EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Kryptologie

Moderní kryptologie: Symetrické blokové šifry

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204

Doc. Ing. Roman Šenkeřík, Ph.D. FAI,
Ústav informatiky a umělé inteligence

Obsah prezentace

- Šifra DES
- Šifra AES
- Šifra IDEA
- Režimy činnosti blokových symetrických šifer

1. Šifra DES

Šifra DES: Úvod

- DES - Data Encryption Standard

- Původně vyvinut jako systém LUCIFER v 60. letech v IBM.
- V roce 1977 přijata jako standard (FIPS 46) pro šifrování dat v civilních státních organizacích v USA a následně se rozšířila i do soukromého sektoru.
- V současnosti je tato šifra považována za nespolehlivou, protože používá klíč pouze o délce 56 bitů. Navíc obsahuje algoritmus slabiny, které dále snižují bezpečnost šifry. Díky tomu je možné šifru prolomit útokem hrubou silou za méně než 24 hodin.
- V roce 2001 nahrazena nástupcem AES - Advanced Encryption standard [1].

Šifra DES: Princip

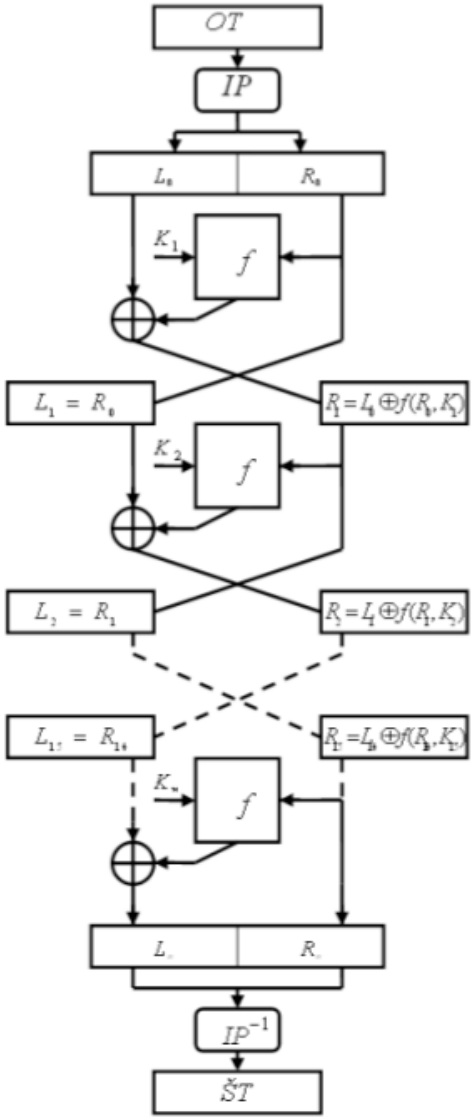
- DES je bloková šifra, která šifruje bloky dat o velikosti 64 bitů.
- Pro šifrování se používá klíč o velikosti 56 bitů.
- Klíč je obvykle vyjádřen jako 64bitová hodnota, avšak každý osmý bit je paritní a je algoritmem ignorován.
- Algoritmus využívá kombinaci dvou kryptografických technik substituce (tj. nahrazení jisté bitové hodnoty jinou hodnotou na základě tabulky) a permutace (tj. jistá záměna pořadí jednotlivých bitů v bloku).

Šifra DES: Princip

- Substituce se provádí pomocí takzvaných S-boxů a permutace pomocí P-boxů.
- Základním stavebním blokem algoritmu DES je jednoduchá kombinace těchto technik (tj. substituce, následovaná permutací), která je modifikována hodnotou klíče.
- Tento cyklus je na šifrovaný blok bitů aplikován šestnáctkrát.

Šifra DES: Celkové schéma

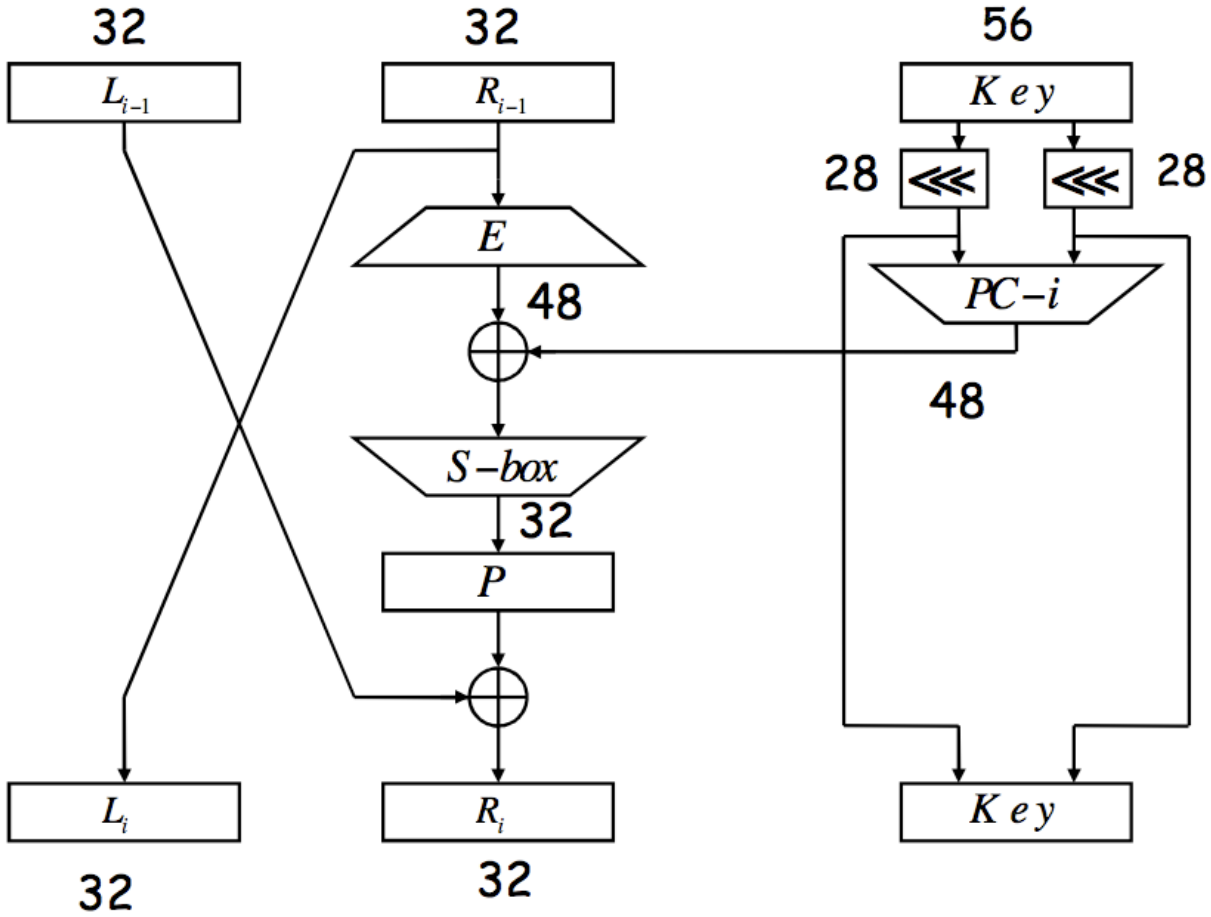
- *IP* – počáteční permutace.
- Operace XOR je značena „křížkem“ v kolečku.



Zdroj: [1]

Šifra DES: Princip

- Detail jedné “rundy” v DES



Zdroj: [1]

Šifra DES: Útok

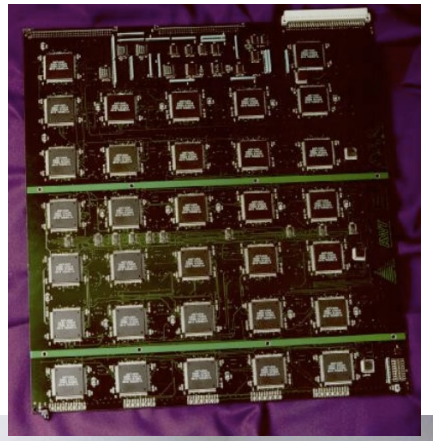
- Možnost útoku hrubou silou na algoritmus DES, která byla teoreticky rozpracovávána už před mnoha lety, byla prakticky demonstrována na jaře roku 1997. Prvním impulzem byla výzva společnosti RSA DSI, která vypsala cenu 10 000 dolarů tomu, kdo rozluští zprávu, zašifrovanou algoritmem DES.

- Rocke Verser vytvořil program, který je možno distribuovat mezi velké množství počítačů a který během nečinnosti počítače (tj. na pozadí) provádí hledání správného klíče.

- Program byl zveřejněn 18. února 1997 a na výzvu reagoval poměrně značný počet účastníků. Dne 17. června byl klíč nalezen. Hledání klíče se účastnilo celkem asi 78 tisíc počítačů.

Šifra DES: Útok

- DES Cracker
- Vytvořen v roce 1998 jako projekt na důkaz, že DES není bezpečný a neprolomitelný.
- Dokázal spočítat DES klíč do 5 dnů
- Cena cca $250 000, výkon 9.10^9 klíčů/s [1].



Zdroj: [2]

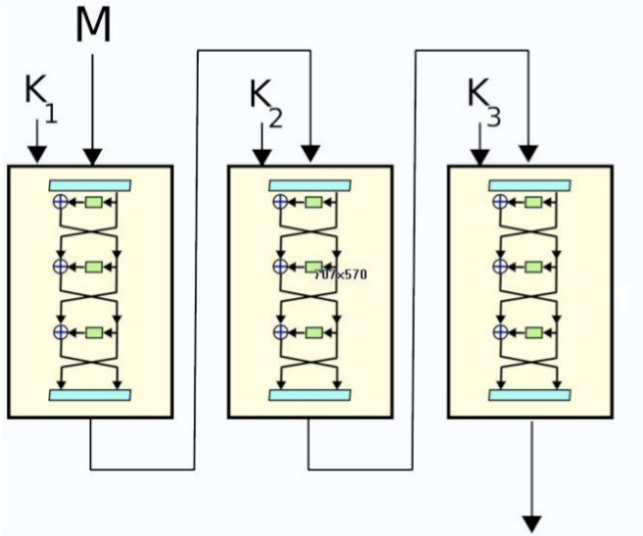
TripleDES - Princip

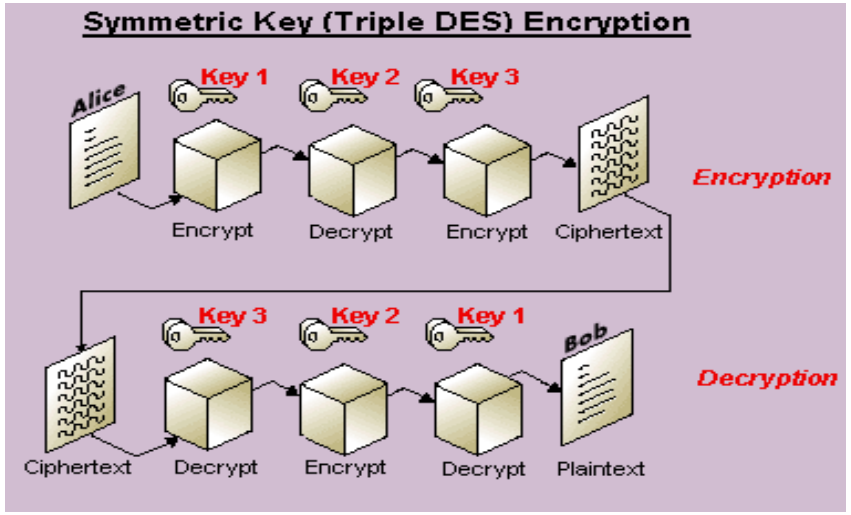
- Vytvořen: 1998 (reakce na prolomení DES). Vznikl 3x použitím původního DES
- Na šifrovanou zprávu se 3x aplikuje šifra DES a získáme 3DES
- Délka klíče vzrostla na 168(3*56) bitů
- Existuje několik běžných standardů.

TripleDES - Princip

- DES EEE3 - jsou používány 3 různé klíče
- DES EDE3 - 3 různé klíče, zašifrování, dešifrování a opět zašifrování
- DES EEE2 - dva klíče, šifrování 1-2-1
- DES EDE2 - dva klíče, zašifrování 1.klíčem, dešifrování 2. klíčem a opět zašifrování 1. klíčem - Nejpoužívanější metoda [1].

TripleDES - Princip





Zdroj: [1]

Další varianty a vlastnosti DES

- N-násobný DES - šifrování s klíčem o délce 56b několikrát za sebou (např. Triple DES)
- DES s nezávislými podklíči - pro každou rundu je použit jiný, nezávislý podklíč, jež není generován z 56b klíče.
- DES-X - ke klíči je před každou rundou přičten mod2 (XOR) další 64b klíč.
- GDES - zobecněný DES (pro urychlení - zranitelnější).
- DES s alternativními S-Boxy - řešení umožňující měnit jejich uspořádání či strukturu. [1]

Další varianty a vlastnosti DES

- RDES - výměna levých a pravých polovin řízena dle klíče
- crypt(3) - varinata DES pro Unixové systémy pro tvorbu hesel
- **Bezpečnost DES záleží na S-Boxech**, vše ostatní jsou lineární operace (lehce odstranitelné) běžnou kryptoanalýzou.
- **Silný lavinový efekt** - změna pouhého jednoho bitu ve vstupních datech nebo klíči vede ke změně celé jedné poloviny výstupních dat [1].

2. Šifra AES

AES - Advanced Encryption Standard

- Vytvořena: 1998 (reakce na prolomení DES). Symetrická šifra s délkou klíče 128, 192, 256 bitů
- Metoda šifruje data postupně v blocích s pevnou délkou 128 bitů (volitelně může být i 192 a 256 bitů).
- Šifra se vyznačuje vysokou rychlostí šifrování dat (stovky MB/s)
- Iterativní (rundová) šifra, obsahuje 10 (defaultně) - 14 rund v závislosti na velikosti klíče a bloku dat. Každá plnohodnotná runda se skládá z následujících operací: [3].

AES - Advanced Encryption Standard

- **ByteSub Transformation**
  - Nelineární vrstva pro zvýšení odolnosti vůči diferenciálním a lineárním kryptoanalytickým metodám

- **ShiftRow Transformation**
  - Lineární vrstva pro posun bajtů v tabulce v cyklickém pořadí

AES - Advanced Encryption Standard

- **MixColumn Transformation**
  - Mixování buňek tabulky (násobení sloupců polynomem, implementace pomoci XOR)

- **AddRoundKey**
  - Přidání cyklického klíče k datům - opět pomocí operace XOR. Klíč je určen pomocí klíčového plánovacího algoritmu.

Šifra AES: Princip

- Existují varianty AES-128, AES-192 a AES-256

Volitelná délka klíče

- 128 bitů …$3{,}4*10^{38}$ klíčů
- 192 bitů …$6{,}2*10^{57}$ klíčů
- 256 bitů …$1{,}1*10^{77}$ klíčů

Volitelná délka bloku

- 128 bitů
- 192 bitů
- 256 bitů

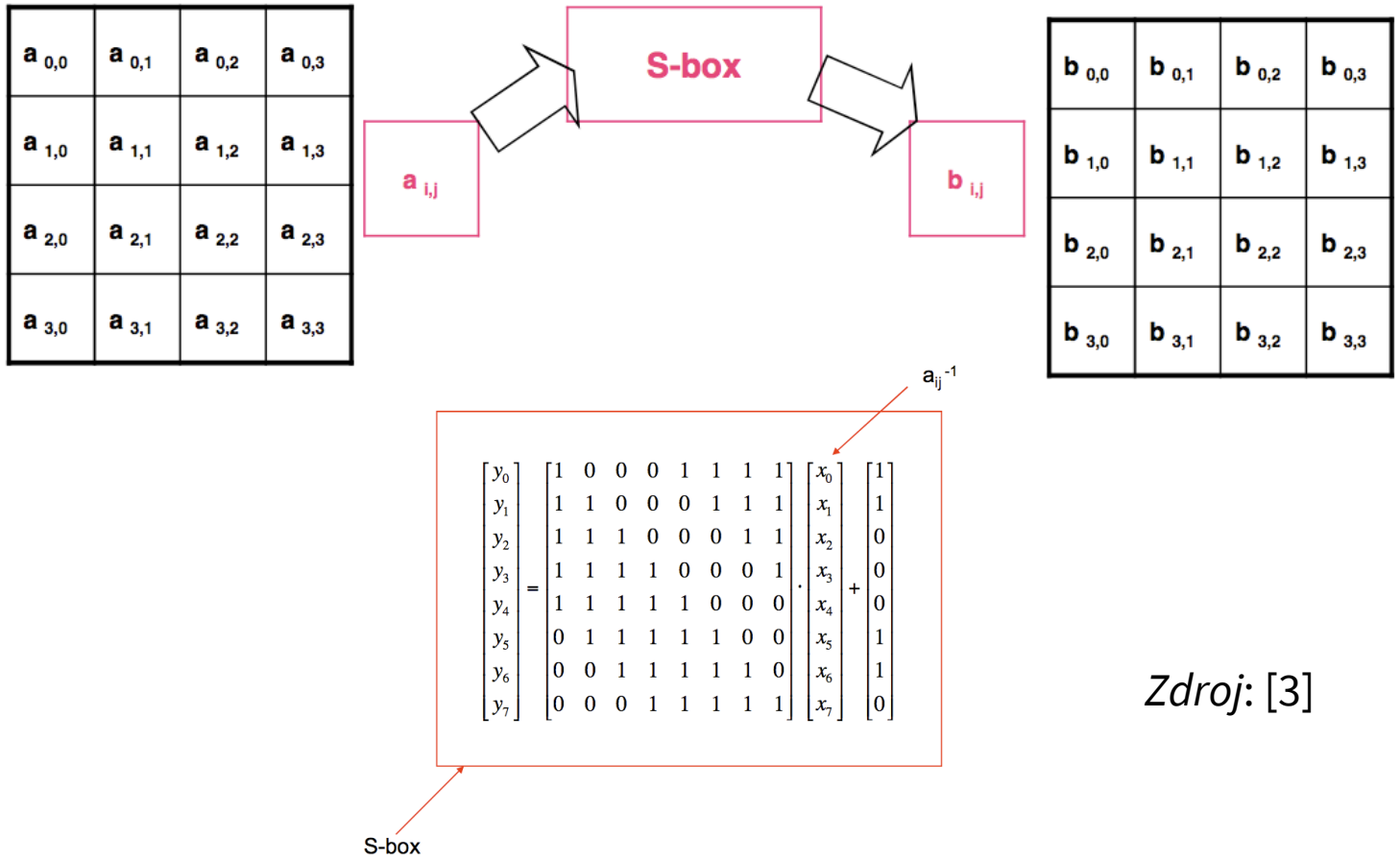
$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$	$k_{0,4}$	$k_{0,5}$	$k_{0,6}$	$k_{0,7}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$	$k_{1,4}$	$k_{1,5}$	$k_{1,6}$	$k_{1,7}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$	$k_{2,4}$	$k_{2,5}$	$k_{2,6}$	$k_{2,7}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$	$k_{3,4}$	$k_{3,5}$	$k_{3,6}$	$k_{3,7}$

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$a_{0,6}$	$a_{0,7}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$	$a_{3,6}$	$a_{3,7}$

Zdroj: [3]

Šifra AES: Princip

- BYTE-SUB Transformation

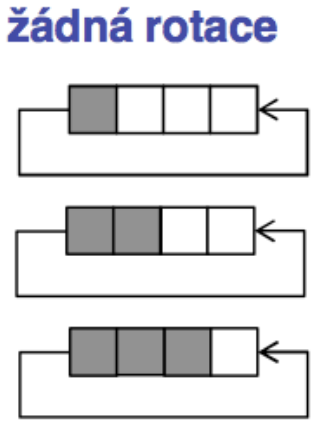


Zdroj: [3]

Šifra AES: Princip

- ShiftRow Transformation

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

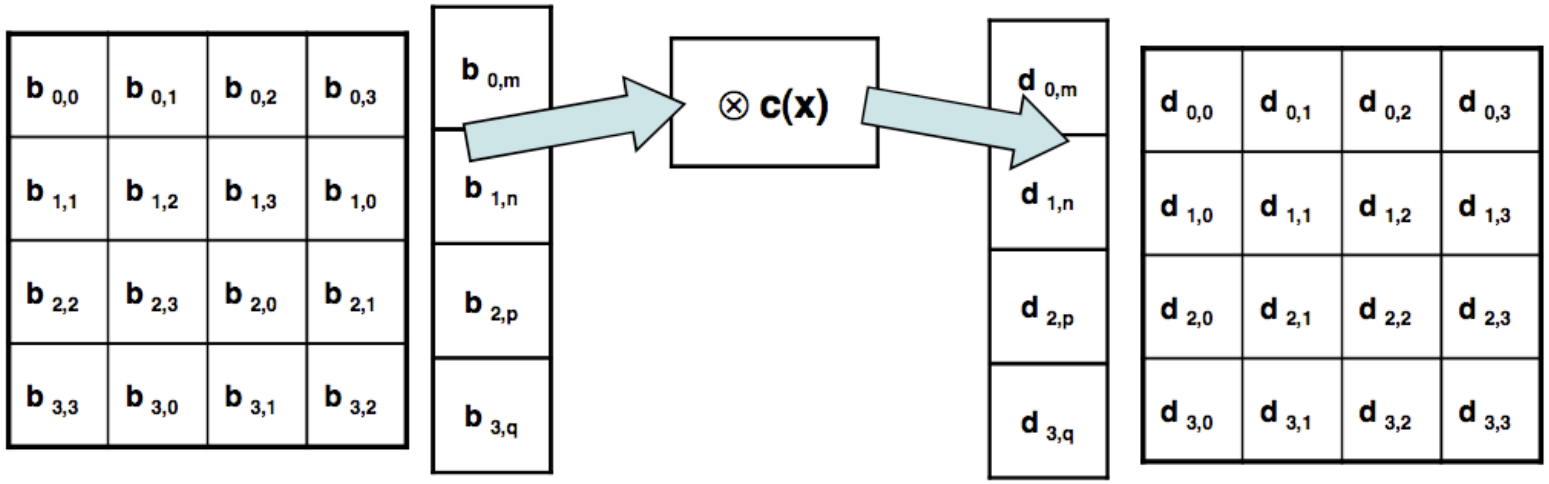


$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,1}$	$b_{1,2}$	$b_{1,3}$	$b_{1,0}$
$b_{2,2}$	$b_{2,3}$	$b_{2,0}$	$b_{2,1}$
$b_{3,3}$	$b_{3,0}$	$b_{3,1}$	$b_{3,2}$

Zdroj: [3]

Šifra AES: Princip

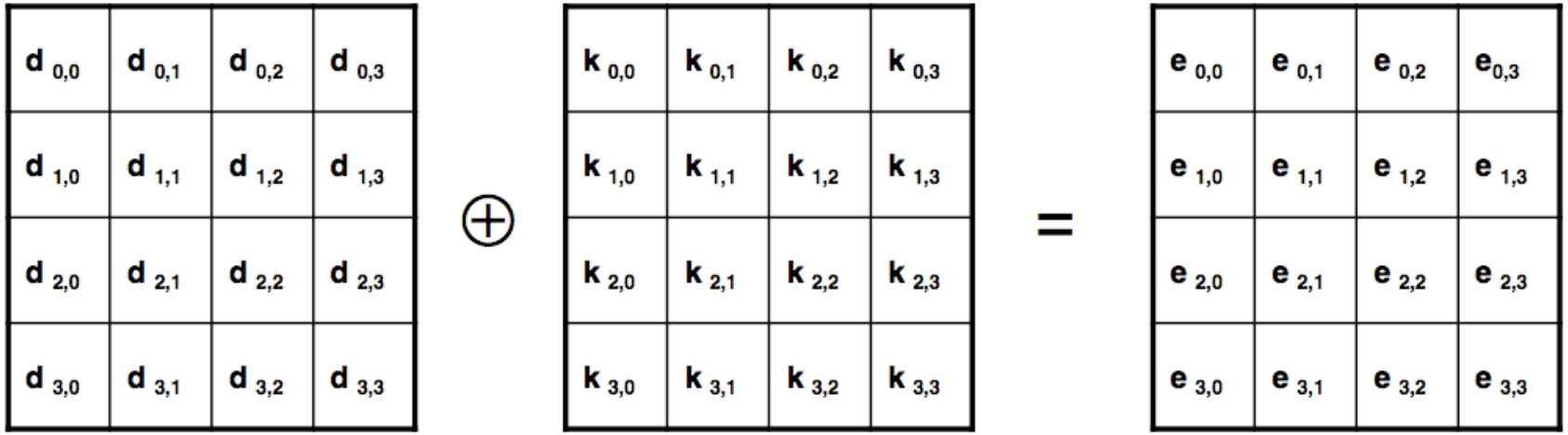
- MixColumn Transformation



Zdroj: [3]

Šifra AES: Princip

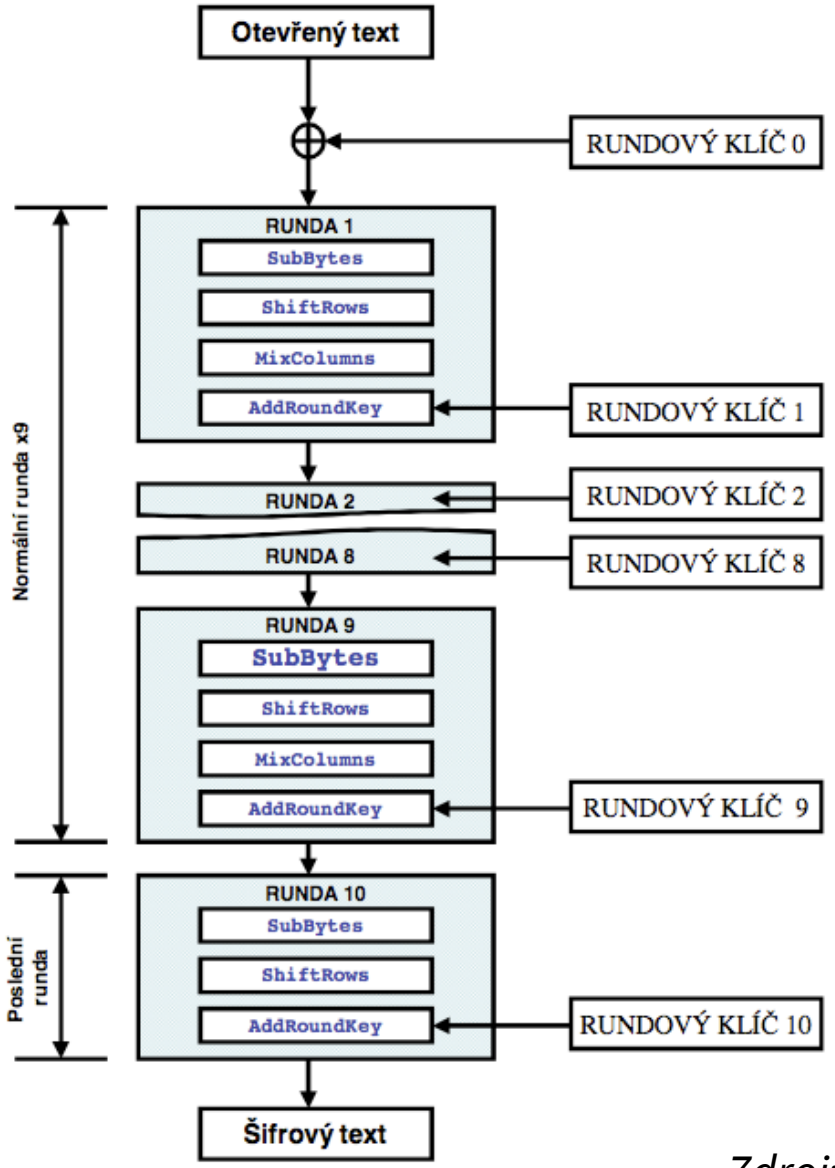
- Add Round Key



Zdroj: [3]

Šifra AES: Princip

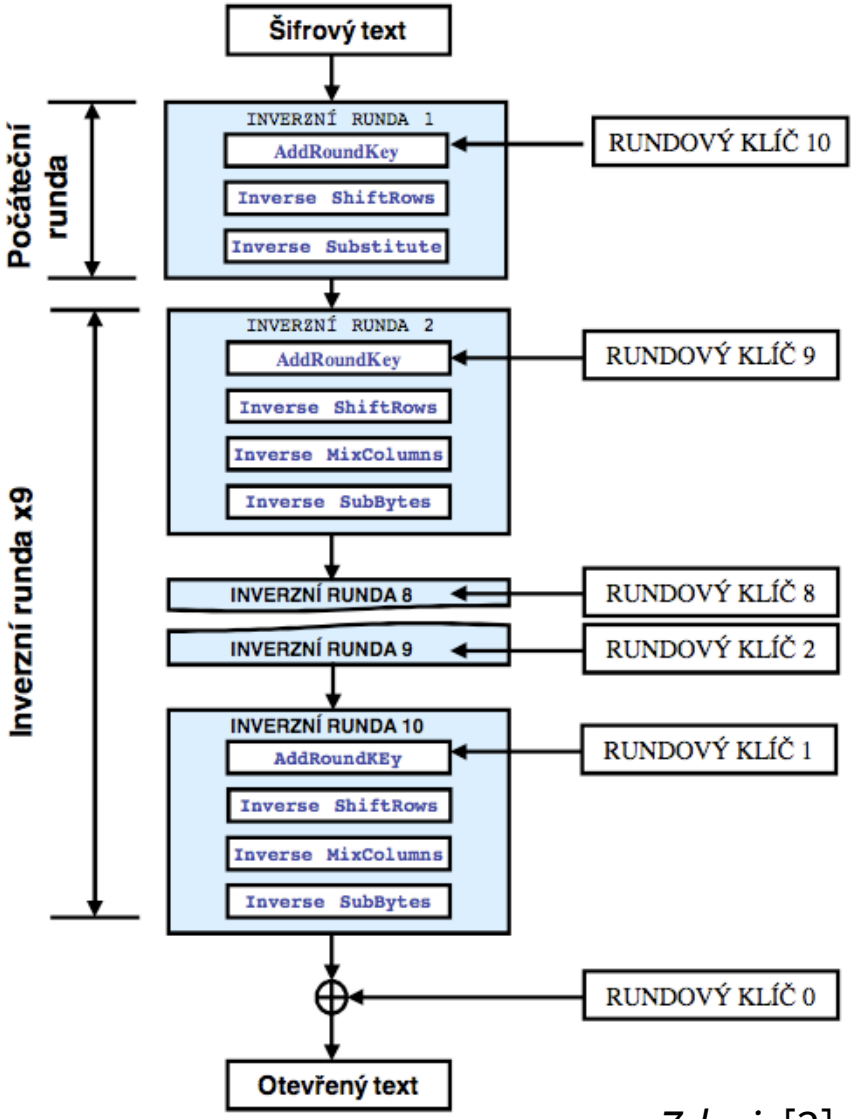
- Šifrování



Zdroj: [3]

Šifra AES: Princip

- Dešifrování



Zdroj: [3]

3. Šifra IDEA

Šifra IDEA: Úvod

- Vytvořena: 1991
- IDEA - International Data Encryption Algorithm
- Symetrická šifra
- Používána například v systému PGP (Prety Good Privacy) nebo v rámci protokolu SSL

Šifra IDEA: Úvod

- Odolná vůči diferenční kryptoanalýze
- IDEA pracuje po 64bitových blocích za použití 128bitového klíče.
- Skládá se z řady osmi identických transformací a vstupní transformace (poloviční průchod).
- Procesy šifrování a dešifrování jsou podobné.

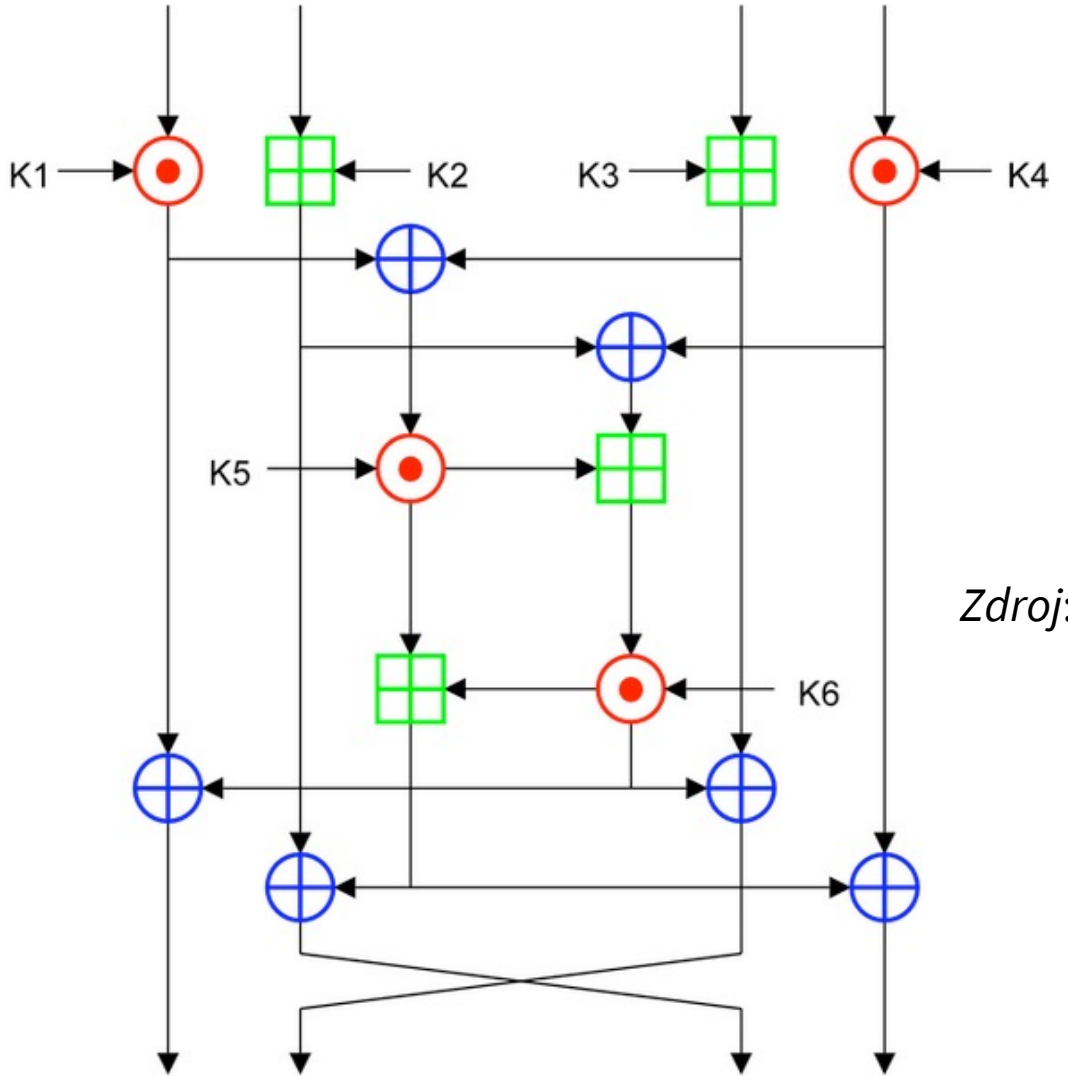
Šifra IDEA: Úvod

- Iterativní šifra - obsahuje 8,5 rund
- IDEA odvozuje velkou část své bezpečnosti ze střídání operací z různých grup – modulární sčítání a násobení a bitové nonekvivalence (XOR) – které jsou v jistém smyslu algebraicky neslučitelné [1].
- V dnešní době postupně nahrazena šifrou CAST.

Šifra IDEA: Princip

- Všechny operace pracují s 16 bitovými řetězci,
- bitová nonekvivalence (znázorněno modrým $\oplus$),
- sčítání modulo 2^{16} (znázorněno zeleným $\boxplus$),
- násobení modulo $2^{16}+1$, kde nulová slova (0x0000) jsou interpretována jako 2^{16} (znázorněno červeným $\odot$).

Šifra IDEA: Schéma



Zdroj: [1]

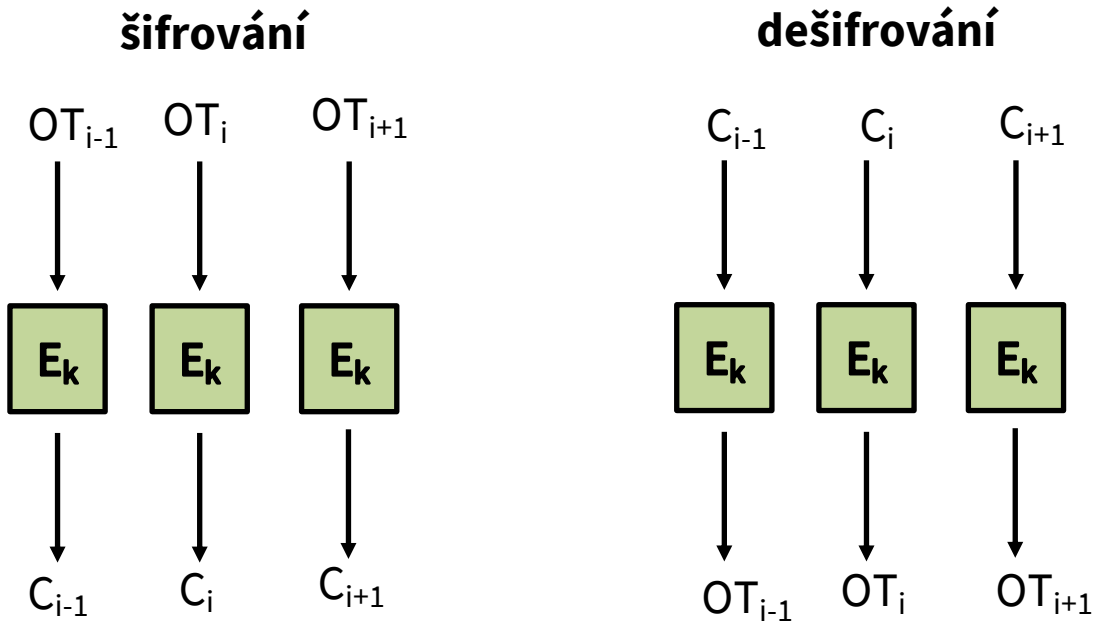
Další symetrické blokové šifry

- Blowfish
- Camellia
- CAST
- SERPENT

4. Režimy činnosti blokových šifer

Režimy činnosti I

- **ECB - Electronic Code Book** (bez jakéhokoliv key-managementu, IV atd...) [4]



Kde:

OT_i - Plaintext (data jež chceme zašifrovat)

E_k - Encryption algorithm (šifrovací algoritmus)

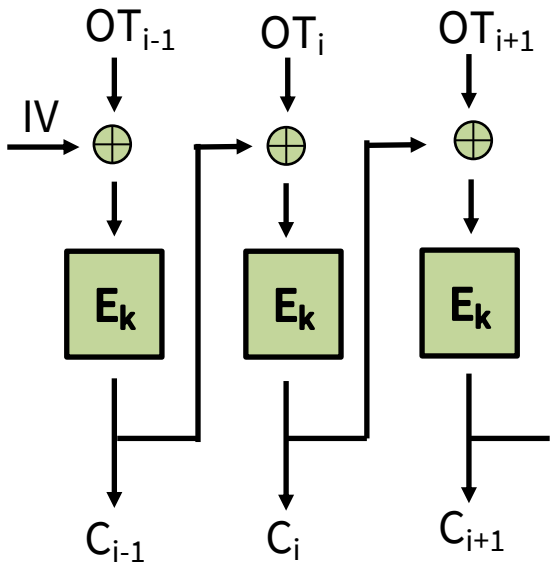
C_i - Cipher - výsledný šifrový výstup

Režimy činnosti II

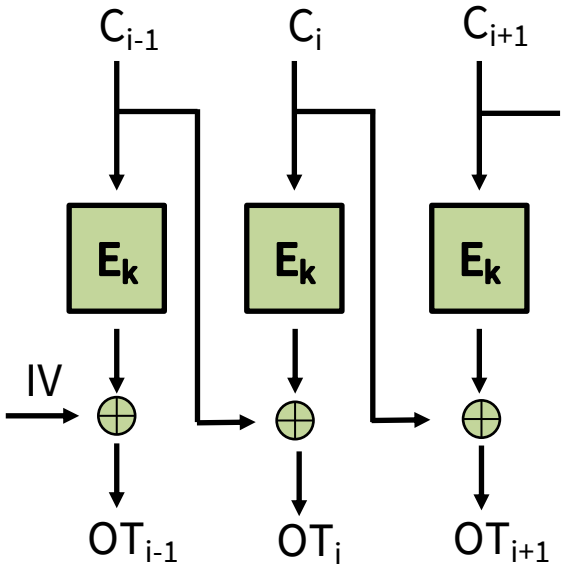
- **Cipher Block Chaining (CBC)** [4]: Operace XOR mezi právě zašifrovaným blokem a blokem vstupních dat jež má být zašifrován.
- Pro první blok se používá XOR mezi 1. blokem dat jež má být zašifrován a IV).

Režimy činnosti II

šifrování



dešifrování



Kde:

OT_i - Plaintext (data jež chceme zašifrovat)

E_k - Encryption algorithm (šifrovací algoritmus)

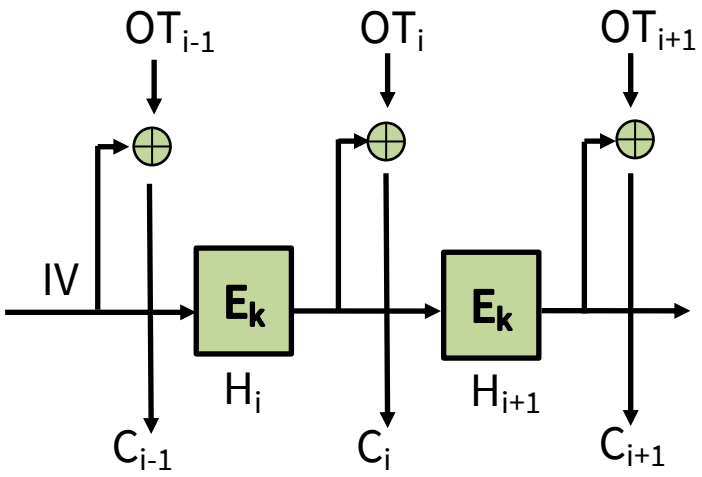
C_i - Cipher - výsledný šifrový výstup

Režimy činnosti III

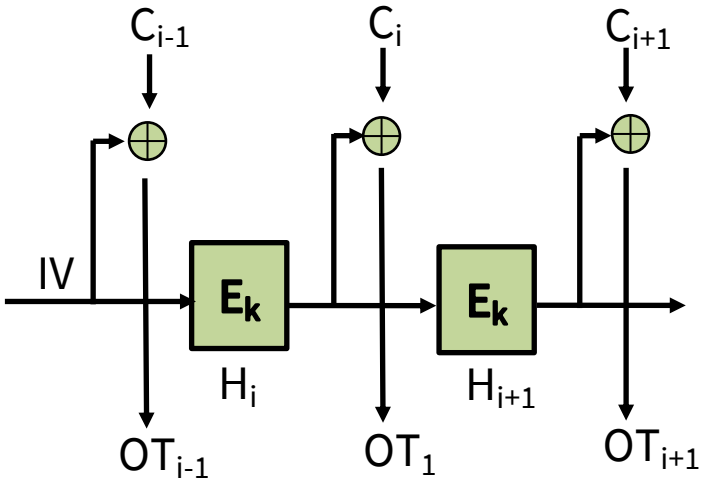
- **Output FeedBack (OFB)** [4]: Simulace proudové šifry, XOR mezi vstupními daty (které nejsou šifrovány) a výstupem blokové šifry.
- Ta zde slouží pouze jako generátor pseudonáhodné posloupnosti, vstupem je pro “první blok” IV, následně další výstup z blokové šifry.

Režimy činnosti III

šifrování



dešifrování



Kde:

OT_i - Plaintext (data jež chceme zašifrovat)

E_k - Encryption algorithm (šifrovací algoritmus)

C_i - Cipher - výsledný šifrový výstup

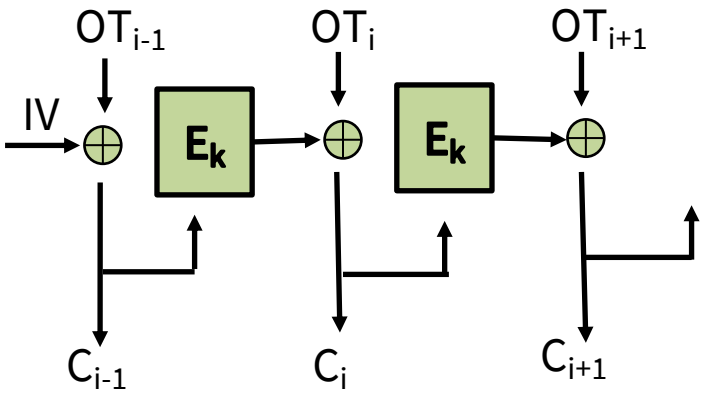
H_i - Hodnota pseudonáhodné posloupnosti

Režimy činnosti IV

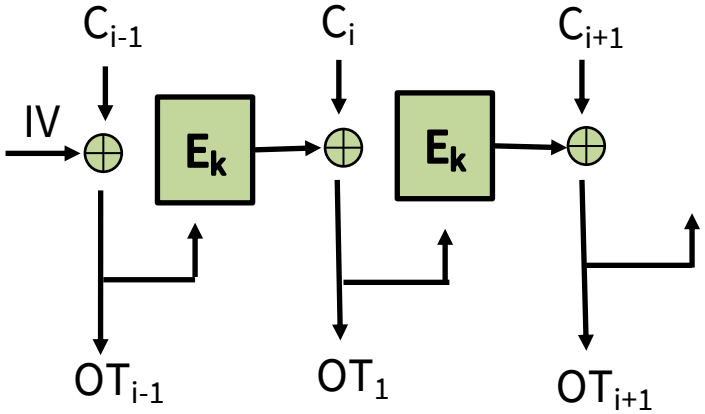
- **Ciphertext FeedBack (CFB)** [4]: Simulace proudové šifry, XOR mezi vstupními daty (které nejsou šifrovány) a výstupem blokové šifry - ta zde slouží pouze jako generátor pseudonáhodné posloupnosti, vstupem je zpětná vazba (šifrovaný text), pro “první blok” je vstupem IV.

Režimy činnosti IV

šifrování



dešifrování



Kde:

OT_i - Plaintext (data jež chceme zašifrovat)

E_k - Encryption algorithm (šifrovací algoritmus)

C_i - Cipher - výsledný šifrový výstup

Seznam odkazů

[1] Moderní blokové šifry I. Tomáš Vaněk. [online]. Dostupné z: http://rantos.cz/IBE-prezentace/P03_Blokove_sifry_v1.4.3SHORT.pdf

[2] Základy moderní kryptologie – Symetrická kryptografie I. Vlastimil Klíma. [online]. Dostupné z: http:// crypto-world.info/klima/mffuk/Symetricka_kryptografie_I_2005.pdf

[3] Moderní blokové šifry AES Kandidáti na AES. Tomáš Vaněk. [online]. Dostupné z: http:// www.rantos.cz/IBE-prezentace/P04_Moderni_blokove_sifry_II_v1.0.9a.pdf

[4] SCHNEIER, Bruce. Applied Cryptography Second Edition: Protocols, algorithms, and source code in C. [1th] ed. New York: John Wiley, 1996. ISBN 0-471-12845-7.

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Děkuji za pozornost

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204