Informatika – Ochrana dat

Radim Farana

Podklady předmětu Informatika
pro akademický rok 2007/2008

Obsah

- Kryptografické systémy s veřejným klíčem,
  - výměna tajných klíčů veřejným kanálem,
  - systémy s veřejným klíčem.
- Elektronický podpis.
- Certifikační autorita.
- Metody zabezpečení komunikace.

Výměna tajných klíčů ve veřejném kanálu

- Diffie-Hellman-Merkle

Whitfield Diffie
* 5. 6. 1944
http://en.wikipedia.org/wiki/Whitfield_Diffie

Martin E. Hellman
* 2. 10. 1945
New York
http://en.wikipedia.org/wiki/Martin_Hellman

Ralph C. Merkle
* 2. 2. 1952
http://www.merkle.com/

1. Oba účastníci si zvolí dvě čísla α a q. A to zcela veřejně.
2. Každý účastník si zvolí tajné číslo X_i a odešle partnerovi Y_i jako výsledek operace:
   $Y_i = \alpha^{X_i} \bmod q$. Kde $i = 1, 2$ pro jednotlivé účastníky.
3. Po výměně vypočítají společný (sdílený) klíč K_{12}:
   $K_{12} = Y_2^{X_1} \bmod q = \alpha^{X_1 X_2} \bmod q$, pro prvního účastníka a
   $K_{12} = Y_1^{X_2} \bmod q = \alpha^{X_1 X_2} \bmod q$, pro druhého účastníka.

Systémy s veřejným klíčem

- Ze šifrovacího klíče nelze učit klíč dešifrovací.
- Funkce $k = f(k^{-1})$ je neinverzibilní.
- Jednocestná funkce (je možno snadno určit $f(x)$ a „velmi nesnadno“ $f^{-1}(x)$).
- Základní principy: zavazadlový problém, faktorizace velkých čísel.

RSA

Ronald L. Rivest
1947, Schenectady, New York
http://theory.lcs.mit.edu/~rivest/

Adi Shamir
1952
http://en.wikipedia.org/wiki/Adi_Shamir

Leonard M. Adleman
* 31. 12. 1945 San Francisco, USA
http://www.crs-lm.org/researchers/researchers.php?id=17

1. Převedeme alfanumerické vyjádření znaků na numerické (obvykle se používá ASCII kód).
2. Text rozdělíme na bloky stejné délky. Obsah jednoho bloku vyjádříme jako $\boldsymbol{x}$.
3. Zvolíme číslo $\boldsymbol{N}$, které je součinem dvou náhodně zvolených 100-místných prvočísel $\boldsymbol{N = p \cdot q}$. Číslo $\boldsymbol{N}$ má tedy 200 míst v dekadickém vyjádření. Přitom chceme, aby platilo $1 \leq \boldsymbol{x} < \boldsymbol{N}$.
4. Zvolíme šifrovací exponent **s**, tak aby byl nesoudělný s $\boldsymbol{\Phi(N)}$, tedy aby platilo $\boldsymbol{(s, \Phi(N)) = (s, (p - 1)(q - 1)) = 1}$.
5. Každý účastník zveřejní čísla $\boldsymbol{N}$ a $\boldsymbol{s}$ spolu se svou adresou v telefonním seznamu.
6. Dále najde číslo $\boldsymbol{t}$, aby vyhovovalo kongruenci $\boldsymbol{t \cdot s \equiv 1 \bmod \Phi(N)}$, respektive $\boldsymbol{t \cdot s \equiv 1 \bmod (p - 1)(q - 1)}$. Protože platí $\boldsymbol{(s, \Phi(N)) = 1}$, má tato kongruence jediné řešení.
7. K šifrování bude použita transformace $\boldsymbol{y = x^s \bmod N}$ a k dešifrování transformace $\boldsymbol{x = y^t \bmod N}$.
8. Šifrovaný text se přenáší běžným přenosovým kanálem.

RSA – příklad použití

- volíme $p = 31$, $q = 37$, odtud $N = 1147$
- určíme $\Phi(N) = (p - 1)(q - 1) = 1080 = 2^3.3^3.5$,
- zvolíme nesoudělný šifrovací exponent $s = 7$,
- určíme dešifrovací exponent $t \cdot 7 \equiv 1 \bmod 1080$, neboli $t.7 - 1 = i.1080$ $t = 463$.

RSA – realizace

- Šifrujeme: $100^7 \bmod 1147 = 803$,
- Dešifrujeme: $803^{463} \bmod 1147 = 100$,
- pro násobení v modulo N platí:
  $x.x \bmod N = (x_1N + x_2)(x_1N + x_2) \bmod N =$
  $= (x_1^2N + 2x_1x_2N + x_2^2) \bmod N = x_2\, x_2 \bmod N$,
- postupné násobení:
  $((x.x \bmod N).x \bmod N)$ ...
- Algoritmus vyžaduje t-1 násobení.

RSA – realizace rozvojem

- Provedeme-li binární rozvoj exponentu,
- $463 = 111001111_B$,
- určíme mocniny x:
  $x^2 \bmod N$, $x^4 \bmod N = x^2\, x^2 \bmod N$, ...
- a postupně násobíme:
  $((x.x^2 \bmod N).x^4 \bmod N)$ ...
- Algoritmus vyžaduje nejvýše $2(\log_2 n)$ násobení.

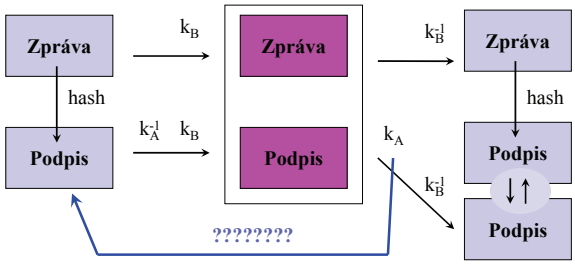
PGP

Philip Zimmermann

http://www.philzimmermann.com

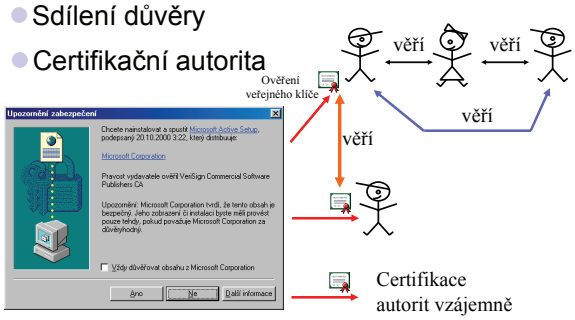
- Pretty Good Privacy
- 1991 první freeware verze.
- Tři roky vyšetřování pro narušení zákona o zákazu vývozu kryptografického software
- RSA a/nebo DH systém pro šifrování náhodného tajného klíče IDEA (International Data Encryption Algorithm)
- Řešení elektronického podpisu

Elektronický podpis

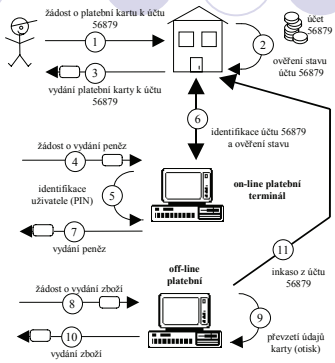


Certifikační autorita

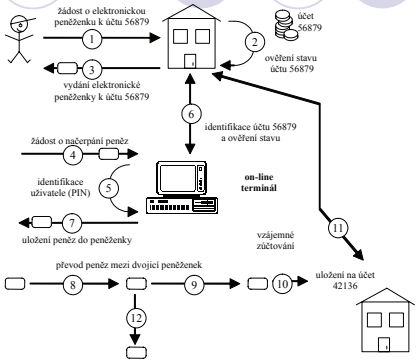
- Sdílení důvěry
- Certifikační autorita



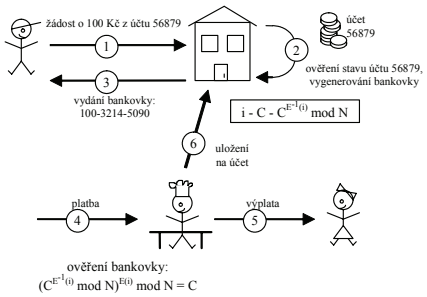
Platební karta



Elektronická peněženka

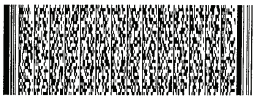


Elektronické peníze



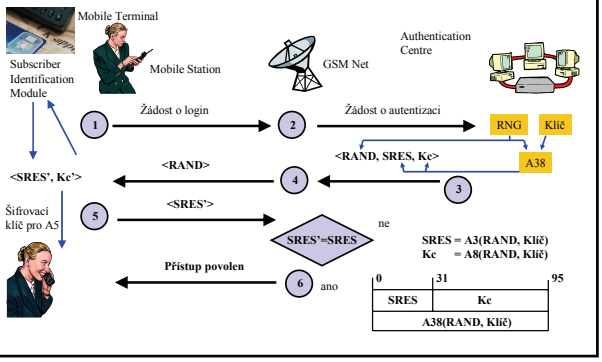
Základní požadavky

- nepadělatelnost
- možnost ověření platnosti bankovky
- přenositelnost z osoby na osobu (fax, e-mail,...)



- anonymita plateb (neidentifikovatelnost)
- nízké náklady na výrobu
- dělitelnost
- problém dvojí úhrady

Zabezpečení mobilní komunikace



Vlastní komunikace