

Cryptofest 2003

Stručný a praktický úvod
do kryptografie

Juraj Ziegler
e@hq.sk

Obsah

- prečo šifrovať
- “ekonomika” šifrovania
- rozdelenie šifier
 - symetrické vs. asymetrické
 - blokové vs. prúdové
 - šifra vs. kontrolný súčet
- výhody a nevýhody
- prax
- odkazy

Prečo šifrovať?

- básnicka otázka
- aby sme obmedzili prístup a pochopenie informácií na vybranú skupinu osôb
- zabezpečili ich nezmeniteľnosť počas prenosu

Ekonomika šifrovania

E = energia a náklady útočníka na prekonanie

Z = zisk útočníka zo získaných informácií

⇒ šifrovať tak aby $E > Z$ (útok sa neoplatí)

- formy útokov

- hrubou silou – časovo náročné (1bit ⇒ 2x čas)

- kryptoanalýza – algoritmicky náročnejšie

- časové hľadisko

- ako dlho musí ostať informácia chránená

Ekonomika šifrovania

- šifrovanie = informácie, algoritmus, kľúč
- čo z toho utajiť?
 - informácie
 - kľúč
- prečo nie algoritmus?
 - možnosť peer review či nemá slabiny
 - security by obscurity nefunguje
 - ak má slabiny, utajenie ich neskrýje

Symetrické šifry

- pri šifrovaní rovnaký kľúč ako pri dešifrovaní
- šifrovanie: $X=EA(K, I)$
- dešifrovanie: $I=DA(K, X)=DA(K,EA(K,X))$
- potreba bezpečne preniesť na K druhej strane
- $d(K) \ll d(I)$
- výnimka Vernamova šifra - $d(K) = d(I)$
 - ⇒ nemožnosť kryptoanalýzy, útok hrubou silou tiež prakticky nemožný
 - ⇒ ak prenesieme bezpečne K, mohli sme aj I

Symetrické šifry

– DES

- klíč 56 bitov
- překonaný, útok hrubou silou v reálnom čase

– TripleDES

- klíč 112 bitov
- encode, decode, encode cyklus

– AES (=Rijndael)

- klíč 128, 192, 256

– Blowfish, Twofish, IDEA, Serpent, ...

Asymetrické šifry

- pri šifrovaní iný kľúč (časť kľúča) ako pri dešifrovaní
- jeden algoritmus pri oboch operáciách
- $X = A(I, PK1, VK2)$
- $I = A(X, PK2, VK1) = A(A(I, PK1, VK2), PK2, VK1)$
- PK – privátny kľúč, VK – verejný kľúč
- VK je možné prenášať nezabezpečeným kanálom, PK je nutné chrániť.

Asymetrické šifry

– RSA

- priekopník
- faktorizácia veľkých čísiel
- od 512b vyššie

– El-Gamal

- problém diskretného logaritmu
- od 768b

– DSA

- 512b – 1024b

Blokové vs. prúdové šifry

- bloková
 - pracuje nad blokom dát pevnej dĺžky
 - rovnaké vstupné bloky → rovnaké výstupné
 - ⇒ spätná väzba – výstup sa primieša do vstupu
 - nutnosť doplniť vstup na hranicu bloku
- prúdová
 - stavový automat – PRNG, každý stav – 1 bit
 - logický súčet so vstupom
 - so spätoväzobnými registrami rýchlejšie ako bl.

Šifra vs. kontrolný súčet

- šifra
 - z výsledku dostaneme späť vstup
 - $d(I) = d(X)$
 - ochrana informácií pred čítaním/zmenou
- kontrolný súčet
 - jednosmerná operácia
 - $d(X) = \text{konštanta}$
 - test zmeny informácií

Kontrolný súčet

- SHA-1
 - 160b
- MD5
 - 128b
 - nájdená kolízia
- MD4
 - známe a potvrdené kolízie
 - kolízia v “použitel’nom” texte

Výhody a nevýhody

- symetrická

- + rýchlejšie
- + menej náročné na CPU
- potreba preniesť kľúč druhej strane bezpečným kanálom

- asymetrická

- + prenos potrebných častí kľúčov cez nebezpečné prostredie
- náročnejšie na CPU
- pomalšie

Prax

- **asymetrické šifry**
 - overenie identity komunikujúcich strán
 - vytvorenie bezpečného kanálu
- **symetrické šifry**
 - šifrovanie samotných informácií
 - náhodný kľúč
 - prenesený pomocou asymetrických šifier
- **kontrolné súčty**
 - kontrola nezmenenosti informácií

Odkazy

- <http://schneier.com>
- <http://www.rsasecurity.com/rsalabs/technotes/>
- <http://www.ssh.fi/support/cryptography/>
- Matematika 5D :)

Otázky

?