Operační mody blokových šifer a hašovací algoritmy

RNDr. Vlastimil Klíma
vlastimil.klima@i.cz

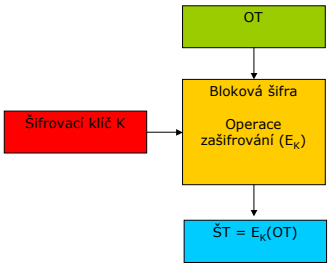
ICZ

Operační mody blokových šifer

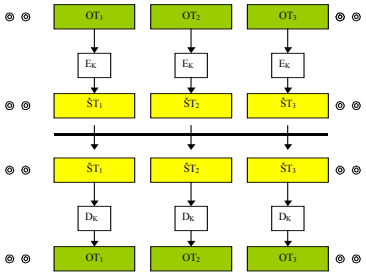
Operační mody blokových šifer

- **způsob použití blokové šifry k šifrování dat**
- dříve FIPS Pub. 81: ECB, CBC, CFB, OFB a v dodatku zmíněn i MAC, MAC v normě ISO 9797
- nyní doporučení NIST ve zvláštní publikaci "A special publication, SP 800-38A, "Recommendation for Block Cipher Modes of Operation" ,12/2001, definuje navíc čítačový modus (CTR), nedefinuje MAC, naznačuje, ale nedefinuje doplňováání
- draft SP-800-38B, definuje RMAC
- vše na www.nist.gov

Bloková šifra



ECB - Electronic Codebook - modus elektronické kódové knihy



Útoky na operační modus ECB

- **pasivní útok**: informace, vyplývající ze shody bloků šifrových textů (databáze)
- Blokové šifry, stejně jako proudové, také samy o sobě nezajišťují *integritu* dat – **aktivní útoky** vložením, vynecháním, opakováním aj. manipulací bloků šifrového textu (databáze, přenos)

databáze platů .....os.č. 162 ...**025** 103,-Kč ....os.č. 163 ...**027** **038**,-Kč .....
kajsůkuiůooiwpqwqqwekaouiolwerkweiosdvůoipášqpéáčcéůywuíta3tdszj34hkf...

..... 3tdszj34 j7čžuths **bgžc4rš7** rg43č7řz .....
..... převeďte 1 0 0 0 ,- Kč .....

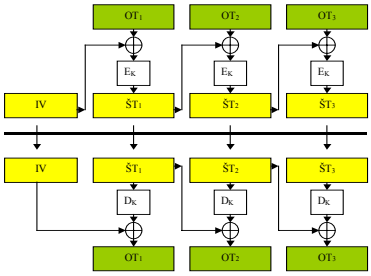
..... 3tdszj34 j7čžuths **bgžc4rš7** **bgžc4rš7** rg43č7řz .....
..... převeďte 1 0 0 0 0 0 0 ,- Kč .....

Použití

- malý blok – existuje slovníkový útok
- šifrování *náhodně* generovaných klíčů nižší úrovně

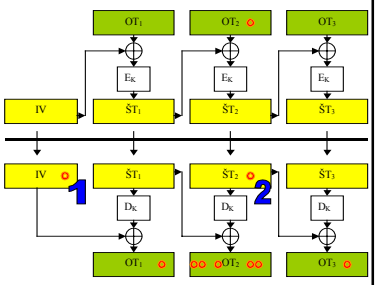
CBC - Cipher Block Chaining - řetězení šifrových bloků

- náhodný IV
- další náhodné masky tvoří předchozí bloky ŠT
- stejné bloky OT – různé bloky ŠT
- skryté kanály (IV)

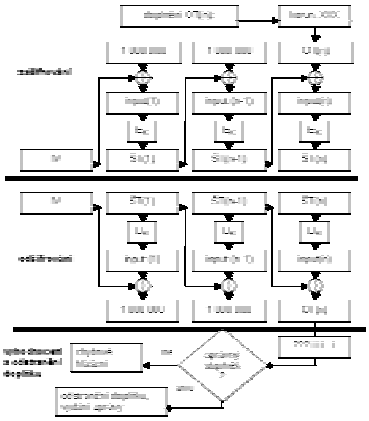


CBC

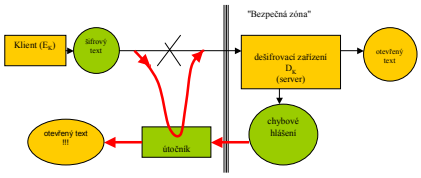
- řetězovitá závislost na OT, ŠT
- ke správnému dešifrování daného bloku OT je potřeba správný předchozí a daný blok ŠT
- odtud plyne samosynchronizační vlastnost na úrovni bloků (chybný blok, výpadek celého bloku)
- jaký je vliv jednobitové chyby v ŠT? - viz 1, 2



CBC

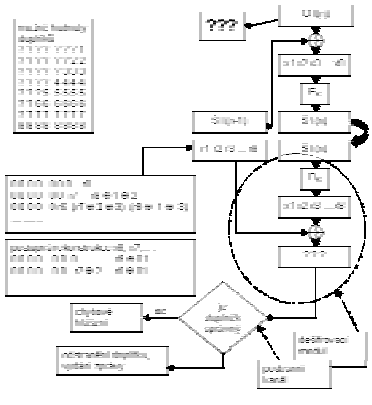


Postranní kanál v modu CBC



- popis útoku Vaudenay 2002
- složitost v průměru 128 krát počet bajtů zprávy
- **výsledkem je celý otevřený text**

Jak to, že to nebylo objeveno dříve?



Protiopatření

- organizační (lze obcházet)
- kryptografická (aby chybové hlášení nedávalo užitečnou informaci)
- Cryptology ePrint Archive: Report 2002/061, http://eprint.iacr.org/2002/061.pdf

Strengthened Encryption in the CBC Mode

Vlastimil Klíma [1] and Tomáš Rosa [1,2]

[1] ICZ, V Olšinách 75, 100 97 Prague 10, Czech Republic, http://www.i.cz
[2] Department of Computer Science and Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Karlovo náměstí 13, 121 35 Prague 2, Czech Republic
{vlastimil.klima, tomas.rosa}@i.cz

May 24, 2002

Zesílené šifrování v modu CBC - varianty

A: $y_N = E_{K4}(D_{K2}(x_N) \oplus E_{K3}(y_{N-1}))$

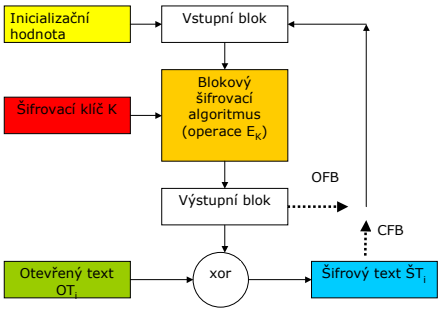
B1: $y_N = E_{K4}(D_{K2}(x_N) \oplus E_{K3}(y_{N-1}) \oplus y_{N-1})$

B2: $y_N = E_{K4}(D_{K2}(x_N) \oplus h(E_{K3}(y_{N-1}))$

C: $y_N = E_{K1}(D_{K1}(x_N) \oplus E_{K1}(y_{N-1}) \oplus y_{N-1})$

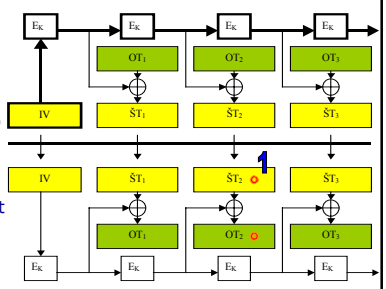
Klíče K2, K3, K4 derivovány jednosměrně z K1

Blokové šifry v proudovém modu CFB a OFB: Cipher/Output Feedback – zpětná vazba ze šifrového textu nebo z výstupu



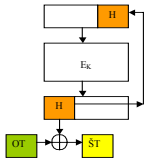
OFB - Output Feedback - zpětná vazba z výstupu

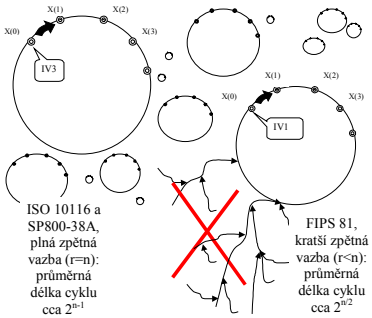
- čistě proudová šifra
- používá pouze E_K
- nulová propagace chyby (1), nesmí vypadnout ani bit
- útoky na OFB - jako na proudové šifry (integrita) + dvojí použití hesla
- kdy by mohlo nastat dvojí použití hesla ?
  - pro nový OT – nutný nový IV
  - perioda hesla?



OFB - Output Feedback - zpětná vazba z výstupu

- konečný automat, podle délky zpětné vazby vytváří strukturu cyklů (s/bez ocásků)
- IV nastavuje jeden z cyklů



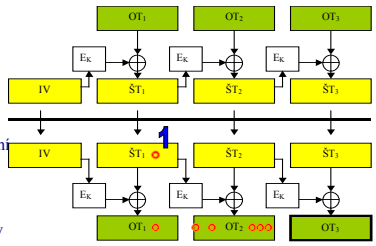


ISO 10116 a SP800-38A, plná zpětná vazba (r=n): průměrná délka cyklu cca 2^{n-1}

FIPS 81, kratší zpětná vazba (r<n): průměrná délka cyklu cca $2^{n/2}$

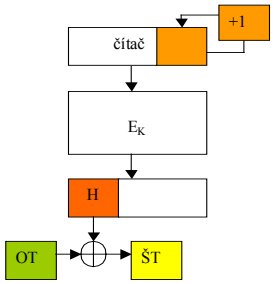
CFB - Cipher Feedback - zpětná vazba ze šifrového textu

- proudová šifra
- používá pouze E_K
- řetězovitá závislost na OT, ŠT
- ke správnému dešifrování je nutný správný předposlední a poslední blok ŠT
- vliv jednobitové chyby v ŠT
- samosynchronizační vlastnost na úrovni bloků (chybný blok, výpadek celého bloku)



CTR – Counter mode – čítačový modus

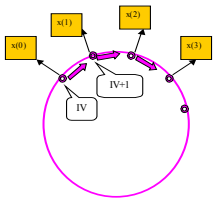
- „nový modus" (1979, D+H)
- čistě proudová šifra
- používá pouze E_K
- výstup lze použít celý nebo část
- různé způsoby inkrementace
- čítač se může týkat jen (dolní) části registru „IV"
- smysl je zaručit různé hodnoty čítače použité během životnosti jednoho klíče



- **hlavní výhoda:** heslo může být vypočítáno jen na základě pozice a IV, nezávisle na ničem jiném

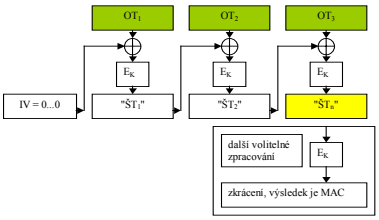
CTR

- konečný automat
- vytváří pouze **jeden** dlouhý cyklus
- IV nastavuje bod v tomto cyklu
- modus definován v SP 800-38A



MAC - Message Authentication Code – autentizační kód zprávy

- podle ISO 9797, SP800-38A, (FIPS 81 to neřešila)
- jako CBC, ale "mezivýsledný" šifrový text se nikam neodesílá
- klíč jiný než pro šifrování
- používá pouze E_K



Závěr k operačním modům

- účel
- principy
- příprava nových modů

Hašovací funkce

Hašovací funkce

Vlastnosti:

- Libovolně dlouhý vstup
- Pevně definovaná délka výstupu

haš, hash, hašový kód = výstupní kód s předem pevně definovanou délkou

Bezpečnostní požadavky

- srovnání zpráva-haš a člověk-otisk prstu
- *jednocestnost (jednosměrnost):*
  - je-li dáno M, je jednoduché vypočítat H(M)
  - je-li dáno H(M), je velmi těžké (výpočetními prostředky prakticky neproveditelné) vypočítat M
- *bezkoliznost - odolnost proti kolizi:*
  - je velmi těžké nalézt jakékoliv i náhodné různé M a M´ tak, aby H(M) = H(M´)

Bezpečnost

- bezkoliznost
  - délka výstupního kódu,
  - kolize existují, jejich nalezení musí být výpočetně neproveditelné
- narozeninový paradox
  - Mějme množinu M o n různých prvcích. Vyberme náhodně k prvků, každý z množiny M (s vracením). Pro k rovno cca $n^{1/2}$ se v daném výběru přibližně s 50% pravděpodobností naleznou dva prvky shodné.
  - Pokud je délka hašového kódu m bitů, tato kolize nastane v množině $2^{m/2}$ haší (zpráv)
  - P(365,23) = 0.507, P(365,30)= 0.706

Použití hašovacích funkcí

- Uložení přihlašovacích hesel
  - nepřímo pomocí hašových kódů
- Kontrola integrity dat (bez klíče)
  - kontrolní součty, haše
- Kontrola integrity dat a zdroje současně (s klíčem)
  - kryptografické kontrolní součty, klíčované hašové autentizační kódy zpráv (HMAC)
- Otisky zpráv pro digitální podpisy
  - výhodné, že hašový kód má pevnou délku
- Otisky klíčů
  - kontrola správnosti kryptografických klíčů při odšifrování
- Další (MGF, deriváty,...)

Hašovací funkce SHA-1

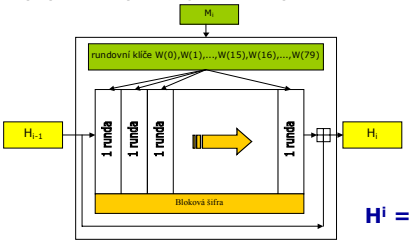
- Secure Hash Standard (Algorithm), platná od 17.4.1995, FIPS PUB 180-1
- určena nejen pro digitální podpisy
- nejrozšířenější hašovací funkce
- nahrazuje všechny ostatní předchůdce (zejména MDx)

SHA-1: postup hašování

- **Doplnění** zprávy M jako u SHA-1
- obecně L bitů, kde $0 \leq L \leq 2^{64} - 1$
- **Rozdělení** na 512bitové bloky M_i (i = 1 až n)
- Příklad zprávy M: „abc"

kompresní funkce f

- H^0 = const. (160 bitů), 32bitová slova
- **$H^i = f(H^{i-1}, M_i)$, i = 1....n**
- h(M) = H^n (nebo jeho část)



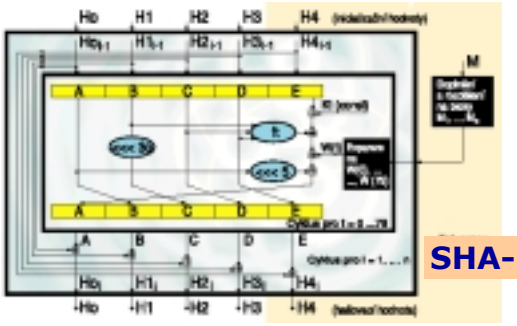
$H^i = f(H^{i-1}, M_i)$

SHA-1: Expanze bloku

- Každý blok M_i (i = 1 až n) je před použitím expandován
  - každé M_i (512 bitů) rozdělíme na 16 32bitových slov W(0) až W(15)
  - expanze: t = 16 ...79:
  - W(t) = (W(t-3) ⊕ W(t-8) ⊕ W(t- 14) ⊕ W(t-16)) <<< 1

    (<<< je cyklický posun)

SHA-1: Hlavní smyčka (5)



SHA-1: funkce a konstanty (3)

- Hlavní smyčka kompresní funkce má 80 rund, v každé se použije jiná funkce ft, 0 <= t <= 79:
  - ft(B,C,D) = (B AND C) OR ((NOT B) AND D) , 0 <= t <= 19,
  - ft(B,C,D) = B XOR C XOR D , 20 <= t <= 39,
  - ft(B,C,D) = (B AND C) OR (B AND D) OR (C AND D) ,40 <= t <= 59,
  - ft(B,C,D) = B XOR C XOR D , 60 <= t <= 79.
- Konstanty K0 až K79:
  - Kt = 5A827999 , 0 <= t <= 19,
  - Kt = 6ED9EBA1 , 20 <= t <= 39,
  - Kt = 8F1BBCDC , 40 <= t <= 59,
  - Kt = CA62C1D6 , 60 <= t <= 79.
- Před zpracováním bloku M1 se H0 až H4 nastaví na inicializační hodnoty
  - H0 = 67452301, H1 = EFCDAB89, H2 = 98BADCFE, H3 = 10325476, H4 = C3D2E1F0.

Hašovací funkce SHA-256, SHA-384, SHA-512

- Secure Hash Standard, FIPS PUB 180-2, schválen 26.8.2002, platnost od 1.2.2003
- podstatně zvýšena bezpečnost
  - v délce kódu
  - ve složitosti výpočtu
- hašovací funkce "pro nové tisíciletí"
- adekvátní bezpečnost AES

SHA-256: shrnutí

- 8 32bitových slov
- cca 2x pomalejší než SHA-1
- bezpečnější (složitější jádro)
- delší hašový kód – menší pravděpodobnost kolizí

SHA-512: základní údaje

- Odlišnosti oproti SHA-256:
  - pracuje se s 64bitovými slovy
  - blok 1024 bitů
  - doplňování do 1024*(n-1)+ 896, následuje 128bitové vyjádření délky zprávy ve dvou 64bitových slovech
  - inicializační konstanty $H0^0$... $H7^0$ odlišné
  - konstanty K256(t) nahrazeny jinými K512(t)
  - vnitřní funkce jiné
  - hlavní smyčka má 80 cyklů

SHA-384

- Odlišnosti oproti SHA-512:
  - inicializační konstanty $H0^0$... $H7^0$ odlišné
- výpočet poté probíhá stejně jako u SHA-512
- z výstupu $H0^n$ ... $H7^n$ se bere pouze prvních šest slov $H0^n$ || $H1^n$ || $H2^n$ || $H3^n$ || $H4^n$ || $H5^n$
- *"zkracováním" výstupu dochází obecně ke snižování bezpečnosti hašovací funkce*

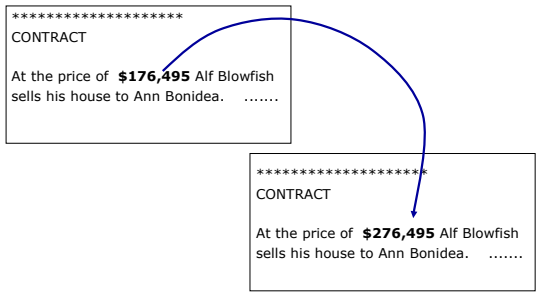
MD –základní údaje

- R.Rivest – MD2, MD4, MD5
- RFC 1319, 1320, 1321
- licencované RSA
- MD5:
  - podobná konstrukce jako SHA-1
  - jednodušší kompresní funkce
  - všechny MD mají 128bitový výstupní hašový kód
    - větší pravděpodobnost kolizí

MD5 – kolize kompresní funkce

- Hans Dobbertin, 1996:
- kolize jen u kompresní funkce, tj. $f(H_{i-1},\mathbf{M_i}) = f(H_{i-1},\mathbf{M_i}')$
- RSA nedoporučuje používat v nových produktech, jen z důvodu kompatibility
  - (pozn.: u MD2 také nalezena kolize u kompresní funkce, 1995, přestala se používat)

MD4 - přímá kolize, Hans Dobbertin (1995), FSE, 1996



HMAC – základní údaje

- keyed-hash MAC, kryptografický kontrolní součet, kryptografická hašovací funkce, klíčovaná haš, **klíčované hašové autentizační kódy zpráv**
- označení podle toho, jakou hašovací funkci používá, např. HMAC-SHA-1
- zpracovává nejen data, ale i klíč
  - výsledek je závislý na klíči a tudíž "nepadělatelný"
  - ověřuje integritu dat a zdroj dat
- odlišuje se od MAC, funkčně podobný
- používá jiné stavební prvky
- je kryptograficky silnější

HMAC

- RFC 2104, ANSI X9.71, FIPS 198
- HMAC-SHA-1 (RFC):
  - blok B=64 bajtů, klíč K, H = SHA-1
  - ipad = řetězec B bajtů 0x36
  - opad = řetězec B bajtů 0x5C
  - klíč K se doplní nulovými bajty do plného bloku délky B

HMAC(M) = H((K xor opad) || **H((K xor ipad)|| M)**)

Srovnání některých hašovacích funkcí

Hash	bitová délka	licence	popis	bezpečnost	rychlost vůči SHA-1	rychlost v MByte/s
MD2	128	ano	RFC 1319	kolize kompr. funkce	0,01	0,709
MD4	128	ano	RFC 1320	kolize	xxx	xxx
MD5	128	ano	RFC 1321	kolize kompr. funkce	2,08	100,738
HMAC-MD5	128	ano	RFC 2202		2,06	99,863
SHA-1	160	ne	RFC 2104, FIPS 180-1,2	bezp.	1	48,462
SHA-256	256	ne	FIPS 180-2	bezp.	0,51	24,746
SHA-384	384	ne	FIPS 180-2	bezp.	0,17	8,246
SHA-512	512	ne	FIPS 180-2	bezp.	0,17	8,246

- C++, kompilace s MS Visual C++ 6.0 SP4 (optimalizace na rychlost), PC/Celeron 850MHz, Windows 2000 SP 1.

Závěr k hašovacím funkcím

- účel
- principy
- bezpečnost
- nejpoužívanější je SHA-1
- od 1.srpna 2002 je platné SHA-1 i SHA-256, SHA-384, SHA-512
- HMAC, nejpoužívanější HMAC-SHA-1 a HMAC-MD5

Závěr k sérii "symetrické šifry"

- klíčové pojmy
- nejznámější algoritmy
- bezpečnost
- i symetrická kryptografie je pole neorané
- stále se ještě nalézají chyby a nedostatky v základních algoritmech
- mnoho příležitostí, jak využít a rozvíjet matematiku - ke kryptografii i kryptoanalýze
- otevřenost a příležitost pro nové objevy

Literatura a další zdroje

Osobní stránka autora
http://cryptography.hyperlink.cz
Archiv článků a prezentací na téma kryptografie a bezpečnost
http://www.decros.cz/bezpecnost/_kryptografie.html
Stránka NIST, normy, dokumenty k AES aj.:
http://csrc.nist.gov/encryption/aes/aes_home.htm
Zdrojové kódy šifer
ftp://ftp.funet.fi/pub/crypt/cryptography/
Bezpečnostní a kryptografický portál
http://www.cs.auckland.ac.nz/~pgut001/links.html