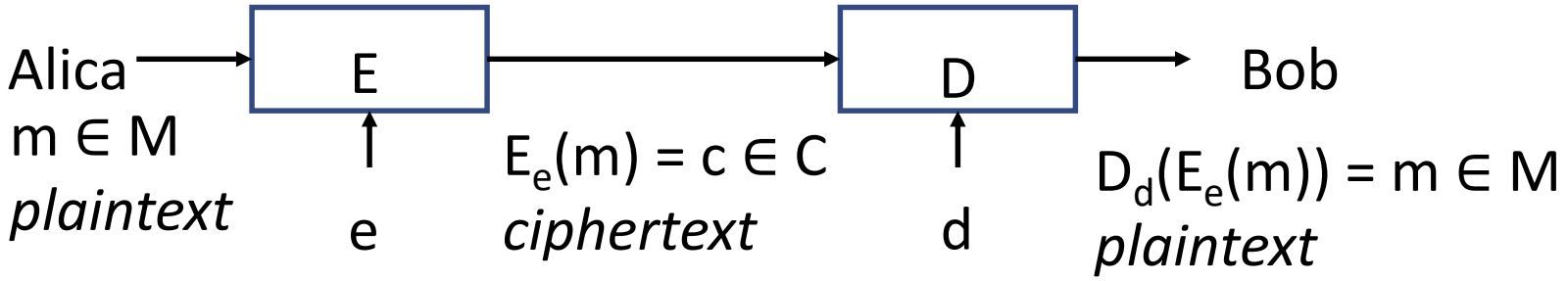
Kryptografické systémy s verejným kľúčom

problémy šifrovania rozdelením kľúča

- medzi dvoma účastníkmi, podvrhnutie identity, veľa správ ...

riešenie – zverejnenie šifrovacieho kľúča

e – verejný kľúč (public key) Boba (šifrovací)
d – súkromný kľúč (private key) Boba (dešifrovací)



Princíp asymetrickej kryptografie

- pre šifrovaciu funkciu E(e, m) = c je výpočet inverznej funkcie $E^{-1}(e, c) = m$
  výpočtovo (algoritmicky dokázateľne) zložitý – jednocestná resp. jednosmerná funkcia (one-way)
- na dešifrovanie existuje funkcia
  $$D(d, c) = E^{-1}(e, c) = m$$
  „zadné vrátka“ (trapdoor) – len ak poznáme d
- z e nie je možné jednoducho vypočítať d !!?

Princíp asymetrickej kryptografie

- pre šifrovaciu funkciu $E(e, m) = c$ je výpočet inverznej funkcie $E^{-1}(e, c) = m$ výpočtovo (algoritmicky dokázateľne) zložitý – jednocestná resp. jednosmerná funkcia (one-way)
- na dešifrovanie existuje funkcia

$$D(d, c) = E^{-1}(e, c) = m$$

„zadné vrátka“ (trapdoor) – len ak poznáme d

- z e nie je možné jednoducho vypočítať d !!?

$x \rightarrow x^e \bmod n \quad (x < n)$?? n nesmie byť prvočíslo

ETF Eulerova funkcia (Euler's totient function)

- E: $x \rightarrow x^e \bmod n \quad (x < n)$

  D: $x^e \bmod n \rightarrow (x^e \bmod n)^d \bmod n = x$
- ak n je prvočíslo, je ľahké z e vypočítať d
- ak by n nebolo prvočíslo ?

Eulerova veta: ak gcd(a,n) = 1 potom $a^{\phi(n)} \equiv 1 \pmod n$

$\phi(n)$ - počet čísel $1 \leq x \leq n$ takých, že gcd(x,n)=1

Eulerova funkcia $\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$

Jednocestná funkcia s ETF

- $E(e, x) : x \rightarrow x^e \bmod n = y \quad (x < n)$

  $D(d, y) : y = x^e \bmod n \rightarrow (x^e \bmod n)^d \bmod n = x$
- nájsť také d, aby $(x^e \bmod n)^d \bmod n = x$?
- ak gcd(a,n) = 1 potom $a^{\phi(n)} \equiv 1 \pmod n$ a teda výpočty v exponente možno robiť mod $\phi(n)$
- vypočítať d, aby $ed \equiv 1 \pmod{\phi(n)}$, potom
  $(x^e \bmod n)^d \bmod n = x^{ed} \bmod n = x^{k.\phi(n)+1} \bmod n =$
  $= x^{k.\phi(n)} \cdot x \bmod n = 1^k \cdot x \bmod n = x$ $\{x < n, \gcd(x,n)=1\}$
- aby niekto iný nespočítal d, nesmie poznať $\phi(n)$
  (ak by n bolo prvočíslo, $\phi(n) = n - 1$ ...)

Jednocestná funkcia pre n = p · q

- $E(e, x) : x \rightarrow x^e \bmod n = y \quad (x < n)$

  $D(d, y) : y = x^e \bmod n \rightarrow (x^e \bmod n)^d \bmod n = x$
- pre n = pq je $\phi(pq) = pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = (p-1)(q-1)$
- vieme vypočítať d, aby $ed \equiv 1 \pmod{(p-1)(q-1)}$, potom

  $(x^e \bmod (p-1)(q-1))^d \bmod (p-1)(q-1) = x^{ed} \bmod (p-1)(q-1) =$
  $= x^{k.(p-1)(q-1)+1} \bmod (p-1)(q-1) = 1^k \cdot x \bmod (p-1)(q-1) = x$
- stačí zvoliť dostatočne veľké n = p · q
- ak bude ťažké rozložiť n na prvočísla, nebude možné ľahko spočítať ani $\phi(n) = (p-1)(q-1)$ a teda ani d z verejného e (problém faktorizácie)

RSA

Rivest, Shamir, Adleman (1977)

Clifford Cocks (1973 uvoľnené 1997)

- zvoliť dostatočne veľké náhodné! prvočísla $p \approx q$
- $n = p \cdot q$ (*modulus*), $\phi(n) = (p-1)(q-1)$
- zvoliť $e < \phi(n)$ aby $\gcd(e, \phi(n)) = \gcd(e,(p-1)(q-1)) = 1$
- vypočítať d, aby $e \cdot d \equiv 1 \pmod{\phi(n)}$
- bezpečne zlikvidovať p, q, $\phi(n)$
- verejný kľúč (n, e) , súkromný kľúč (n, d)
- pre $m < n$: $E_{n,e}(m) = m^e \bmod n = c$, $D_{n,d}(c) = c^d \bmod n$

RSA príklad

- $p = 7$, $q = 13$, $n = pq = 91$, $e = 5$
- $\phi(n) = 6 \cdot 12 = 72$
- EEA: $-2 \cdot 72 + 29 \cdot 5 = 1$ $\quad 29 \cdot 5 \equiv 1 \pmod{72}$
- $(n, e) = (91, 5)$ $\quad (n, d) = (91, 29)$

- šifrovanie pre $m = 3$ $\quad c = 3^5 = 243 \equiv 61 \pmod{91}$
- dešifrovanie $\quad 61^{29} = 61^{16+8+4+1} \equiv 3 \pmod{91}$

Korektnosť RSA

- ak gcd(m,n) = 1, podľa Eulerovej vety

$$D\big(E(m)\big) = (m^e)^d \; mod\; n = m^{1+k\phi(n)} mod\; n =$$

$$= m \cdot \left(m^{\phi(n)}\right)^k mod\; n = m\; mod\; n = m \qquad \text{(vlastnosti ETF)}$$

- ak gcd(m,n) > 1 nech m = m‘· p^r , gcd(m‘,n) = 1

$$D\big(E(m)\big) = (\mathrm{m}' \cdot \mathrm{p}^{\mathrm{r}})^{ed} \; mod\; n = m'\left(p^{1+k\phi(n)}\right)^r mod\; n$$

z FLT: $1 = p^{(q-1)} \; mod\; q = p^{k(q-1)(p-1)} mod\; q = p^{k\phi(n)} mod\; q$

potom $p^{k\phi(n)} = 1 + t \cdot q$ a $p^{1+k\phi(n)} = p + t \cdot n \equiv p\; mod\; n$

a teda $D\big(E(m)\big) = (m' \cdot p^r)\; mod\; n = m$

implementačné postupy

šifrovanie : jednoduchý verejný exponent e = 65537
= $(10000000000000001)_2$

dešifrovanie : namiesto c^d mod n počítať
c^d mod p a c^d mod q

- súkromný kľúč $p, q, dp = d \; mod \; (p-1)$, $dq = d \; mod \; (q-1)$, $q_{inv} = q^{-1} mod \; p$
- z čínskej vety o zvyškoch (CRT)

$$m_p = c^{dp} mod \; p, \qquad m_q = c^{dq} mod \; q$$

$$\boldsymbol{m = m_q + q \cdot \left(q_{inv} \cdot \left(m_p - m_q\right) mod \; p\right)}$$

- overenie: $m \; mod \; p = m_p \quad m \; mod \; q = m_q$

CRT – Chinese reminder theorem

- výpočty s veľkými číslami pomocou niekoľkých výpočtov s menšími nesúdeliteľnými modulmi

Čínska veta o zvyškoch (Čína, 1. storočie) :

Pre vzájomne nesúdeliteľné čísla $m_1, m_2, \dots, m_n$ a celé čísla $a_1, a_2, \dots, a_n$ existuje jediné (modulo $M = \prod_{i=1}^{n} m_i$) riešenie systému kongruencií $x \equiv a_i \ (mod\ m_i)\ \ i \in \{1, \dots, n\}$ v tvare $x = \sum_{i=1}^{n} a_i M_i y_i \ mod\ M$, kde $M_i = M/m_i$ a $y_i = M_i^{-1} mod\ m_i$

- ak očakávame výsledok menší ako M, môžeme výpočty realizovať v moduloch m_i a výsledky sčítať podľa CRT

pre dvojicu prvočísel p, q je možné dešifrovanie $m = c^d\ mod\ pq$ riešiť pomocou $m_p = c^d\ mod\ p; m_q = c^d\ mod\ q;$
$q_{inv} = q^{-1} mod\ p; p_{inv} = p^{-1} mod\ q$ (hodnoty y_1, y_2)
ako $m = (m_p q q_{inv} + m_q p p_{inv})\ mod\ pq$

CRT - počítanie vojakov (príklad)

spočítať počet vojakov (234) – zoradiť do 29-stupu a 31-stupu a spočítame posledný rad

29-stupy	31-stupy
29 vojakov	31 vojakov
29 vojakov	31 vojakov
29 vojakov	31 vojakov
29 vojakov	31 vojakov
29 vojakov	31 vojakov
29 vojakov	31 vojakov
29 vojakov	31 vojakov
29 vojakov	17 vojakov
2 vojakov	

$$x \equiv 2 \ \ (mod\ 29)$$

$$x \equiv 17\ (mod\ 31)$$

$$y_1 = 31^{-1} mod\ 29 = 2^{-1} mod\ 29 = 15$$

$$y_2 = 29^{-1} mod\ 31 = (-2)^{-1} \mathrm{mod}\ 31 = 15$$

$$x \equiv 2 \cdot 31 \cdot \mathrm{y}_1 + 17 \cdot 29 \cdot \mathrm{y}_2 =$$
$$= 62 \cdot 15 + 493 \cdot 15 \quad (mod\ 899)$$

$$x \equiv 8325 \equiv 234 \ \ (mod\ 899)$$

$$x = 234 + 899 \cdot k$$

RSA s CRT

- $p = 7$, $q = 13$, $n = pq = 91$, $e = 5$
- $\phi(n) = 6 \cdot 12 = 72$
- EEA : $-2 \cdot 72 + 29 \cdot 5 = 1$ $\quad 29 \cdot 5 \equiv 1 \pmod{72}$
- $d = 29$, $dp = 5$, $dq = 5$, $qinv = 6$ $\quad (13 \cdot 6 \equiv 1 \pmod 7)$
- $(n, e) = (91, 5)$ $\quad (n, d) = (91, 29)$

- šifrovanie pre $m = 3$ $\quad c = 3^5 = 243 \equiv 61 \pmod{91}$
- dešifrovanie $m_p = 61^5 \equiv 5^5 \equiv 5^4 \cdot 5 \equiv 2 \cdot 5 \equiv 3 \pmod 7$
- $m_q = 61^5 \equiv 9^5 = 9^4 \cdot 9 \equiv 9 \cdot 9 \equiv 3 \pmod{13}$
- $m = 3 + 13(6(3-3) \bmod 7) = 3$

Square-and-Multiply algoritmus

- $x \rightarrow x^e \bmod n$
  $e = e_r e_{r-1} e_{r-2} \ldots e_0$ v binárnom zápise
- $y = x$
  for i = r-1 downto 0 do
  $\quad y = y^2 \bmod n$
  $\quad$ if $e_i = 1$ then $y = (y * x) \bmod n$
  endfor
  return (y)

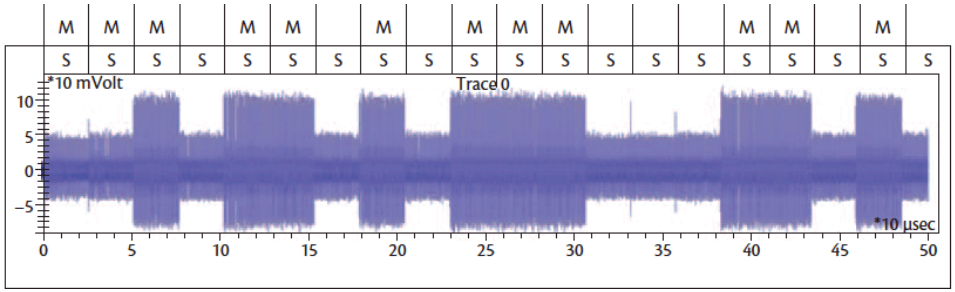
pre $(165)_2 = 10100101$

$3^{165} \bmod 263$

$3^{165} = (3^{82})^2 \cdot 3 = ((3^{41})^2)^2 \cdot 3 = ((3^{40} \cdot 3)^2)^2 \cdot 3 =$
$= (((((3^5)^2)^2)^2 \cdot 3)^2)^2 \cdot 3 =$
$= (((((((3^2)^2) \cdot 3)^2)^2)^2 \cdot 3)^2)^2 \cdot 3 \equiv$
$\equiv (((((81 \cdot 3)^2)^2)^2 \cdot 3)^2)^2 \cdot 3 \equiv ((11 \cdot 3)^2)^2 \cdot 3 \equiv$
$\equiv 54 \cdot 3 \equiv 162 \pmod{263}$

k	x=3	$3^k \bmod 263$
1		3
10	SQ	3·3=9
100	SQ	9·9=81
101	MUL	81·3=243
1010	SQ	59049≡137
10100	SQ	96
101000	SQ	11
101001	MUL	11·3=33
1010010	SQ	1089≡37
10100100	SQ	1369≡54
10100101	MUL	54·3=162

Square-and-Multiply – timing attack



- rôzne časy výpočtu (počet 1 v kľúči)
- side channel attack - sledovanie záťaže (resp. elmg vyžarovania)
- pomocou CRT resp. modifikácia SM

```
y = x
for i = r-1 downto 0 do
    y = y^2 mod n
    if e_i = 1 then y = (y * x) mod n
    else    z = (y * x) mod n
endfor
return (y)
```

k	x=3	3^k mod 263
1		3
10	SQ	3·3=9
100	SQ	9·9=81
101	MUL	81·3=243
1010	SQ	59049≡137
10100	SQ	96
101000	SQ	11
101001	MUL	11·3=33
1010010	SQ	1089≡37
10100100	SQ	1369≡54
10100101	MUL	54·3=162

Zraniteľnosti RSA

- rovnaké modulá (resp. prvočísla)
- ak $d < \sqrt{n}$ dá sa rekonštruovať 1/4 dolných bitov d
- (p-1) a (q-1) by mali mať veľký prvočíselný faktor
- silné p - (p-1) aj (p+1) majú veľké prvočíselné faktory
- gcd(p-1,q-1) by mal byť malý

(NIST 2016) pred útokmi hrubou silou (COA, CPA)

- 112 bitov 3DES kľúča ≈ 2048 bitov RSA
- 128 bitov AES kľúča ≈ 3072 bitov RSA
- 192 bitov AES kľúča ≈ 7680 bitov RSA
- 256 bitov AES kľúča ≈ 15360 bitov RSA

Útoky na RSA - výplň (padding) PKCS#1 v 1.5

- CPA útoky – ak je |P| malá, možno si vygenerovať všetky zašifrované správy v indexovej tabuľke
- CCA útoky – CCA1 zoznamom otázok na dešifrovanie
  CCA2 – adaptívne dešifrovanie (napr. podpisy ...)
- útoky na homomorfnú vlastnosť RSA
  $E(m_1) \cdot E(m_2) = (m_1^e \bmod n)(m_2^e \bmod n) =$
  $= (m_1^e \cdot m_2^e) \bmod n = (m_1 \cdot m_2)^e \bmod n = E(m_1 \cdot m_2)$
- výplň bloku + redundancia + randomizácia
- PKCS (Public-Key Cryptography Standards RSA Labs.)
  0x00 | 0x02 | PS | 0x00 | m
  PS – reťazec pseudonáhodých bajtov (aspoň 8)

OAEP (Optimal Asymmetric Encryption Padding)

k-bitový blok (2048 b)

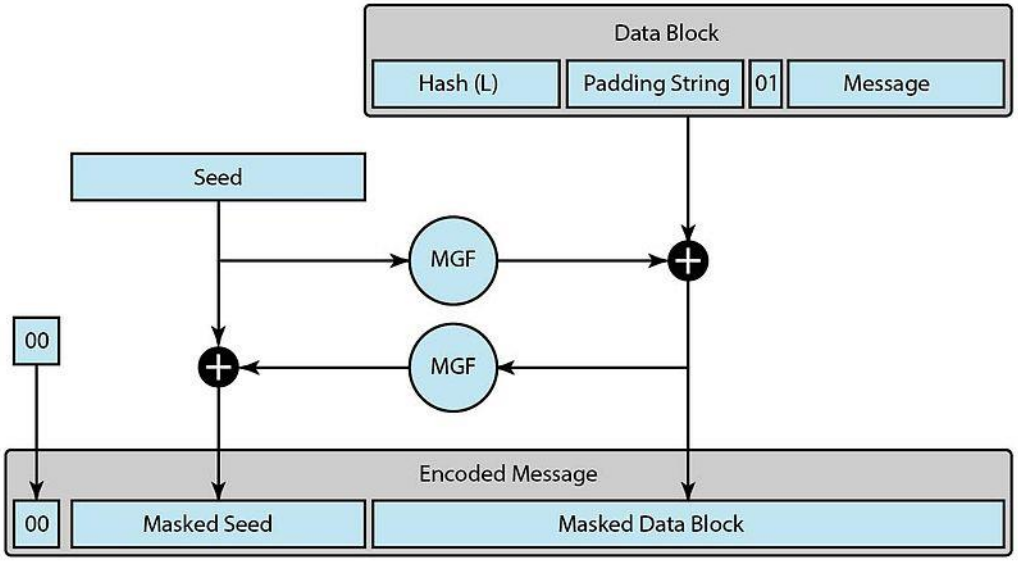
$|m| = 160\ (256)$ b

L – label (nemusí byť)

$|seed| = |Hash(L)| = h$

2 Feistelove rundy

$MGF_h: \{0,1\}^{k-h-1} \rightarrow \{0,1\}^h$



$MGF_{k-h-1}: \{0,1\}^h \rightarrow \{0,1\}^{k-h-1}$ funkcie na generovanie masky

PS – reťazec $k - |m| - 2 \cdot h - 2$ nulových bajtov 0x00

$DB = Hash(L) \mid PS \mid 0x01 \mid m$

$EM = 0x00 \mid seed \oplus MGF_h(DB \oplus MGF_{k-h-1}(seed)) \mid$
$\mid (DB \oplus MGF_{k-h-1}(seed))$

Výber prvočísel

- náhodný výber z nepárnych čísel (rovnakej dĺžky)
- hustota prvočísel - počet prvočísel, menších ako n

$$\pi(n) \approx n/\ln(n)$$

- testovanie prvočíselnosti - Eratostenovo sito
- Solovay-Strassen s Jacobiho symbolmi (pravdep.)
- AKS (Agrawal-Kayal-Saxena) primality test (2002) v polynomiálnom čase s nepraktickým exponentom
- testy využívajúce Malú Fermatovu vetu

Test prvočíselnosti

- ak n prvočíslo ⇒ pre všetky a $a^{n-1} \equiv 1 \pmod{n}$
- ak existuje a, že $a^{n-1} \not\equiv 1 \pmod{n}$ ⇒ n nie je prvočíslo
- koľko a treba vyskúšať, aby bolo n prvočíslo s veľkou pravdepodobnosťou ?
  (FLT test prvočíselnosti ..., AKS)
- (Carmichael 1910) Carmichaelove čísla
  zložené čísla C, že ∀a gcd(a,C) = 1: $a^{C-1} \equiv 1 \pmod{C}$
  (najmenšie 561 = 3 . 11 . 17)

Miller-Rabinov test

- $n - 1 = t \cdot 2^s$ (nepárne t) pre náhodné $1 < a < n$
  postupnosť $a^t, (a^t)^2, (a^t)^4, \ldots, (at)^{2^s} = a^{n-1} \equiv 1 \pmod n$
- ak p je prvočíslo, má 1 **práve dve** odmocniny -1 a 1; teda
  $((a^t)^{2^{s-1}})^2 = (a^t)^{2^s} \equiv 1 \pmod n \Rightarrow (a^t)^{2^{s-1}} \bmod n \in \{-1, 1\}$
- Miller-Rabin: stačí testovať a^t, a^{2t}, a^{4t} kým nadobudne hodnotu -1 resp. 1 (p-1 resp. 1) – ak nikdy, tak je n zložené, inak (s chybou najviac 1/4) je n prvočíslo
- z = a^t mod n; if z == 1 then return(„likely prime“);
  for i = 0 to s-1 do if z == (n-1) then return(„likely prime“)
  else z = z^2 mod n; endif; endfor;
  return(„composite“)
- po 10 testoch je chyba ~ $1/4^{10} = 1/2^{20}$
  (pre n < 3 215 031 751 stačí testovať 2,3,5 a 7 ...)

Miller-Rabinov test príklad

$n = 252601, \qquad n - 1 = 2^3 \cdot 31575$

$a = 85132$

$a^{31575} \equiv 191102 \pmod{252601}$

$a^{31575 \cdot 2} \equiv 184829 \pmod{252601}$

$a^{31575 \cdot 2^2} \equiv 1 \pmod{252601}$

252601 je teda zložené číslo

(pretože $184829^2 \equiv 1 \pmod{252601}$ je 184829 ďalšia odmocnina jednotky mod 252601)

Faktorizačné algoritmy

- Eratostenovo sito – deliteľnosť prvočíslami $\leq \sqrt{n}$
- Fermatova faktorizácia
  $n = x^2 - y^2 = (x + y)(x - y)$ - stačí zapísať n ako rozdiel štvorcov (cca |p-q|/2 krokov)
- ak má (p-1) len malé faktory $b = a^{B!} \equiv a^{(p-1)k} \equiv 1 \pmod n$ potom $p \mid \gcd(b-1,n)$ ...
- kvadratické sito $x^2 \equiv p_1^{k1} p_2^{k2} \ldots p_t^{kt} \pmod n$ ...
  hľadáme x a y, aby $x^2 \equiv y^2 \pmod n$ a $x \not\equiv \pm y$
  potom gcd(x-y, n) je netriviálny faktor n
- Pollard's rho algoritmus
- Shorov algoritmus (kvantový výpočet)

kvadratické sito - príklad

- faktorová báza pre $x^2 \equiv p_1^{k1}\, p_2^{k2} \ldots p_t^{kt} \pmod n$
  kde p_i je i-te prvočíslo podľa veľkosti, je postupnosť k1, k2, …, kt, …

(pre $3397^2 \equiv 2^5.5.13^2 \pmod{3837523}$ je 5,0,1,0,0,2,…)

pre faktorizáciu 3837523 - niekoľko faktorových báz:

1964^2	0 2 0 0 0 3 0 0	hľadáme súčet báz, zložený z párnych čísel :	
3397^2	5 0 1 0 0 2 0 0		
8077^2	1 0 0 0 0 0 0 1	$3397^2 \cdot 8077^2 \cdot 9398^2$	6 0 6 0 0 2 0 2
9398^2	0 0 5 0 0 0 0 1	$1964^2 \cdot 14262^2$	0 2 2 2 0 4 0 0
14262^2	0 0 2 2 0 1 0 0		

$(3397.8077.9398)^2 \equiv 2^6.5^6.13^2.19^2 \equiv (2^3.5^3.13.19)^2 \pmod{3837523}$
teda $3590523^2 \equiv 247000^2 \pmod{3837523}$
ale $3590523 \equiv -247000 \pmod{3837523}$ nefaktorizuje …

$(1964.14262)^2 \equiv 3^2.5^2.7^2.13^4 \equiv (3.5.7.13^2)^2 \pmod{3837523}$
teda $1147907^2 \equiv 17745^2 \pmod{3837523}$
a gcd(1147907-17745, 3837523) = 1093 teda 3837523 = 1093.3511

Faktorizácia - rozklad na prvočísla

RSA Labs - Factoring Challenge 1991-2007

- RSA-100 330 b $1000 1991
- RSA-130 430 b $14527 1996
- RSA-140 463 b $17226 1999
- RSA-155 512 b $9383 1999
- RSA-576 576 b $10000 2003
- RSA-640 $20000 2005
- RSA-704 $30000 2012
- RSA-220 729 b 2016
- RSA-230 762 b 2018
- RSA-768 768 b $50000 2009
- RSA-250 829 b 2020
- RSA-1024 $100000 ???

princíp RSA

- jednoducho vypočítateľná ale ťažko invertovateľná funkcia $x \rightarrow x^e \bmod pq$ ($x < pq$)

  $x^e \bmod pq \rightarrow x$?
- nájsť také d, aby $(x^e \bmod pq)^d \bmod pq = x$ je také ťažké, ako poznať $\phi(pq)$, čo je zase ekvivalenté problému faktorizácie $n = pq$
- ak poznáme $\phi(pq)$, je výpočet exponentu d, aby $ed \equiv 1 \pmod{\phi(pq)}$, jednoduchý. Jednoduchý je aj výpočet $x^e \bmod pq \rightarrow (x^e \bmod pq)^d \bmod pq = x$
- výpočet $x^e \bmod pq \rightarrow x$ pre známe e a súčin pq nie je zložitejší, ako riešenie problému faktorizácie

kvadratické zvyšky (quadratic residues)

- jednoducho vypočítateľná ale ťažko invertovateľná funkcia $x \rightarrow x^2 \bmod n \quad (x < n)$

  $x^2 \bmod n \rightarrow x$?
- y je kvadratický zvyšok modulo n ak existuje x, že $x^2 \equiv y \pmod n$ (nie všetky čísla zo $\mathbb{Z}_n$ sú k.z.)
- ak **n je prvočíslo p**, potom ak $a^2 \equiv b^2 \pmod p$, platí $p|(a^2-b^2) \Rightarrow p|(a-b)(a+b)$, teda ak odmocnina existuje, budú to práve dve čísla $\{a, p-a\}$
  a riešenie $(p - x)^2 = p^2 - 2px + x^2 \equiv x^2 \equiv y \pmod p$ pre $p \equiv 3 \pmod 4$ je $x = \pm y^{(p+1)/4} \bmod p$

kvadratické zvyšky modulo pq

- jednoducho vypočítateľná ale ťažko invertovateľná funkcia $x \to x^2 \bmod n \quad (x < n)$

  $x^2 \bmod n \to x$?
- y je kvadratický zvyšok modulo n ak existuje x, že $x^2 \equiv y \pmod n$ (nie všetky čísla zo $\mathbb{Z}_n$ sú k.z.)
- pre **n=pq** riešenie $x^2 \equiv y \pmod{pq}$ dostaneme z CRT ak vieme riešenie $z^2 \equiv y \pmod p$ a $z^2 \equiv y \pmod q$
- pokiaľ $p \equiv q \equiv 3 \pmod 4$, vieme vypočítať riešenia $z_{1,2} = \pm\, y^{(p+1)/4} \bmod p$, $z_{3,4} = \pm\, y^{(q+1)/4} \bmod q$ na čo ale musíme poznať p a q, teda faktorizáciu n

Rabinov kryptosystém

Rabin (1979)

- dostatočne veľké prvočísla $p \equiv q \equiv 3 \pmod 4$
- verejný kľúč $n = pq$, súkromný kľúč (p, q)
- pre $m < n$: $E_n(m) = m^2 \bmod n = c$
- $D_{p,q}(c)$: $m \in \pm (c^{(p+1)/4} \bmod p) \cdot q \cdot (q^{-1} \bmod p) \pm$
  (podľa CRT) $\pm (c^{(q+1)/4} \bmod q) \cdot p \cdot (p^{-1} \bmod q)$
  a podľa platnej štruktúry (napr. OAEP) identifikujeme správne m (zo štyroch možností)
- nájdenie riešenia je dokázateľne ekvivalentné faktorizácii n

Merkle-Hellmanovo plnenie batoha

- Merkle, Hellman - subset-sum problem
- množina $\mathrm{B} = \{b_1, b_2, \dots, b_n\}$ $b_i \in \mathbb{N}$, $S \in \mathbb{N}$
- existujú $x_i \in \{0,1\}$ (podmnožina B), že platí
  $x_1 b_1 + x_2 b_2 + \cdots + x_n b_n = S$?
  (je možné batoh veľkosti S presne zaplniť komponentami z B ?)
- NP-úplný problém (vyskúšať všetky možnosti)
- ak $\forall i$: $b_i > \sum_{j=1}^{i-1} b_j$ postupnosť B je superrastúca – riešenie je lineárne – postupujeme od najväčšieho b_n - ak sa vmestí, musíme ho vziať, pretože zo zvyškom by sme už batoh nenaplnili ...
  riešenie je jediné ! (možno ním kódovať správu)

Merkle-Hellmanovo plnenie batoha

príklad :

B = {2,3,6,13,27,52}

S = 70

Riešenie:

2, 3, 13, 52

2	3	6	13	27	52
≤2	≤5	≤5	≤18	≤18	≤ 70
Áno 1	Áno 1	Nie 0	Áno 1	Nie 0	Áno 1

Merkle-Hellmanovo plnenie batoha

$\mathrm{B} = \{b_1, b_2, \dots, b_n\}, b_i \in \mathbb{N}$ superrastúca, M, W$\in \mathbb{N}$ M > $\sum_{i=1}^{n} b_i$, W < M, gcd(W,M) = 1

- súkromný kľúč : B, M, W^{-1} ($W^{-1}W \equiv 1 \pmod M$)
- verejný kľúč : $A = \{a_1, a_2, \dots, a_n\} =$
  $= \{Wb_1 \ mod \ M, Wb_2 \ mod \ M, \dots, Wb_n \ mod \ M\}$
  (to už nebude superrastúca postupnosť – transformuje „ľahký“ problém na „ťažký“, pre inverznú transformáciu treba M a W^{-1})
- šifrovanie : m = $m_1 m_2 \dots m_n$ v binárnom tvare $m_i \in \{0,1\}$
  c = $m_1 a_1 + m_2 a_2 + \cdots + m_n a_n$
- dešifrovanie : S = $(W^{-1}c) \ mod \ M = (W^{-1}\sum_{i=1}^{n} m_i a_i) \ mod \ M =$
  $= \sum_{i=1}^{n} m_i (W^{-1} W b_i mod \ M) = \sum_{i=1}^{n} m_i b_i$
  a vypočítame m = $m_1 m_2 \dots m_n$ riešením subset-sum problému pre superrastúcu postupnosť B a sumu S

Merkle-Hellmanov kryptosystém - príklad

$M = 105, \quad W = 31$

$105 > 2+3+6+13+27+52$, $\gcd(31,105) = 1$

$W^{-1} = 61 \quad 61*31 = 1891 \equiv 1 \pmod{105}$

2	3	6	13	27	52

↓

62	93	81	88	102	37	VK

$2 * 31 \bmod 105 = 62$

$3 * 31 \bmod 105 = 93$

$6 * 31 \bmod 105 = 81$

$13 * 31 \bmod 105 = 88$

$27 * 31 \bmod 105 = 102$

$52 * 31 \bmod 105 = 37$

PT	1	1	0	1	0	1
∑	62 + 93		+ 88		+ 37	
CT			280			

S $\quad 61*280 \bmod 105 = 70$

2	3	6	13	27	52
Áno	Áno	Nie	Áno	Nie	Áno
1	1	0	1	0	1

Merkle-Hellman analýza

- pred útokmi hrubou silou - aspoň 200 prvkov postupnosti s 200 - 500 bitovými hodnotami ...
- prvky postupnosti A môžeme pred zverejnením permutovať permutáciou, ktorá bude potom súčasťou súkromného kľúča a použije sa jej inverz pri dešifrovaní
- existuje polynomiálne aproximačné riešenie, ktorým je možné transformovať A na takmer superrastúcu postupnosť (s požadovanou presnosťou) – systém je prakticky nepoužiteľný

Ďakujem za pozornosť.

jozef.jirasek@upjs.sk