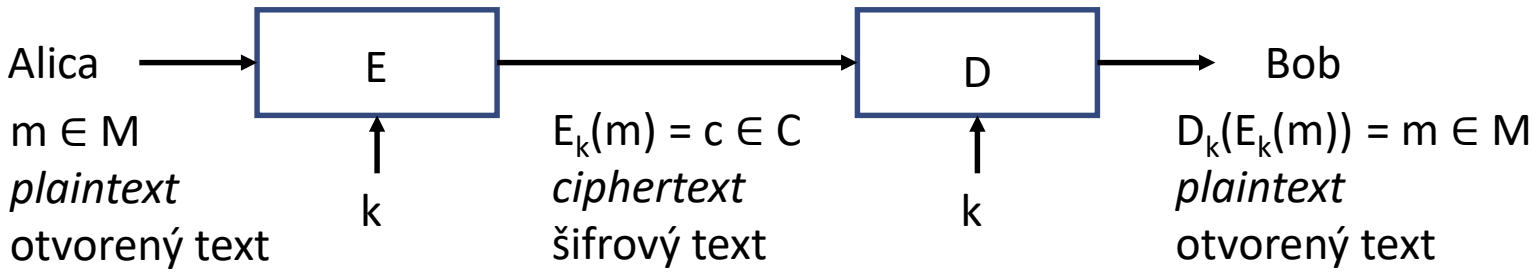
Kryptografické systémy
Asymetrická kryptografia - úvod

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 :

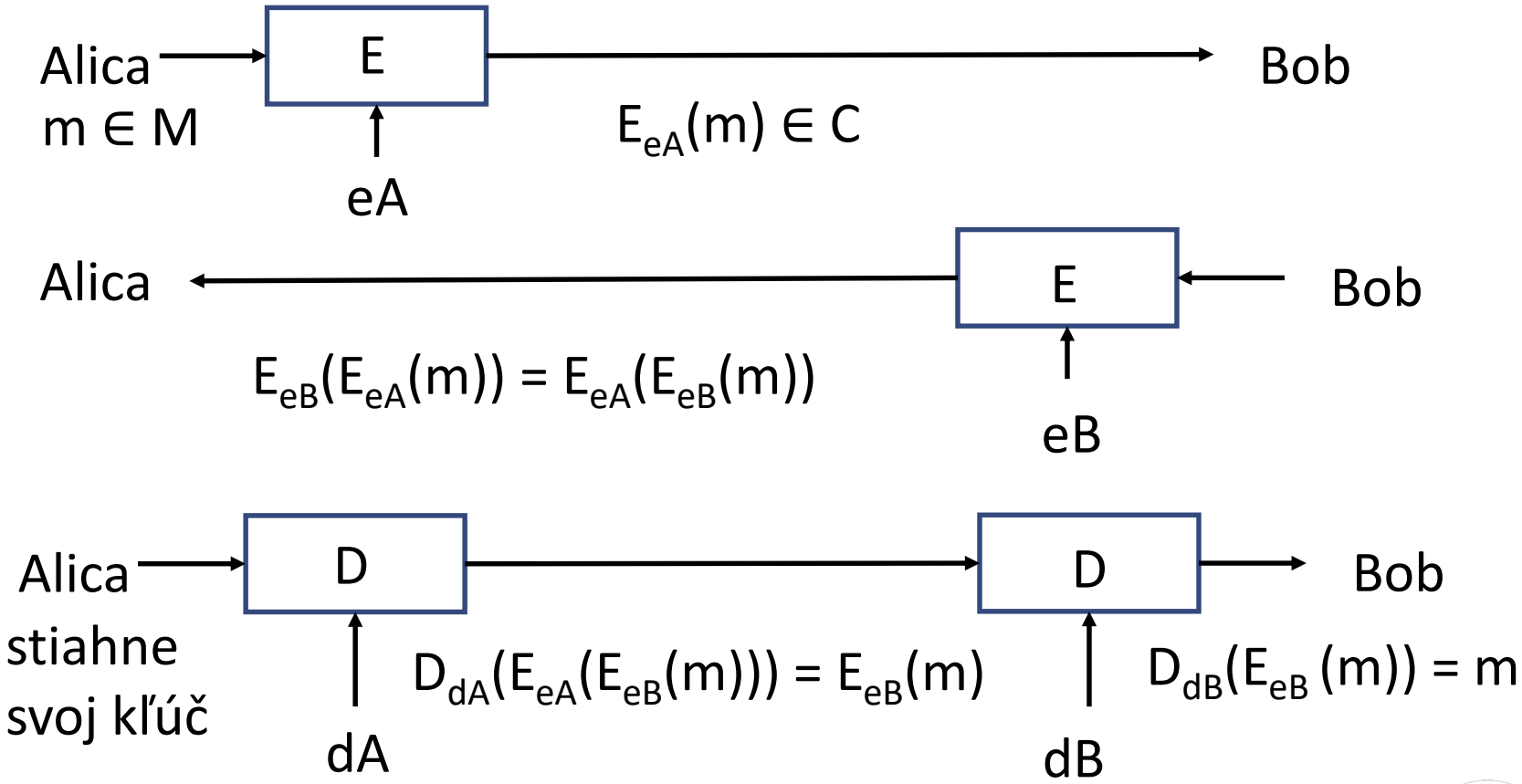
e – šifrovací kľúč

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 $m < p$)

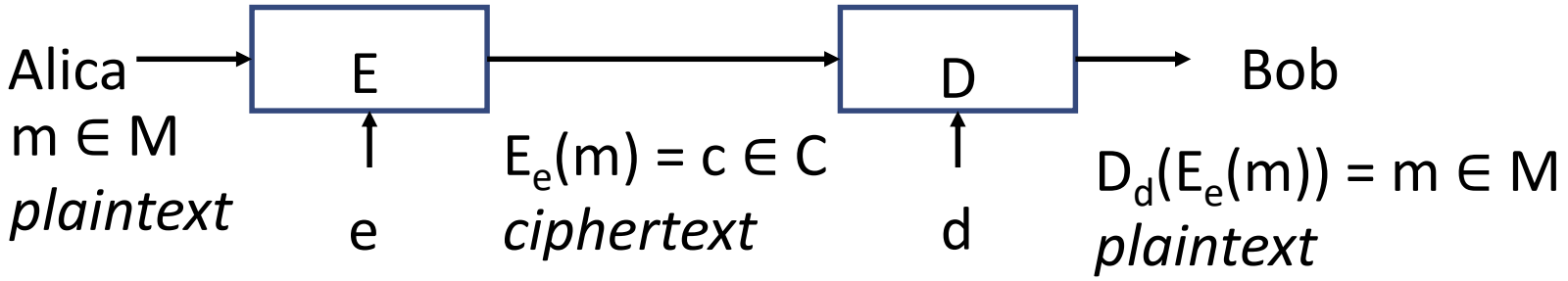
Kryptografické systémy s verejným kľúčom

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 $\quad 61^{29} = 61^{16+8+4+1} \equiv 3 \pmod{91}$

Ďakujem za pozornosť.

jozef.jirasek@upjs.sk