Symetrické šifry, DES

Jiří Vejrosta

Fakulta jaderná a fyzikálně inženýrská, ČVUT

Klíče

- Symetrická šifra
  - tajný klíč
  - klíč stejný u odesilatele i příjemce
- Asymetrická šifra
  - k šifrování se užívá veřejného klíče
  - příjemce dešifruje prostřednictvím svého soukromého klíče
  - přibližně 50 krát pomalejší než symetrické šifrování

Typy symetrického šifrování

- Bloková šifra
  - šifruje po blocích určité délky
- Proudová šifra
  - šifruje po jednotlivých znacích
  - dvakrát rychlejší než bloková šifra
- MAC
  - authentization code
  - slouží k ověřování původu dat

Blokové šifry

- působí na bloky dat dané délky, většinou 64 nebo 128 bitů
- šifrovány pomocí tajného klíče
- bloky stejné délky b
- zprávu m zašifrujeme užitím klíče k délky κ z prostoru klíčů $\mathcal{K}$ na šifrovanou zprávu c
- $c = \mathrm{ENC}_k(m)$
- $m = \mathrm{DEC}_k(c)$

Blokové šifry

Jak vybírat klíč a odkud

Pro daný klíč, b-bitovou blokovou šifru zobrazíme množinu $\mathcal{M}$ 2^b b-bitových vstupů na stejnou množinu 2^b b-bitových výstupů.

$$\mathcal{M} = \{\overbrace{0\ldots00}^{b}, \overbrace{0\ldots01}^{b}, \overbrace{0\ldots10}^{b}, \ldots, \overbrace{1\ldots1}^{b}\}$$

Toužíme po tom, aby každý možný výstup bloku byl užit nejvýše jednou. Zobrazení je permutací vstupu. Použitím nového klíče obdržíme novou permutaci.

Blokové šifry

- b určuje počet možných permutací
- κ je počet generovaných permutací
- 2^{κ} možných klíčů
- počet všech permutací tedy je $(2^b)! \overset{\text{Stirling}}{\approx} 2^{(b-1)2^b}$
- volíme pouze z malého zlomku všech permutací
- permutace je třeba volit tak, aby mezi nimi nebylo možno vypozorovat žádný vztah

DES

- Data Encryption Standard
- symetrický klíč, bloková šifra
- jedna z nejčastěji implementovaných šifer na světě

Historie DES

- 1973 - US National Bureau of Standards vypisuje soutěž na blokovou šifru pro federální účely
- 1975 publikován - předpokládaná trvanlivost 10 let
- již v době vzniku pochyby o jeho bezpečnosti, stroj na prolomení měl však vysokou odhadní cenu
- v 70. a z části v 80. letech neúspěšné pokusy o prolomení
- 1993 - kryptoanalytik Matsui - lineární kryptoanalýza
- 1994 - skutečně zrekonstruován klíč - 40 dní nepřetržitého počítání
- 1998 - DES Cracker - na hardwaru založený kompletní vyhledávač klíče
- 2004 - DES oficiálně stažen, nástupcem je Triple-DES

Parametry DES

- 64 bitové bloky
- 56 bitový klíč
- bity číslujeme $\{1 \ldots 64\}$

Feistelova šifra

- jednoduchá varianta DES
- b-bitová šifra
- r sérií identické struktury - roundovací funkce a výměna
- $\frac{b}{2}$ bitů projde postupně roundovacími klíči $k_1, \ldots, k_r$
- po použití roundovací funkce výměna bitů

Feistelova šifra

Formální zápis

Mějme vstupní zprávu m, kde $m = (u_0 \parallel v_0)$, u_0, v_0 jsou 32-bitové řetězce a $\parallel$ je operátor bitového zřetězení.
Další hodnoty u_i, v_i pro $1 \leqslant i \leqslant r$ jsou generovány pomocí roundovací funkce $f(\cdot, \cdot)$ a šifrovaného textu daného jako $c = (u_r \parallel v_r)$ vztahy

$$\left.\begin{aligned} v_i &= u_{i-1} \oplus f(v_{i-1}, k_i), \\ u_i &= v_{i-1}, \end{aligned}\right\} \quad \text{pro} \quad 1 \leqslant i \leqslant r-1$$

$$\begin{aligned} v_r &= u_{r-1} \oplus f(v_{r-1}, k_r), \\ u_r &= v_{r-1}, \end{aligned}$$

Roundovací funkce DES

- expanze ze 32 na 48 bitů (zdvojení části vstupu)
- užití roundovacího klíče
- bity rozděleny do 8 skupin po 6 - užití v S-boxech
- S-box vrátí 32 bitů
- permutace

Roundovací klíč

- 56 bitový klíč (původně 64 bitů, každá osmý ven z parity)
- permutační volba 1 (PC1) rozdělí 56 bitů na dvě 28 bitové části
- PC2 je dá dohromady a vytvoří 48 bitový klíč

S - box

- jediná nelineární komponenta šifry
- ze skupiny 6 bitů vrací 4 bity
- ze 48 tedy dostáváme 32 bitů
- 4 řádky permutací čísel $\{0 \ldots 15\}$
- dva vnější bity vyberou řádek, zbylé 4 sloupec
- vyhledané číslo je návratovou hodnotou

triple - DES

- 3 užití DES
- máme tedy klíč efektivní kryptografické síly délky 168 bitů
- běžně užívána verze 112 bitů
- softwarově náročnější

triple - DES

- mějme klíče (k_1, k_2, k_3), různé varianty
- 2-klíčový $\mathrm{ENC} - \mathrm{DEC} - \mathrm{ENC}$ $\quad c = \mathrm{ENC}_{k_1}(\mathrm{DEC}_{k_2}(\mathrm{ENC}_{k_1}(m)))$
- 2-klíčový $\mathrm{ENC} - \mathrm{ENC} - \mathrm{ENC}$ $\quad c = \mathrm{ENC}_{k_1}(\mathrm{ENC}_{k_2}(\mathrm{ENC}_{k_1}(m)))$
- 3-klíčový $\mathrm{ENC} - \mathrm{DEC} - \mathrm{ENC}$ $\quad c = \mathrm{ENC}_{k_3}(\mathrm{DEC}_{k_2}(\mathrm{ENC}_{k_1}(m)))$
- 3-klíčový $\mathrm{ENC} - \mathrm{ENC} - \mathrm{ENC}$ $\quad c = \mathrm{ENC}_{k_3}(\mathrm{ENC}_{k_2}(\mathrm{ENC}_{k_1}(m)))$

DES-Cracker

- $2^{56} \approx 72 \cdot 10^{15}$
- hrubá síla - prochází celý prostor klíčů
- stroj zbudovaný Electronic Frontier Foundation (1998)
- měl demonstrovat nedostatečnou délku klíče
- prolomí klíč přibližně za 24 hodin

AES

- Advanced Encryption Standard
- zavedeno v roce 2001
- šifra Rijndael (Daemen, Rijmen)
- bloková šifra (128 bit)
- symetrický klíč (128, 196 nebo 256 bitů)

Popis AES

- velikost bloku, resp. klíče může být libovolným násobkem 32, maximálně však 128, resp. 256 bitů
- velikost klíče AES specifikuje počet cyklů
- 10, resp. 12, resp. 14 cyklů pro 128, resp. 192, resp. 256 bitový klíč
- každý cyklus se skládá ze čtyř fází
- v první fázi dochází k rozšíření klíče - roundovací klíče jsou odvozeny ze šifrovacího klíče pomocí Rijndaelovy tabulky klíčů

Bezpečnost AES

- National Security Agency (NSA) považuje AES za dostatečně bezpečné
- 192 a 256 bitová verze užívány NSA k šifrování přísně tajných informací
- dnes se říká, že AES bude bezpečná, a tedy i používaná, přibližně 20 až 30 let (pro srovnání DES dávali 10 let života a jak to dopadlo)