UKRY - Symetrické blokové šifry

Martin Franěk (frankiesek@gmail.com)

Fakulta jaderná a fyzikálně inženýrská, ČVUT Praha

18. 3. 2013

Obsah

Typy šifer

Asymetrické šifry

- Veřejný klíč pro šifrování a privátní klíč pro dešifrování
- – Vysoká výpočetní náročnost
- \+ Není potřeba výměna tajného klíče

Symetrické šifry

- Také zvané konvenční
- „Stejný” klíč pro šifrování i dešifrování
- \+ Nízká výpočetní náročnost
  - 100 – 1000x proti asymetrickým
- – Nutnost sdílení tajného klíče
  - Lze odstranit kombinací s asymetrickými šiframi

Typy šifer

Synchronní šifry

- Klíč je nezávislý na šifrovém či otevřeném textu
- Přidání/ztráta znaku „rozbije” synchronizaci – ta se neobnoví

Nesynchronní šifry

- Klíč je závislý na N znacích otevřeného textu
- Přidání/ztráta znaku „rozbije” synchronizaci – ta se neobnoví

Asynchronní/samosynchronní šifry

- Klíč je závislý na N znacích šifrového textu
- Při přidání/ztrátě znaku se sama znovu synchronizuje po N znacích

Typy šifer

Proudové šifry

- Každý znak šifrován zvlášť
- Obvykle kombinace s pseudonáhodnou posloupností

Blokové šifry

- Otevřený text rozdělíme do bloků délky $k \in N$
- Poslední blok lze doplnit „vatou”
- Každý blok zakódovat pomocí klíče
  - Stejný klíč na všechny bloky nežádoucí
  - Různé operační mody (modes of operation)

Operační mody

ECB – Electronic code book

- Stejné bloky otevřeného textu stejný šifrový text
- Často opakované bloky lze odhadnout
- Bloky lze bez detekce vkládat / zaměňovat / odstraňovat
  - Např. záměna ’1 |00|0 K|č |’ -> ’1 |00|00|00|0 K|č |’

CBC – Cipher block chaining

- Přidává závislost aktuálního bloku na šifrovém textu předchozího bloku
- První blok závisí na „IV” - inicializační blok
  - Lze odeslat nešifrovaně

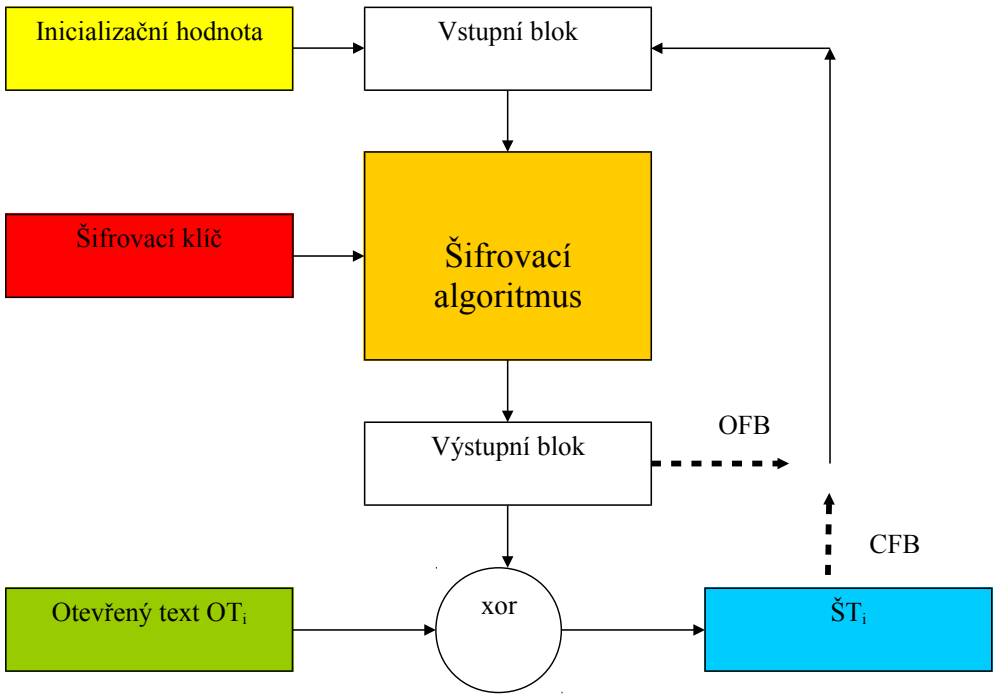
Operační mody - převod na proudovou šifru

CTR – Counter mode

- IV inicializuje čítač
- Šifruje se výstup čítače

CFB a OFB

- Šifrovací funkce se používá pro generování klíče



Vylepšení modů

Solení – Salting

- Vylepšení metod využívajících IV
- Z IV vypočteme transformací IV'
- Teprve IV' využijeme k šifrování

MAC – Message Authentication Code

- Přenos kontrolního součtu
- Zajišťuje integritu a autentizaci dat
- Ochrana proti chybám v kanále i útokům
- Šifrování jiným klíčem, než zbytek zprávy
- Možnost využití např. hashovacích funkcí

Příklady blokových šifer

Blowfish

- Autor B. Schneierem (1994)
- Velikost bloku 64 bitů a délkou klíče nejvýše 448b (tj. 56B)
- Neplacená nelicencovaná alternativu k DES
- Na rozdíl od DES dodnes nebyla prolomena

GOST

- 64-bitový blok a 256-bitový klíč
- Navržena v Sovětském svazu.

IDEA

- 64 bitový blok a 128-bitový klíč
- Považována za jeden z nejsilnějších algoritmů

RC2, RC5, atd...

Příklady proudových šifer

FISH

- Založena na zpožděném Fibonacciho generátoru s posuvným registrem

RC4 – Rivest Cipher 4 (ARC4, ARCFOUR)

- Vyvinuto 1987
- Zveřejněno 1994 (anonymně, problém s copyrightem)
- Nevyužívá posuvné registry – vhodnější pro SW implementaci
- Použití ve WEP, WPA, RDP, SSL, HTTPS

AES

Advanced Encryption Standard

- 1997 výběrové řízení NIST na nástupce DES
- 15 kandidátů, 5 ve finále
- 2001 – Rijndael zvítězil
- Délká klíče 128,192,256 bitů
- 128-bit blok
- 10, 12, 14 průchodů
- „128 bitů zaručuje utajení na několik desítek let dopředu”

Historie DES

- Data encryption standard
- 70's –Vývoj v IMB + National Security Agency
- 1973 – Ministerstvo obchodu USA vyhlašuje soutěž
  - Bezpečnost i při neutajení algoritmu
  - Dostupnost
  - Vhodnost pro různé aplikace
  - Výkon
  - Ekonomičnost
- 1974 – DES vyhrává v druhém kole
- Odvozen z interní šifry IBM Lucifer
- 1975 – Patentováno, Bezplatně k použití v USA
- 1977 – Pojmenování DES + standard

Historie DES

- Vyvinut pro ochranu citlivých dat ve státní správě (mimo armádu)
- Předpokládaná životnost 15 let
- NSA si vymohla utajení části designu (S-Boxy)
- Podezření, že jsou navrženy, aby NSA mohla dešifrovat
- 1979 – Vyšetřování zvláštní komisí
- 1988 – NSA přestává doporučovat použití DES

DES

- Data Encryption standard
- 64-bit bloky
- 56-bit klíč (7 + 1 parita) – generuje 16 48-bit podklíčů
- 16 průchodů
- Krátký klíč vlivem NSA
- Zvýšení bezpečnosti pomocí 3DES (2 – 3 klíče)
  - \+ Bezpečnější 112-bit/168-bit klíč
  - \- Pomalejší

S-DES

„Simplified DES" – pro studijní účely

8-bit blok, 10-bit klíč, 2 průchody

IP (3, 5, 2, 7, 4, 10, 1, 9, 8, 6) EP (x_4, x_1, x_2, x_3, x_2, x_3, x_4, x_1)

P_{10} (3, 5, 2, 7, 4, 10, 1, 9, 8, 6) P_8 (6, 3, 7, 4, 8, 5, 10, 9)

P_4 (2, 4, 3, 1)

S-boxy

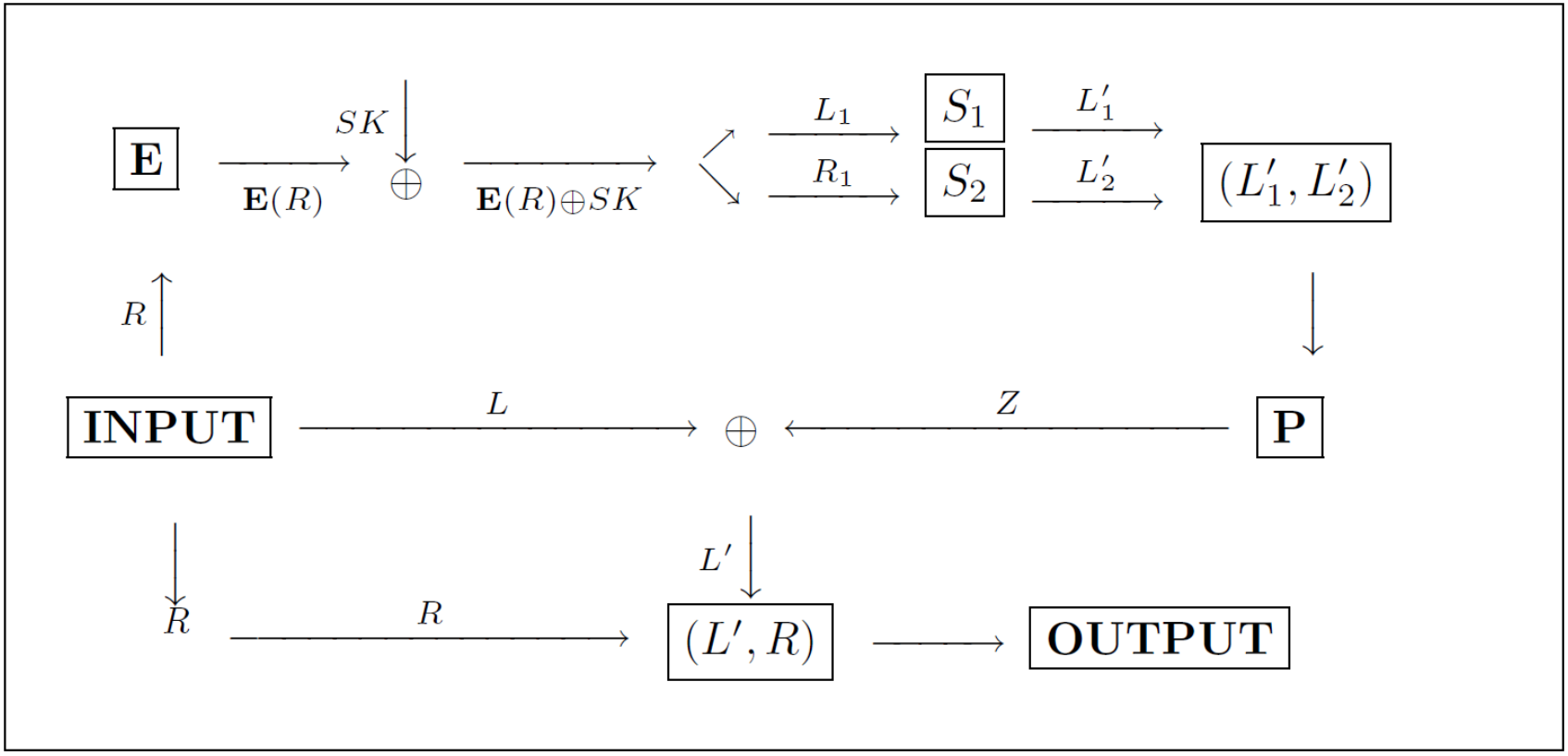
S0		x_2	0	0	1	1
		x_3	0	1	0	1
x_1	x_4					
0	0		01	00	11	10
0	1		11	10	01	00
1	0		00	10	01	11
1	1		00	01	11	10

S1		x_2	0	0	1	1
		x_3	0	1	0	1
x_1	x_4					
0	0		00	01	10	11
0	1		10	00	01	11
1	0		11	00	01	10
1	1		10	01	00	11

S-DES Algoritmus

1. Nagenerujeme si klíče S_k ze zadaného klíče
   1. P_{10}(k) rozdělíme napůl a aplikujeme LS1
   2. Na výsledek aplikujeme P_8 a získáme sk1
   3. Na výsledek LS1 aplikujeme LS2, P_8 a získáme sk2
2. Na blok otevřeného textu (m) aplikujeme $IP = INPUT$
3. INPUT rozdělíme na dvě části (L, R)
4. R rozšíříme na 8-bit pomocí $EP(R)$
5. $EP(R) \oplus S_k$ rozdělíme na dvě části $(L1, R1)$
6. $L1$ a $R1$ vstoupí do $S0$ resp $S1$
7. Výstup permutujeme pomocí $P_4 = Z$
8. $Z \oplus L = L'$
9. $OUTPUT = (L', R)$
10. Opakujeme kroky 3 – 9 (Nový INPUT je SW(OUTPUT))
11. Výstup permutujeme IP^{-1}

S-DES Algoritmus



S-DES Příklad

1. $k = (0010010111), P_{10}(k) = (1000010111)$, $LS1(10000, 10111) = (0000101111), P_8(0000101111) = (00101111) = sk1$, $LS2(00001, 01111) = (0010011101)$, $P_8(0010011101) = (11101010) = sk2$
2. $m = (10100101), IP(m) = (01110100) = INPUT$
3. $L = (0111) R = (0100)$
4. $E(0100) = (00101000), (00101000) \oplus (00101111) = (00000111), L1 = (0000), R1 = (0111)$
5. $S0(0000) = (01) = L'_1, S1(0111) = (11) = L'_2$
6. $P_4(0111) = (1110) = Z, L \oplus Z = (0111) \oplus (1110) = (1001) = L'$
7. $OUTPUT = (L', R) = (10010100)$
8. $INPUT = SW(OUTPUT) = (01001001)$
9. a zopakujeme kroky $2 - 8$ (vyjde $OUTPUT = (01101001)$)
10. $IP^{-1}(01101001) = (00110110) =$ šifrový text

Literatura

[1] Richard A. Mollin. An Introduction to Cryptography (second edition). Chapman & Hall/CRC, 2007
Označení ve školní knihovně B17526

[2] http://kmlinux.fjfi.cvut.cz/~balkolub/Vyuka/leto2012/DES_Kopecky.pdf

[3] http://kmlinux.fjfi.cvut.cz/~balkolub/Vyuka/leto2011/Havlicek.pdf

[4] http://owebu.bloger.cz/Bezpecnost/Sifrovani-Symetricke-sifrovani

[5] http://www.karlin.mff.cuni.cz/~tuma/ciphers08/sifry7.ppt

[6] http://www.wikipedia.org/