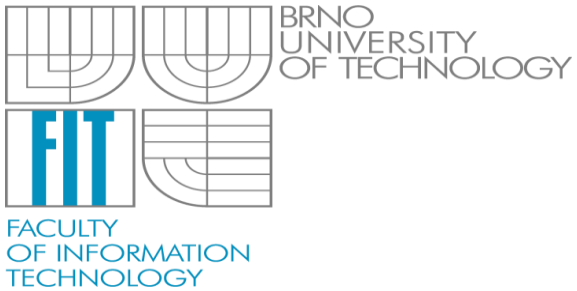
Asymetrická kryptografie a elektronický podpis

Ing. Dominik Breitenbacher
ibreiten@fit.vutbr.cz
Mgr. Radim Janča
ijanca@fit.vutbr.cz



Obsah cvičení

- Asymetrická, symetrická a hybridní kryptografie Kryptoanalýza
- Elektronický podpis a hašovací funkce
- Matematické problémy, na kterých je založena asymetrická k.
- RSA
- Faktorizace RSA

- **Symetrické šifry**
- symetrický klíč stejný pro šifrování i dešifrování
- výrazně rychlejší než asymetrická kryptografie
- nutnost sdílet stejný klíč – problém spolehlivé distribuce
- doporučená velikost klíče – 128, 256, 512 bitů
- příklady symetrických šifer – AES, DES, Blowfish, Serpent

- **Asymetrické šifry**
- - klíčový pár – veřejný a soukromý klíč
- - veřejný klíč – použití pro šifrování nebo ověření podpisu
- - soukromý klíč – použití pro dešifrování nebo vytvoření podpisu
- - doporučená velikost klíče – 1024(!), 2048, 4096 bitů
- - příklady asymetrických šifer – RSA, Diffie-Hellman, ElGamal

Hybridní šifrování

- Kombinuje výhody symetrické a asymetrické kryptografie
  - Rychlost šifrování vs. jednoduchá distribuce klíčů
  - Symetrické šifry mohou být až 100000x rychlejší než asymetrické

- Postup šifrování vstupních dat:
  1. Vygenerujeme náhodný symetrický klíč (musí sdílet obě strany)
  2. Tímto klíčem zašifrujeme vstupní data
  3. Pomocí veřejného klíče příjemce zašifrujeme symetrický klíč
  4. Odešleme zašifrovaná data a zašifrovaný klíč
  5. Příjemce pomocí svého privátního klíče dešifruje symetrický klíč
  6. Pomocí symetrického klíče (předán bezpečným způsobem) dešifruje data

- **Elektronický podpis zajišťuje:**
  - integritu
  - autenticitu podepsaného
  - nepopiratelnost
  - na rozdíl od šifrování nic neutajuje

- **Hašovací funkce**
  - Asymetrická kryptografie je pomalá, abychom podepisovali celý dokument
  - Podepisuje se pouze haš dokumentu vytvořená hašovací funkcí
  - Typicky se používá hašovací funkce z rodiny SHA (160, 384, 512 bitů)
  - Hašovací funkce musí splňovat několik vlastností:
    Odolnost vůči získání předlohy, Odolnost vůči získání jiné předlohy, Odolnost vůči nalezení kolize

- **Generování klíčů**
  - Zvolíme dvě různá prvočísla p, q
  - Spočteme $n = p*q$ *(veřejný modulus)*
  - Dále $\varphi = \pi(p)*\pi(q) = (p-1)*(q-1)$
  - Volba náhodného přirozeného e, $1 < e < \varphi$, $GCD(e, \varphi) = 1$
  - Vypočteme d tak, že $e*d \equiv 1 \bmod \varphi$ neboli $d \equiv e^{-1} \bmod \varphi$
  - Veřejný klíč je dvojice *(n, e)*, privátní klíč je dvojice *(n, d)*

- **Šifrování a dešifrování**
  - zpráva m, $0 \leq m \leq n - 1$
  - šifrovaná zpráva $c = m^e \bmod n$
  - původní zpráva $m = c^d \bmod n$

1. Jeden z účastníků zveřejní čísla α, m, která jsou společná
2. Každý účastník komunikace zvolí vlastní parametr Alice a a Bob b
3. Alice a Bob spočte hodnotu $A = \alpha^a \bmod m$, $B = \alpha^b \bmod m$
4. $K = \alpha^{a.b} \bmod m = B^a \bmod m = A^b \bmod m$

- protokol slouží k ustanovení společného tajemství
- protokol je postaven na problému diskrétních logaritmů
- protokol je zranitelný útokem typu man-in-the-middle

- **Problém faktorizace velkých čísel (RSA)**
  - násobení čísel je snadné (výpočetně, časově)
  - problém faktorizace velkého čísla je NP problém (viz dále)

- **Diskrétní logaritmus (Diffie-Hellman, ElGamal)**
  - mějme čísla *Y, α, m, k, kde α je generátorem cyklické grupy*
  - $Y = \alpha^k \bmod m$
  - číslo *k nazveme diskrétním logaritmem čísla Y při základu α*
  - *číslo k není tímto vztahem určeno jednoznačně, se vzrůstající hodnotou čísla k se zvyšuje náročnost výpočtu*

- **Generování klíčů**
  - Zvolíme dvě různá prvočísla p, q
  - Spočteme $n = p*q$ *(veřejný modulus)*
  - Dále $\varphi = \pi(p)*\pi(q) = (p-1)*(q-1)$
  - Volba náhodného přirozeného e, $1 < e < \varphi$, $GCD(e, \varphi) = 1$
  - Vypočteme d tak, že $e*d \equiv 1 \bmod \varphi$ neboli $d \equiv e^{-1} \bmod \varphi$
  - Veřejný klíč je dvojice *(n, e)*, privátní klíč je dvojice *(n, d)*

- **Šifrování a dešifrování**
  - zpráva m, $0 \leq m \leq n - 1$
  - šifrovaná zpráva $c = m^e \bmod n$
  - původní zpráva $m = c^d \bmod n$

RSA – Trochu matematiky před příkladem

- Horní celá část

  $a = \lceil n \rceil$

  $\lceil 5.6 \rceil = 6$

  $\lceil 5.1 \rceil = 6$

- Modulo – Dělení, ale zajímá nás pouze zbytek

  7 mod 3 = 1

  6 mod 2 = 0

- Pro jednoduchost si povolíme, že ≡ = =
- a^2 – čtverec

RSA – Příklad – Generování klíčů

- Zvolíme $p = 47$ a $q = 59$
- $\varphi = (47 - 1)*(59 - 1) = 2668$
- Zvolíme $e = 17$
- Pak $d = 17^{-1} \bmod 2668 = 157$

- Veřejný klíč $k_{pub} = (2773, 17)$
- Soukromý klíč $k_{priv} = (2773, 157)$

- Zadání:

  Zašifrujte text: ,,ITS ALL“ , znaky abecedy jsou reprezentovány celým číslem, které reprezentuje jejich pozici v abecedě. Tzn. A = 01, …, Z = 26, mezera = 00.

- Řešení:

  ITS ALL = 0920 1900 0112 1200

  $C_1 = 0920^{17} \bmod 2773 = 0948$

  $C_2 = 1900^{17} \bmod 2773 = 2342$

  $C_3 = 0112^{17} \bmod 2773 = 1084$

  $C_4 = 1200^{17} \bmod 2773 = 1444$

  Zašifrovaná zpráva: 0948 2342 1084 1444

- Přijatá zpráva: 0948 2342 1084 1444

- Řešení:

  $M_1 = 0948^{157} \bmod 2773 = 0920$

  $M_2 = 2342^{157} \bmod 2773 = 1900$

  $M_3 = 1084^{157} \bmod 2773 = 0112$

  $M_4 = 1444^{157} \bmod 2773 = 1200$

- Podepisování:

  $S = M^d \bmod n$

- Proces, při kterém se snažíme zpětně nalézt faktory složeného čísla
- Nelze efektivně řešit v polynomiálním čase (NP-problem) – co to znamená?

Délka čísla	Doba faktorizace
40 dec	1,32s
50 dec	10,72s
60 dec	32,23s
70 dec	9m 44s
80 dec	1h 54m
90 dec	5h 58m
100 dec	2d 16h 13m

- 60 dekadických číslic:

  397065232130193047814752568290263592317550422290020341635017

- Zkusmé dělení (Metoda kanadských dřevorubců):
  - Nejjednodušší faktorizační metoda
  - Exponenciální složitost
  - V každém kroku pouze inkrementuje dělitele a zkouší, zda zadané číslo je dělitelné tímto dělitelem
  - Př: Faktorizujte číslo n = 35 metodou zkusmého dělení:

    35 / 3 = 11 zb. 2 X

    35 / 4 = 8 zb. 3 X

    35 / 5 = 7 zb. 0 => Výsledek je 35 = 5*7

  - Nápady na vylepšení?

- Fermatova metoda:
  - Efektivní pro faktorizaci čísla složeného ze sobě blízkých čísel
  - Exponenciální složitost
  - Základ nejpoužívanějších metod
  - Založena na:

    $n = a^2 - b^2 = (a - b)*(a + b)$
  - Což lze přepsat do tvaru:

    $b^2 = a^2 - n$
  - Nejdříve nastavíme *a* na:

    $a = \lceil \sqrt{n} \rceil$
  - Pokud rovnice neplatí, inkrementujeme *a* o 1 a znovu ověříme platnost rovnice

Faktorizace RSA – Fermatova metoda – Příklad

- Faktorizujte číslo n = 1649 Fermatovou metodou

$$a = \lceil \sqrt{n} \rceil$$

$x = 41^2 - 1649 = 32$

$x = 42^2 - 1649 = 115$

$x = 43^2 - 1649 = 200$

⋮

$x = 57^2 - 1649 = 1600 = 40^2 = b^2$

$n = 57^2 - 40^2 = (57 - 40)*(57+40) = 17*97$

- Pollardova *p – 1* metoda:
  - Exponenciální složitost
  - Založena na Malé Fermatově větě: $a^{p-1} \equiv 1 \bmod p$
  - Pokud chceme pokrýt *m* prvočísel, pak volíme $M = (p_1 - 1)* \ldots *(p_m - 1)$
  - Položíme tedy $c = a^M - 1$
  - Pokud je zadané číslo *n* dělitelné některým prvočíslem p, pak bude platit:

    $GCD(c, n) = p$

- Faktorizujte číslo n = 133 Pollardovou *p – 1* metodou
- Řešení:

  Odhadneme, že číslo bude dělitelné jedním z prvních 3 lichých prvočísel, tzn. 3, 5 nebo 7.

  Vytvoříme tak M = (3 – 1)*(5 – 1)*(7 – 1) = 48 a $a = 2$

  Položíme $c = a^M - 1 = a^{48} - 1 = 2^{48} - 1 = 281474976710655$

  Výsledkem je GCD(281474976710655, 133) = 7 a tedy n = 7*19

- Co ale třeba n = 91 = 7*13 anebo n = 679 = 7*97 ?

  $281474976710655 = 3^2*5*7*13*17*97*241*257*673$

Faktorizace – Další metody

- Kvadratické síto – QS
- Multipolynomiální kvadratické síto – MPQS
- Samoinicializující se kvadratické síto – SIQS
- Obecné číselně teoretické síto – GNFS
- Eliptické křivky
- a další…

- Zadání naleznete na stránkách předmětu

Děkuji za pozornost