Bezpečnost v informačních technologiích (KIV/BIT)

4. Šifrování veřejným a soukromým klíčem (asymetrické šifry)

Ing. Pavel Král, Ph.D.

Katedra informatiky a výpočetní techniky
Západočeská Univerzita

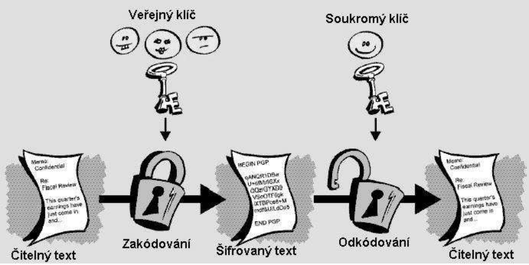
4. března 2015

Obsah

Šifrování s veřejným klíčem

- problém distribuce klíčů $\rightarrow$
- 1976 Diffie & Hellman: dva klíče (šifrovací a dešifrovací)
  - možnost odvození dešifrovacího z šifrovacího
- zveřejnění šifrovacího klíče $\rightarrow$ veřejný klíč
- utajení dešifrovacího klíče $\rightarrow$ tajný (soukromý) klíč

Asymetrické šifry



- E šifrovací fce
- D dešifrovací fce
- VK_p šifrovací (veřejný) klíč příjemce P
- SK_p dešifrovací (soukromý) klíč příjemce P
- P plaintext (znak, nebo blok)
- C šifrový text

Šifrování

- $C = E_{VK_p}(P)$

Dešifrování

- $P = D_{SK_p}(C)$

- začátek: každý příjemce vygenerování veřejného a soukromého klíče
- $\rightarrow$ problém: zprávy pro více příjemců

Zavazadlový algoritmus

Bezpečnost v informačních technologiích (KIV/BIT)

Ing. Pavel Král, Ph.D.

Asymetrické šifry

Algoritmus RSA

El Gamalův systém

- první algoritmus pro šifrování veřejným klíčem
- Merkle & Hellman
- použití pouze pro šifrování
- založen na NP složitosti zavazadlového (knapsack) problému
- z bezpečnostního hlediska označen za nevyhovující $\times$ demonstrace využití NP složitosti v kryptografii

Zavazadlový algoritmus - princip

- předměty o hmotnosti $m_1, \ldots, m_N$
- potřeba zabalit z těchto předmětů zavazadlo o váze M
- $\rightarrow$ musí platit: $M = b_1.m_1 + b_2.m_2 + \ldots + b_N.m_N$, kde
- **cíl**: najít koeficienty $b_i \in \{0; 1\}$ pro $i \in \{1, \ldots, N\}$

- zakódování zprávy = tajný výběr podmnožiny předmětů $\rightarrow$ zavazadlo
- zveřejnění: celk. hmotnost M + seznam všech předmětů $m_1, \ldots, m_N$
- potřeba zjištění, které předměty v zavazadle ???
- problém ve volbě hmotností předmětů:
  - jednoduchý problém $\rightarrow$ možnost rozluštění kdokoli
  - složitý problém $\rightarrow$ nerozluští nikdo
  - **autoři návrh převodu: jednoduchý problém $\rightarrow$ složitý** pomocí modulární aritmetiky

Šifrování:

P =	0	1	1	1	0	0
Hmotnosti	1	5	6	11	14	20
C =			??? = 22			

- hmotnosti: $1, 5, 6, 11, 14$ a 20 (zveřejněno)
- váha zavazadla: 22 (zveřejněno)

- hledám koeficienty: $22 = ???$

Zavazadlový algoritmus
Triviální příklad

Šifrování:

$$\begin{array}{rcccccc} P = & 0 & 1 & 1 & 1 & 0 & 0 \\ \text{Hmotnosti} & 1 & 5 & 6 & 11 & 14 & 20 \\ C = & & \multicolumn{4}{c}{5+6+11=22} & \end{array}$$

- hmotnosti: $1, 5, 6, 11, 14$ a 20 (zveřejněno)
- váha zavazadla: 22 (zveřejněno)
- hledám koeficienty: $22 = 5 + 6 + 11$

Zavazadlový algoritmus - princip - podrobně
Tvorba klíčového páru

Volba soukromého klíče

- množina koeficientů = superrostoucí posloupnost
- platí tedy: $\sum_{i=1}^{k} m_i < m_{i+1}$ - snadné nalezení (= soukromý klíč)
- $\times$ posloupnost není superrostoucí - velmi obtížné určení (= veřejný klíč)

Transformace soukromého klíče na klíč veřejný

- vynásobení $\forall$ prvků superrostoucí posloupnosti číslem $p \ mod \ q$, kde:
  - $q > \sum_{i=1}^{N} m_i$
  - p nesmí mít žádné společné součinitele s modulem $mod \ q$

Vystavení veřejného klíče

Zavazadlový algoritmus - princip - podrobně

Šifrování zprávy (pomocí veřejného klíče)

Dešifrování

Transformace šifrových bloků na snadný problém

- vynásobení čísel reprezentujících šifrové bloky výrazem $p^{-1}\ mod\ q$

Dešifrování pomocí soukromého klíče

Zavazadlový algoritmus - příklad

Tvorba klíčového páru:

1. volba soukromého klíče: $\{2, 3, 6, 13, 27, 52\}$
2. transformace na veřejný klíč: vynásobení zvoleným $p \; mod \; q$, $p = 31$, $q = 105$: $\{62, 93, 81, 88, 102, 37\}$
3. vystavení veřejného klíče

Šifrování (veřejným klíčem):

1. rozdělení zprávy na bloky: $011000110101101110 \rightarrow 011000\ 110101\ 101110$ (dle počtu prvků klíče)
2. $011000 \rightarrow 93 + 81 = 174$
   $110101 \rightarrow 62 + 93 + 88 + 37 = 280$
   $101110 \rightarrow 62 + 81 + 88 + 102 = 333$
3. $\rightarrow$ šifrový text: $C = \{174, 280, 333\}$

Zavazadlový algoritmus - příklad

Dešifrování (soukromým klíčem):

1. příjemce: znalost hodnot $p = 31$ a modulu $q = 105$ a soukromého klíče $\{2, 3, 6, 13, 27, 52\}$
2. určení p^{-1}: $31.(p^{-1}) \equiv 1 \; (mod \; 105) \rightarrow p^{-1} = 61$
3. $C = \{174, 280, 333\}$ vynásobení výrazem 61 mod 105 + rozklad $\rightarrow$ položky soukromého klíče $\rightarrow$ zpráva
4. $174 \times 61 \text{ mod } 105 = 9 = 3 + 6$
   $280 \times 61 \text{ mod } 105 = 70 = 2 + 3 + 13 + 52$
   $333 \times 61 \text{ mod } 105 = 48 = 2 + 6 + 13 + 27$
5. $P = 011000\ 110101\ 101110$

Zavazadlový algoritmus - poznámky

- autor Merkle - jistota s bezpečností algoritmu $\rightarrow$ nabídka 100,- \$ za rozluštění - Shamir (druhý z autorů alg. RSA) rozluštil
- $\rightarrow$ zesílení algoritmu - nabídka 1000,- \$ za rozluštění - Rivest (první z autorů alg. RSA)
- $\rightarrow$ zavazadlový algoritmus (+ alg. z něho odvozené) se nepovažuje za bezpečný

Algoritmus RSA

- 1977 - **R**ivest, **S**hamir, **A**dleman (RSA) - návrh nového šifrovacího algoritmu veřejného klíče
- nejznámější a nejpoužívanější
- použití dosud: dostatečné délka klíče $\rightarrow$ považován za bezpečný
- vhodný pro šifrování i pro el. podpis

Algoritmus RSA - princip

Předpoklad:

- rozklad velkého čísla na součin prvočísel (faktorizace) = velmi obtížná úloha
- žádný algoritmus faktorizace, který by pracoval alespoň v polynomiálním čase vůči velikosti binárního zápisu čísla n
- $\rightarrow$ z čísla n ($n = p \times q$) praktická nemožnost zjištění p a q v "rozumném" čase
- $\times$ násobení dvou velkých čísel je jednoduchá úloha
- potřeba volby dostatečně velkých prvočísel (100-200 míst nebo více), prvočísla řádově stejně velká

Algoritmus RSA - popis

Tvorba klíčů

- výběr dvou velkých prvočísel p a q
- výpočet $n = p \,.\, q$
- výpočet $x = (p-1)(q-1)$
- volba klíče e (celé číslo; $e < x$; e je s x nesoudělné)
- nalezení klíče d tak, aby $de \equiv 1 \; (mod \; x) \rightarrow$
- $d = e^{-1}(mod \; x)$ (výpočet d pomocí rozšířeného Euclidova algoritmu)
- d tajný (soukromý) klíč; e a n veřejný klíč
- p a q nepotřebné $\rightarrow$ možno odložit $\times$ utajit

Algoritmus RSA - popis

Šifrování

- rozdělení zprávy na bloky P_i kratší než n
- $C_i = P_i^e mod\ n$

Dešifrování

- $P_i = C_i^d mod\ n$

Poznámky

- možnost šifrování klíčem d a dešifrování pomocí e
- Rychlost:
  - HW realizace: asi 1000 $\times$ pomalejší než DES
- Bezpečnost:
  - $n >= 2048 \rightarrow$ alg. považován za bezpečný

Algoritmus RSA - příklad

Tvorba klíčů

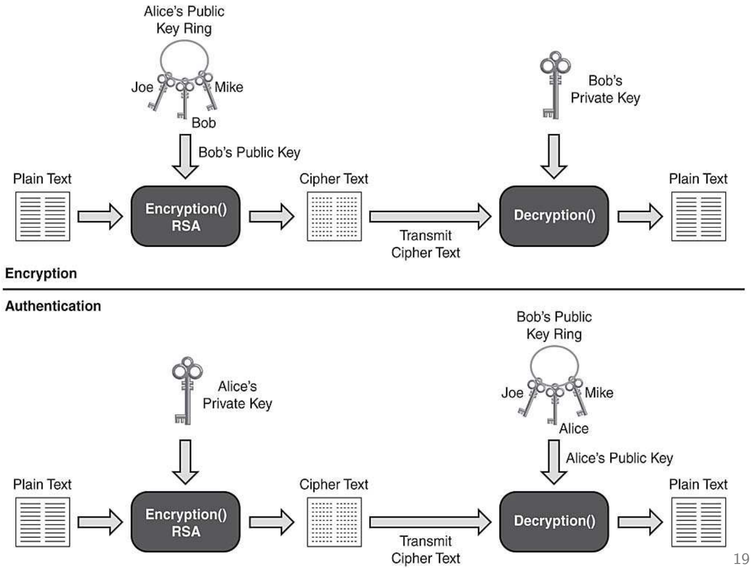
- $p = 47,\ q = 71$ (prvočísla)
- $n = p\ .\ q = 3337$ (modul, veřejný)
- náhodná volba klíče $e = 79$ (veřejný, šifrovací exponent)
  - e nemá žádné společné součinitele s $x = (p-1)(q-1) = 46 * 70 = 3220$
- $d = 79^{-1} mod\ 3220$ (Euclidův rozšířený alg.) $\rightarrow$
- $d = 1019$ (soukromý, dešifrovací exponent)

Šifrování:

- Zpráva: 688
- $C = 688^{79} mod\ 3337 = 1570$

Dešifrování:

- $P = 1570^{1019} mod\ 3337 = 688$



Alice's Public Key Ring
Joe
Mike
Bob
Bob's Public Key
Bob's Private Key
Plain Text
Encryption() RSA
Cipher Text
Transmit Cipher Text
Decryption()
Plain Text
Encryption
Authentication
Alice's Private Key
Bob's Public Key Ring
Joe
Mike
Alice
Alice's Public Key
Plain Text
Encryption() RSA
Cipher Text
Transmit Cipher Text
Decryption()
Plain Text

El Gamalův systém

- založen na obtížnosti výpočtu diskrétních logaritmů v konečném tělese
- nepatentován
- použití pro šifrování i el. podpis
- nevýhoda: délka šifrového textu $= 2\times$ délka otevřeného textu
- více viz [1]

El Gamalův systém - šifrování

Generování klíčů

- volba: p, g a $x \leftrightarrow p$ .. prvočíslo, $g < p$, $x < p$
- výpočet: $y = g^x mod\ p$
- $VK = \{y,\ g,\ p\}$
- $SK = \{x\}$
- g a p .. možno sdílet skupinou uživatelů

Šifrování

- náhodná volba $k \leftrightarrow$ žádný spol. dělitel s $(p-1)$
- $K = y^k mod\ p$
- $Ca = g^k mod\ p$
- $Cb = P.K\ mod\ p$

Dešifrování

- $K = Ca^x mod\ p \leftrightarrow K.K^{-1} = 1(mod\ p)$
- $P = K^{-1} Cbmod\ p$

El Gamalův systém - šifrování - příklad

- $P = 100$
- $p = 139,\ g = 3,\ x = 12,\ k = 52$
- $VK = ?$
- $SK = ?$
- $C = ?$
- $P = ?$ (zkouška)

El Gamalův systém - šifrování - příklad

- $P = 100$
- $p = 139,\ g = 3,\ x = 12,\ k = 52$

Výpočet VK, SK

- $y = g^x mod\ p = 3^{12} mod\ 139 = 44$
- $VK = \{y,\ g,\ p\} = \{44,\ 3,\ 139\}$
- $SK = x = 12$

Šifrování

- $K = y^k mod\ p = 44^{52} mod\ 139 = 112$
- $Ca = g^k mod\ p = 3^{52} mod\ 139 = 38$
- $Cb = P.K\ mod\ p = 100.112\ mod\ 139 = 80$

Dešifrování

- $K = Ca^x mod\ p = 38^{12} mod\ 139 = 112 \leftrightarrow$ $K.K^{-1} = 1(mod\ p) = 36$
- $P = K^{-1} Cb\ mod\ p = 36 \times 80\ mod\ 139 = 100$

Metoda eliptických křivek

- 1985 - návrh metody: Neal Koblitz a Victor S. Miller (nezávisle)
- založena na algebraických strukturách eliptických křivek nad konečnými poli
- více viz kniha [2]

Taher El Gamal,
"A public key cryptosystem and a signature scheme based on discrete logarithms,"
in *Proceedings of CRYPTO 84 on Advances in cryptology*, New York, NY, USA, 1985, pp. 10–18, Springer-Verlag New York, Inc.

Alfred J. Menezes,
Elliptic Curve Public Key Cryptosystems,
Springer, 1993.