

Šifrování

Kafková Petra

■ Kryptografie

- Věda o tvorbě šifer
- (z řečtiny: kryptós = skrytý, gráphein = psát)

■ Kryptoanalýza

- Věda o prolamování/luštění šifer

■ Kryptologie

- Věda o šifrování
- obecné označení pro kryptografii a kryptoanalýzu

■ Šifra/Šifrování - algoritmus $OT \rightarrow \check{S}T$, klíč

OT = otevřený text, $\check{S}T$ = šifrový text

Třídění algoritmů

- Podle počtu používaných klíčů:
 - Symetrické šifry
 - Asymetrické šifry

 - Hashovací funkce

Symetrické šifry

■ Proudové

- zpracovávají OT po bitech
- každý znak otevřeného textu je šifrován jinou transformací, kterou určuje jeho pozice a odpovídající hodnota hesla na této pozici.
- použijeme pokud není vhodné/možné čekat na zbývající znaky bloku
- malá propagace chyby

Symetrické šifry 2/2

■ Blokové

- zpracovávají OT v blocích
- všechny bloky OT jsou šifrovány toutéž transformací
- mode (volíme podle typu dat)
 - ECB mode (electronic codebook)
 - CBC mode (cipher block chaining)
 - CFB mode (cipher feedback)
 - ...
- Padding
- Inicializační vektor IV
- *DES* (IBM, 1977), *AES* (2001)

Asymetrické šifry

- Veřejný (šifrování) a soukromý (dešifrování) klíč
- **Výhody**
 - Větší bezpečnost a pohodlí používání (snazší management klíčů)
- **Nevýhody**
 - Rychlost (i 100-1000x pomalejší než konvenční šifry)
 - Náročnější generování klíče (uchováváme v “containers”, na čipových kartách, šifrovacích tokenech)
- Použití často společně s konvenčními:
OT se zašifruje SŠ s náhodně vygenerovaným klíčem. Klíč se zašifruje AŠ (PGP, SSL,...)

Hashovací funkce

- „jednosměrná kryptografie“
- Hash ze zprávy je pokaždé stejný
- Nelze identifikovat původní dokument z hashe
- Malá změna vstupu > velká změna výstupu (continuity!)
- kontrola integrity dat, rychlé porovnání dvojice zpráv, indexování, vyhledávání apod.
- vytváření tzv. otisku zprávy (message digest) → digitální podpisy

Použití šifrování

- Internet : e-mail, internetové bankovníctví, on line nákupy...
- Prokázání identity: elektronický podpis
- Kontrola přístupu : satelitní TV
- Mobilní telefony

Vernamova šifra

- jediná o které je formálně prokázáno, že je bezpečná
- ke zprávě operací XOR připojí dokonale náhodný klíč stejné délky, jako zpráva sama
- tím se problém přesune z přenesení zprávy na přenesení klíče
- Čili jediná její nevýhoda je, že je nepoužitelná

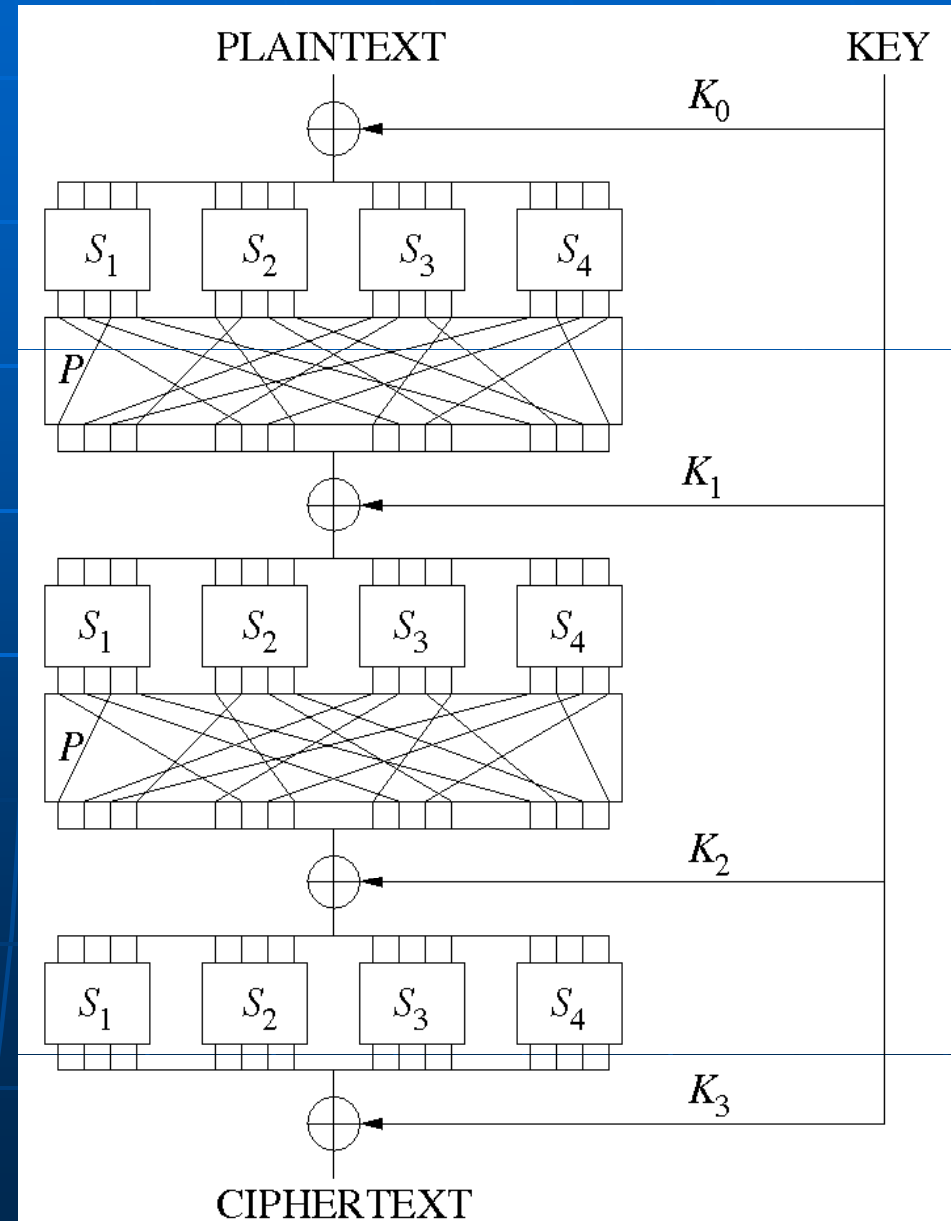
AES (Advanced Encryption Standard)

- 1997 vyhlášena veřejná soutěž amerického úřadu pro standardizaci (NIST) o federální šifrovací standard
- {zastaralý standard DES (6/97 prolomen)}
- vybrána šifra **Rijndael** (Joan Daemenem a Vincent Rijmen)

- Symetrická bloková šifra
- Bloky s pevnou délkou 128 bitů
- Délka klíče může být 128, 192 nebo 256 bitů
- Vyznačuje se vysokou rychlostí šifrování

SP network (AES)

- Substitution Permutation network (série matematických operací)
- S-box
 - One-to-one (kvůli reversibilitě)
 - Změna jednoho vstupního bitu změní cca půl výstupu
 - Každý bit výstupu závisí na všech bitech vstupních
 - “substituční šifra”
- P-box
 - Vstupem je výstup předchozího S-boxu, po permutaci je výstup P-boxu vstup pro další kolo S-boxu
 - “transpoziční šifra”
- Rychlejší než Feistel network



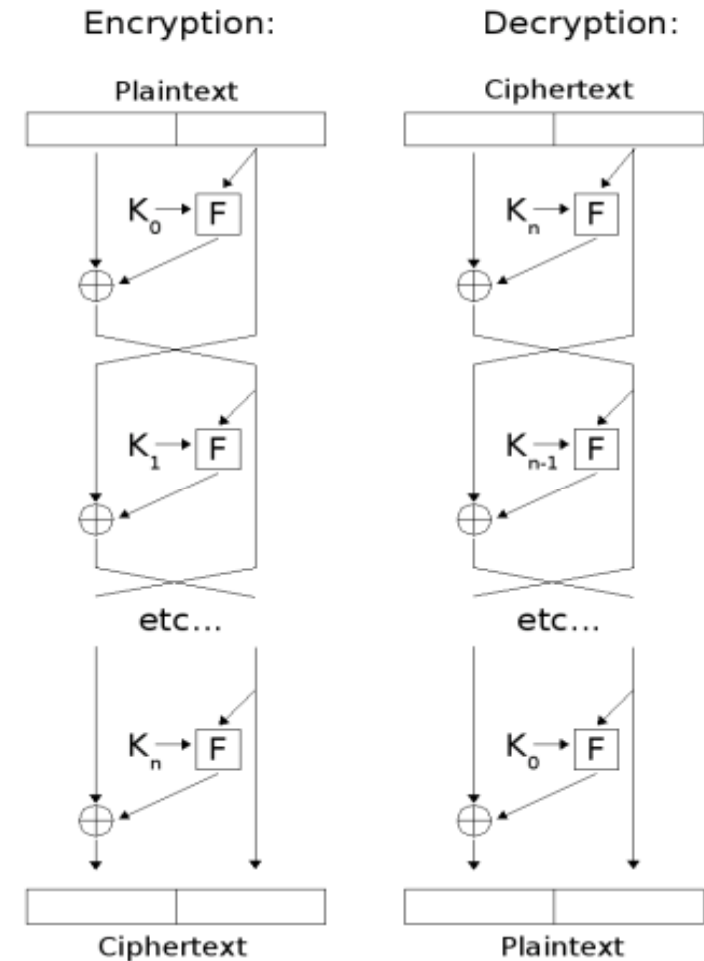
DES (Data Encryption Standard)

- Schváleno jako standard v r.1976
- Založeno na šifře Lucifer od Horsta Feistela, IBM
- Bezpečné (ale pomalé) ve formě Triple DES (aplikujeme DES třikrát s třemi různými klíči)
- DES-X, GDES,... ale nahrazeno AES

- Symetrická bloková šifra
- Délka klíče - 56-bitů (64, ale jen 56 je skutečně použito)
- Délka bloku - 64 bitů
- DES je Feistelova šifra o 16ti rundách

Feistel network (DES)

- Několikanásobná iterace jednoduchých šifrovacích fcí (iterační postup zjednodušoval implementaci pro tehdejší HW)
- Blok OT se dělí na poloviny, klíč se dělí na podklíče, každý podklíč definuje transformaci, na konci každého kola se bity levé a pravé poloviny párově zpracují operací XOR
- Výhoda oproti SP network - round function F nemusí být zvratná



Feistel Cipher

Srovnání DES a AES

| | AES | 3DES |
|--------------------------------|---|----------------------------|
| Délka klíče (bity) | 128,192,256 | 64,128,192 (56,112,168) |
| Délka bloku (bity) | 128,192,256 | 64 |
| Operace | XOR, cyklický posun, maticové sčítání a násobení v GF | XOR, permutace |
| Slabé klíče | ne | ano |
| | AES | DES* |
| čas šifrování (cycles) | 13538 | 17458 |
| Příprava algoritmu (cycles) | 2278 | 12320 |

* Hodnoty pro 3DES budou zhruba trojnásobné

Děkuji za pozornost

- Zdroje:
- <http://www.aspnet.cz/articles/147-symetricke-sifrovani-aes-rijndael-v-net.aspx>
- <http://www.aspnet.cz/Articles/148-asymetricke-sifrovani-rsa-v-net-sprava-klicu.aspx>
- <http://en.wikipedia.org/wiki/Cryptography>
- <http://www.garykessler.net/library/crypto.html#intro>
- <http://www.satcentrum.com/clanky/973/systemy-kodovani-ktery-je-ten-pravy/>
- http://en.wikipedia.org/wiki/Substitution-permutation_network
- <http://www.specnaz.cz/index.php?id=55&art=283&cat=34&l=0>
- http://www.tydlin.cz/__static/clanky-a-prace/bakalarka/kryptografie-a-jeji-aplikace-v-zabezpecenem-prenosu-souboru.pdf