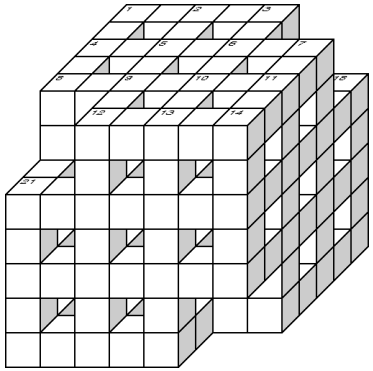
České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky

Moderní blokové šifry I



Ing. Tomáš Vaněk, Ph.D. tomas.vanek@fel.cvut.cz

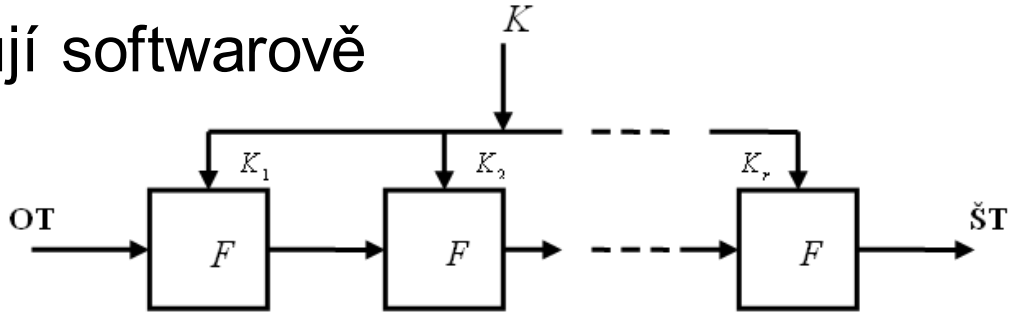
Osnova

- Feistelova šifra
- Zobecněná Feistelova šifra - EFN
- DES
- 3DES

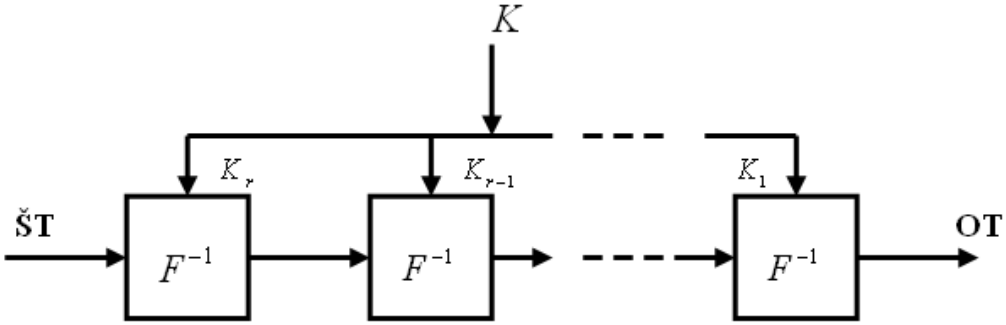
Iterované blokové šifry

- otevřený text i šifrový text mají pevnou délku
- ŠT ze získá z OT pomocí opakované **rundové funkce**
- vstupem do rundové funkce je klíč a výstup z předchozí rundy
- obvykle se implementují softwarově

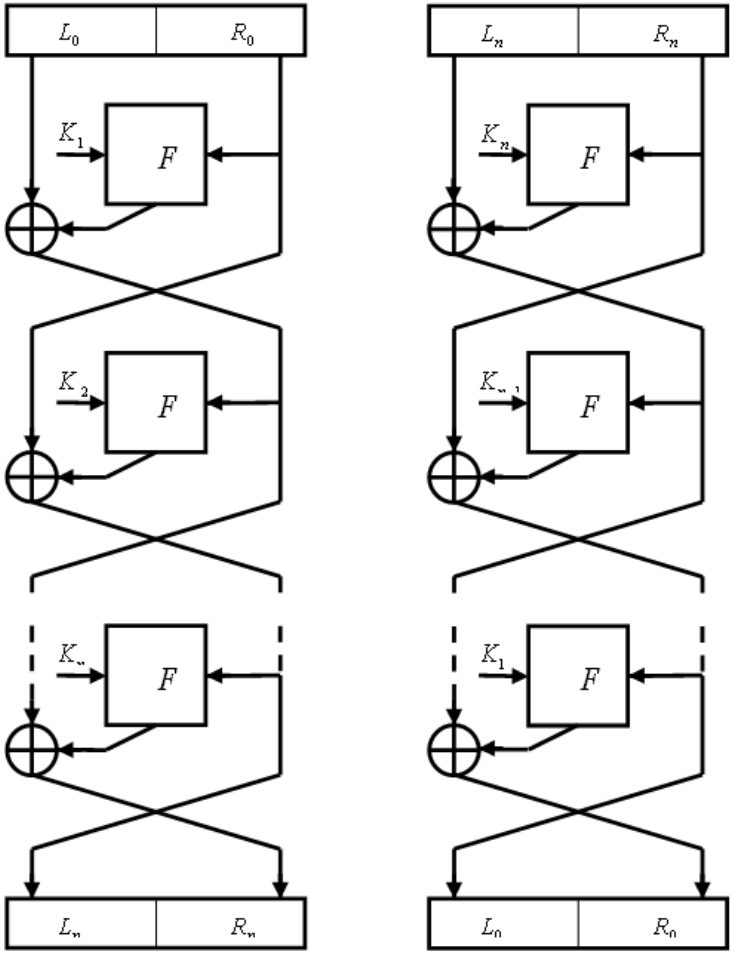
Šifrování pomocí iterované šifry



Dešifrování iterované šifry



Feistelova šifra



- Feistelova šifra představuje určitý typ blokových šifer
- nejedná se o konkrétní algoritmus
- hodně moderních symetrických blokových šifer má Feistelovu strukturu

Feistelova šifra

- Rozdělíme blok otevřeného textu na levou a pravou část:
  OT = (L_0, R_0)
- Pro každou rundu $i=1,2,...,n$, spočítáme

  $L_i = R_{i-1}$

  $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

  kde f je rundová funkce a K_i je podklíč

  ŠT = (L_n, R_n)
- Dešifrování: ŠT = (L_n, R_n)
- V každé rundě i $i=n, n-1, \ldots, 1$, spočteme

  $R_{i-1} = L_i$

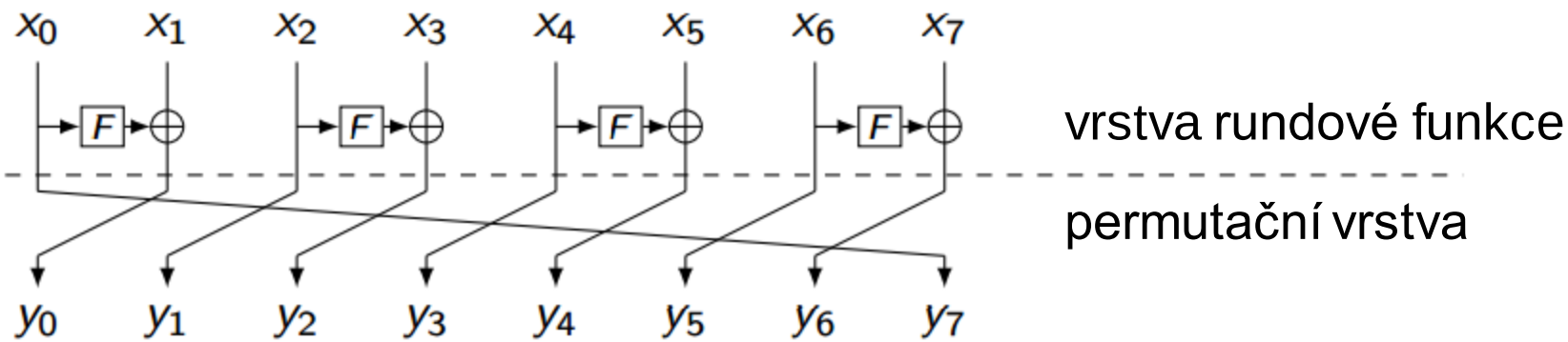
  $L_{i-1} = R_i \oplus f(R_{i-1}, K_i)$

  kde f je rundová funkce a K_i je příslušný podklíč

  OT = (L_0, R_0)
- Tento „vzorec“ funguje pro jakoukoliv funkci $f()$
- Bezpečné šifry jsou, ale pouze pro některé funkce $f()$

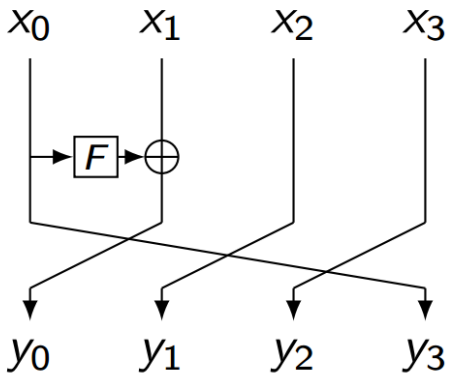
EFN - Zobecněné Feistelovy šifry

- představeny v 1989
- rozdělení bloku OT do $k \geq 2$ n-bitových částí
- obsahuje dvě vrstvy:
  - vrstva rundové funkce
  - permutační vrstva



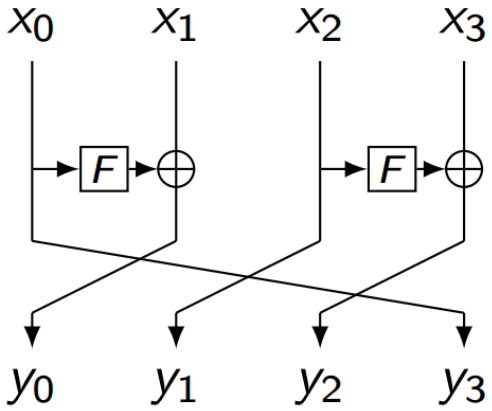
+ vhodné pro malé implementace (velikost podbloku = velikost S-boxu)
- horší difúze mezi podbloky pro rostoucí k

EFN - Zobecněné Feistelovy šifry



Typ I

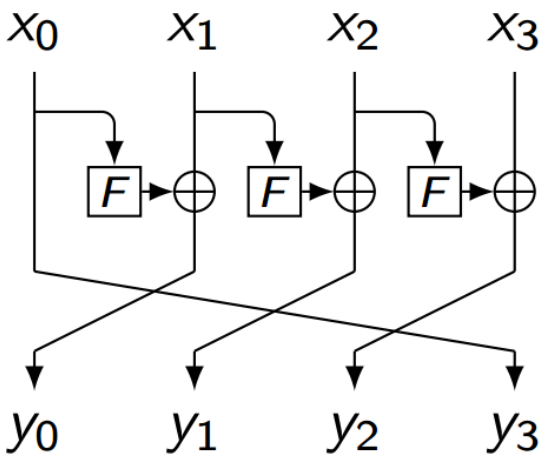
- pouze jedna F funkce
- $y_0, y_1, \ldots, y_{n-1}, y_n = x_1 \oplus F(x_0), x_2, \ldots, x_n, x_1$
- Algoritmy: CAST-256, Lesamnta

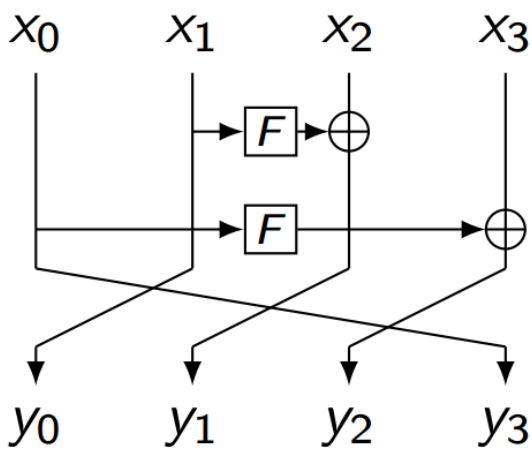


Typ II

- jedna *F* funkce pro každé dva sousedící bloky
- lepší difúze než Typ I
- $y_0, y_1, \ldots, y_{n-1}, y_n = x_1 \oplus F(x_0), x_2, x_3 \oplus F(x_2), \ldots x_n, x_{n-1} \oplus F(x_0)$
- Algoritmy: HIGHT, CLEFIA

EFN - Zobecněné Feistelovy šifry





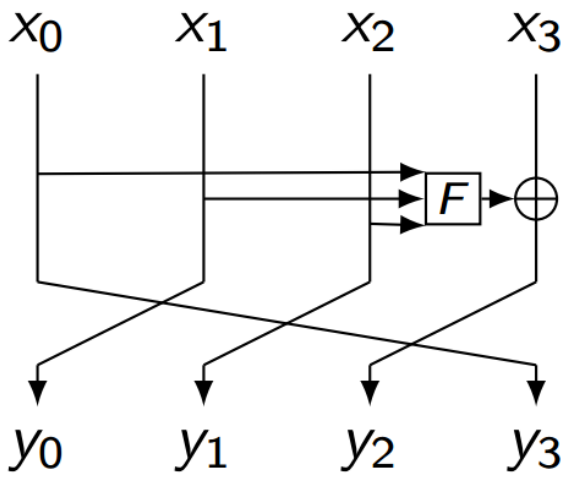
Typ III

- pro každý blok existuje vlastní *F* funkce
- difúze skoro stejně rychlá jako u Typu II
- $y_0, y_1, \ldots, y_{n-1}, y_n = x_1 \oplus F(x_0), x_2 \oplus F(x_3), \ldots x_n \oplus F(x_{n-1}), x_1$

Nybergova EFN

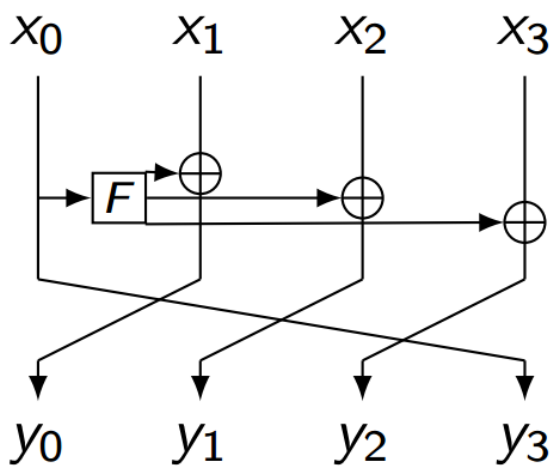
- dvě *F* funkce
- $y_0, y_1, \ldots, y_{n-1}, y_n = x_1, x_2 \oplus F(x_1), x_3 \oplus F(x_0), x_0, \ldots, x_n \oplus F(x_{n-3}), x_{n-3}$

EFN - Zobecněné Feistelovy šifry



EFN s přetíženým vstupem

- pro každý blok existuje vlastní $y_0, y_1, \ldots, y_{n-1}, y_n = x_1, x_2, x_3 \oplus F(x_0, x_1, x_2), x_0, \ldots, x_n \oplus F(x_{n-3}, x_{n-2}, x_{n-1}), x_{n-3}$
- Algoritmy: MD-x, SHA-1,2

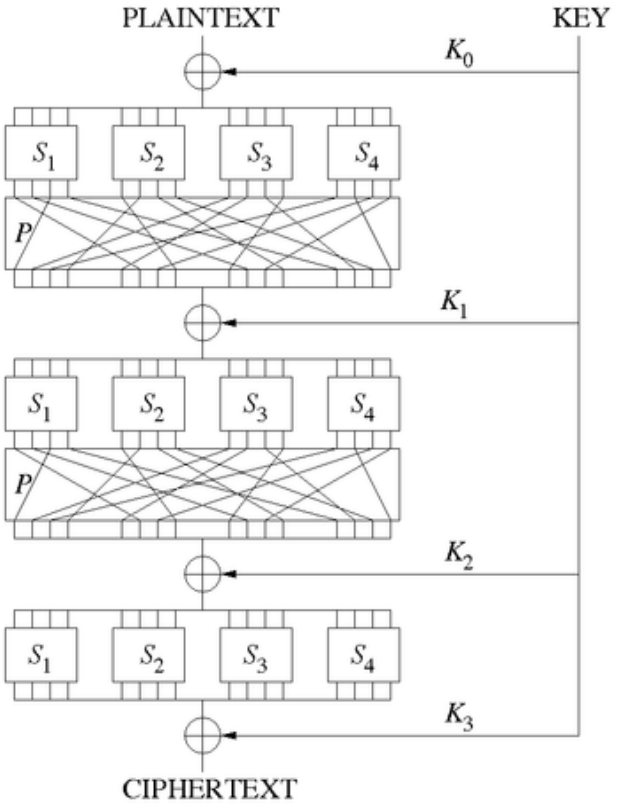


EFN s přetíženým výstupem

- $y_0, y_1, \ldots, y_{n-1}, y_n = x_1 \oplus F(x_0), x_2 \oplus F(x_0), x_3 \oplus F(x_0), x_0 \ldots, x_{n-2} \oplus F(x_{n-3}), x_{n-3}$
- Algoritmy: MARS

SP (Substitučně-permutační) síť

- SPN – Substitution-Permutation Network
- AES
- 2vrstvy
  - S-boxy
    - symetrické (1:1); lavinový efekt
  - P-box
    - výstupní bity z jednoho S-boxu jsou přivedeny na vstup co nejvíce S-boxů



Lavinový efekt

- vhodná (a vyžadovaná) vlastnost šifrovacích algoritmů
- změna jednoho bitu v bloku vstupních dat nebo v klíči vede ke změně přibližně jedné poloviny výstupních bitů
- ztěžuje kryptoanalýzu
- vymyslel Horst Feistel

Round	AES	Number of bits that differ
	0123456789abcdeffedcba9876543210 0023456789abcdeffedcba9876543210	1
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	657470750fc7ff3fc0e8e8ca4dd02a9c c4a9ad090fc7ff3fc0e8e8ca4dd02a9c	20
2	5c7bb49a6b72349b05a2317ff46d1294 fe2ae569f7ee8bb8c1f5a2bb37ef53d5	58
3	7115262448dc747e5cdac7227da9bd9c ec093dfb7c45343d689017507d485e62	59
4	f867aee8b437a5210c24c1974cffeabc 43efdb697244df808e8d9364ee0ae6f5	61
5	721eb200ba06206dcbd4bce704fa654e 7b28a5d5ed643287e006c099bb375302	68
6	0ad9d85689f9f77bc1c5f71185e5fb14 3bc2d8b6798d8ac4fe36a1d891ac181a	64
7	db18a8ffa16d30d5f88b08d777ba4eaa 9fb8b5452023c70280e5c4bb9e555a4b	67
8	f91b4fbfe934c9bf8f2f85812b084989 20264e1126b219aef7feb3f9b2d6de40	65
9	cca104a13e678500ff59025f3bafaa34 b56a0341b2290ba7dfdfbddcd8578205	61
10	ff0b844a0853bf7c6934ab4364148fb9 612b89398d0600cde116227ce72433f0	58

DES – základní informace

- v 60. letech IBM vyvinula šifru Lucifer
  - pod vedeném Horsta Feistela
  - délka bloku 64-bitů
  - délka klíče 128 bitů
- v roce 1973 vyhlásil úřad NBS (National Bureau of Standards) „výběrové řízení“ pro národní šifrovací standard – Data Encryption Standard (DES)
- IBM přihlásila do řízení modifikovaný Lucifer, který byl později schválen a přijat jako DES
- schválen jako norma FIPS-46 (Federal Information Processing Standards) pro šifrovaní **neklasifikovaných informací**
- používal se až do roku 2001, kdy byl standardizován jeho nástupce AES

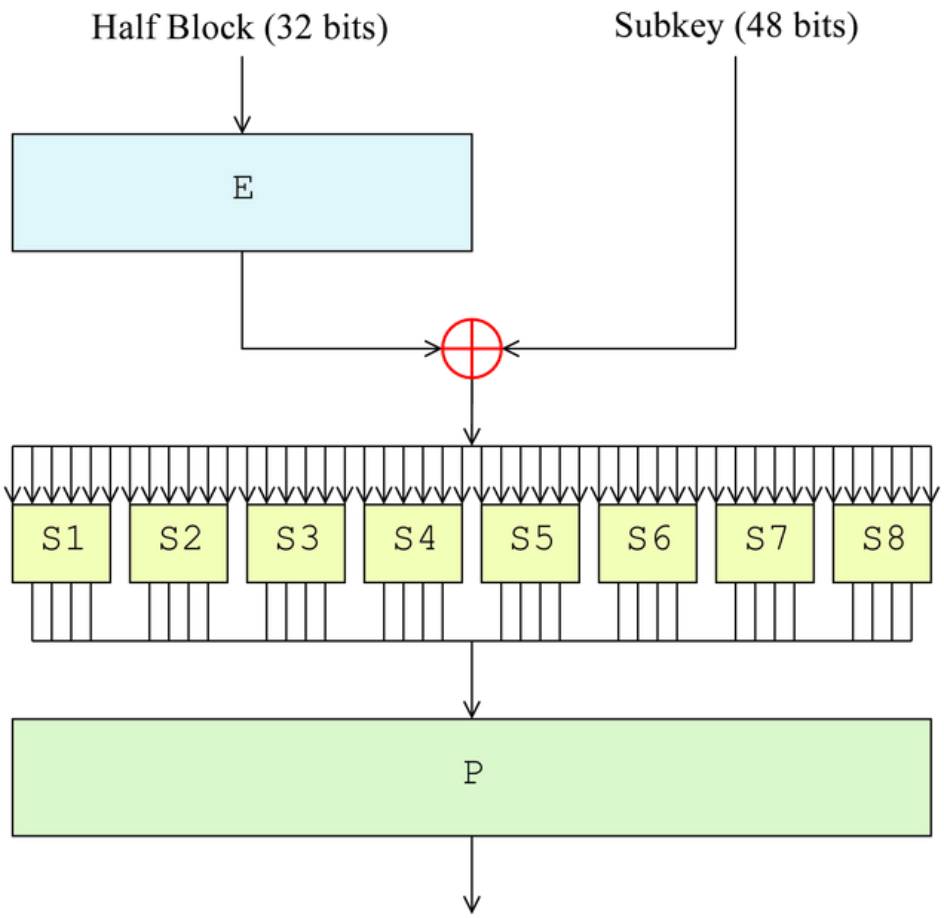
DES – základní informace

- vznik DESu byl „kontroverzní“
  - NSA ho tajně upravila + zkrátila klíč
  - úpravy nebyly dodnes oficiálně popsány
  - hovořilo se o implementaci „zadních vrátek“ do algoritmu – nepotvrzeno
  - spíše šlo o posílení vůči v té době veřejnosti neznámým kryptoanalytickým metodám - diferenciální kryptoanalýze
    - 16.2.2011potvrzeno na konferenci RSA Security Conference technickým ředitelem NSA
    - http://gcn.com/articles/2011/02/16/rsa-11-nsa--no-des-backdoor.aspx?s=gcndaily_170211

DES v číslech

- šifra Feistela typu
- délka bloku 64 bitů
- délka klíče 56 bitů
- 2^{56} = 72,057,594,037,927,900
- 16 rund
- v každé rundě je použito jiných 48 bitů klíče (podklíč, rundový klíč)
- v každé rundě se s blokem vykonávají stejné jednoduché operace
- bezpečnost DESu závisí na konstrukci “S-boxu”
  - z pohledu bezpečnosti nejdůležitější část
  - jediný nelineární prvek v DESu

DES - operace v rundě – 8 paralelních S-boxů



http://en.wikipedia.org/wiki/Data_Encryption_Standard

DES S-box č.1

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
01	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
10	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
11	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

- 8 různých S-boxů
- 6 vstupů, 4 výstupy – nelineární operace
- první a poslední bit vstupního řetězce určují řádek
- vnitřní čtyři bity určují sloupec
- v průsečíku se nachází výsledek

Příklad: na vstupu je hodnota 100011

DES S-box č.1

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
01	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
10	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
11	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

- 8 různých S-boxů
- 6 vstupů, 4 výstupy – nelineární operace
- první a poslední bit vstupního řetězce určují řádek
- vnitřní čtyři bity určují sloupec
- v průsečíku se nachází výsledek

Příklad: na vstupu je hodnota 100011

zvolíme řádek 11-

DES S-box č.1

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
01	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
10	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
11	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

- 8 různých S-boxů
- 6 vstupů, 4 výstupy – nelineární operace
- první a poslední bit vstupního řetězce určují řádek
- vnitřní čtyři bity určují sloupec
- v průsečíku se nachází výsledek

Příklad: na vstupu je hodnota 100011

zvolíme řádek 11

zvolíme sloupec 0001

DES S-box č.1

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
01	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
10	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
11	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

- 8 různých S-boxů
- 6 vstupů, 4 výstupy – nelineární operace
- první a poslední bit vstupního řetězce určují řádek
- vnitřní čtyři bity určují sloupec
- v průsečíku se nachází výsledek

Příklad: na vstupu je hodnota 100011

zvolíme řádek 11

zvolíme sloupec 0001 průsečík 12 (1100 binárně)

Bezpečnost DESu

- nejjednodušší útok
  - hrubá síla
  - najít správný klíč z celkem 2^{56} klíčů
- DES je komplementární
  - $y = E_k(x) \Leftrightarrow \bar{y} = E_{\bar{K}}(\bar{x})$, kde $\bar{x}$ je bitový doplněk x
  - redukce problémů na polovinu
  - stačí uhodnout pouze 2^{55} klíčů
- Paměťová náročnost - $E_K(P)$ pro všechna K ~ 960PB
- TMTO - Time/Memory TradeOff
  - 1980 – M. Hellman
  - 1 TB paměti
  - 5 dní výpočtů

Bezpečnost DESu

- bezpečnost DESu závisí především na S-boxech
  - vše ostatní v DESu jsou lineární operace
  - lineární = „lehce“ odstranitelné
- S-box – substituční tabulka
- ani po 30 letech nebyla nalezena žádná “zadní vrátka (back-door)”
- nejefektivnější útokem dnes je útok hrubou silou
- existuje řada variant DESu (DESX, crypt(3), GDES, RDES, s^nDES, DES s nezávislými podklíči,…) které měly být rychlejší, bezpečnější, ale většinou je jejich bezpečnost nižší…

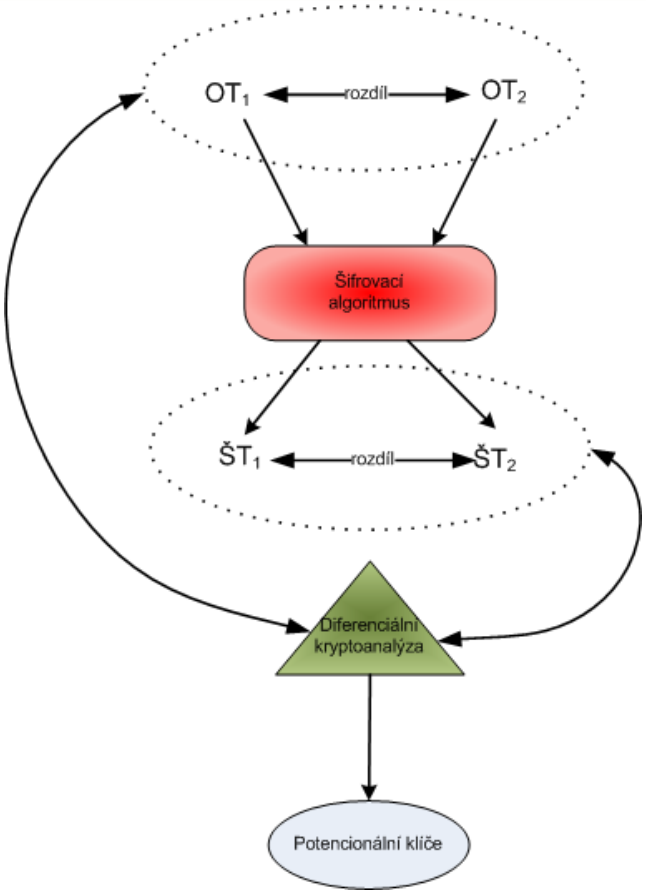
- **Jednoznačný závěr:** návrháři DESu (resp. modifikátoři původního Luciferu) věděli co dělají

Diferenciální kryptoanalýza

- varianta útoku se znalostí vybraných OT
- jeden z nejdůležitějších pokroků (zveřejněných) v moderní kryptoanalýze
- znám NSA již v 70.letech v době návrhu DESu
- publikován v 1990 - Murphy, Biham & Shamir
- mocný nástroj pro analýzu blokových šifer
- v současnosti se používá k analýze moderních blokových šifer (s různou mírou úspěchu)
- DES je odolný vůči DK (na rozdíl od Luciferu)

Diferenciální kryptoanalýza

- statistický útok na šifry Feistelova typu
- předpoklad: máme k dispozici dvojice OT + k němu příslušný ŠT
- rozdíl mezi $d_P = P_1 \oplus P_2$, $d_C = C_1 \oplus C_2$
- vztah mezi d_C a d_P může odhalit informace o klíči
- abychom získali dobré diference d_P je potřeba mít k dispozici **mnoho párů** d_C a d_P
- D.K. umožní najít **některé** bity klíče, zbytek se získá hrubou silou



Diferenciální kryptoanalýza

- Změna problému z „Jaký klíč vygeneruje pár (OT_0, $ŠT_0$)?" na „Jaká množina klíčů může vyvolat změnu $ŠT_0$ na $ŠT_1$ změnou jednoho bitu v OT_0?“
- Útok pomocí diferenciální kryptoanalýzy na DES s 8 rundami vyžaduje:
  - 2^{14} = 16,384 vybraných OT, nebo
  - 2^{38} známých párů OT-ŠT
- Útok na DES se 16 rundami vyžaduje:
  - 2^{47} vybraných OT, nebo
  - přibližně $2^{55.1}$ známých párů OT-ŠT
- diferenciální kryptoanalýza není příliš efektivní
- **Návrháři DESu o DK 100% věděli!**

Lineární kryptoanalýza

- statistická metoda (stejně jako DK)
- analýza vnitřní struktury algoritmu
- náhrada celé šifry (velkou) množinou lineárních rovnic

- DES je lineární až na S-boxy
- Jak aproximovat S-box lineární funkcí ?
  - Těžko – neexistuje dobrá lineární aproximace žádného jednoho konkrétního bitu na výstupu, **ALE**
  - **existují** lineární kombinace výstupů, které lze aproximovat pomocí lineárních kombinací vstupů
- DES není optimalizován proti této technice
    - ale i tak to vyžaduje velké množství dvojic OT…
    - odhad části klíče a zbytek se spočte hrubou silou

Prolomení DES

- Když byl DES standardizován, útok hrubou silou byl technicky nemožný (výkon / cena tehdejších počítačů)
- 28.1.1997 - RSA Security vypisuje soutěž „DES Challenge“
- Úkol: rozluštit zprávu zašifrovanou pomocí DESu
- Odměna: 10.000$
- Proč: důkaz nízké bezpečnosti DESu
- 18.6.1997 – první prolomení DESu hrubou silou
  - zúčastnilo se 78.000 počítačů
  - ve špičce 14.000 během 24 hodin
  - klíč nalezen za 96 dní (prohledána cca ¼ prostoru klíčů)

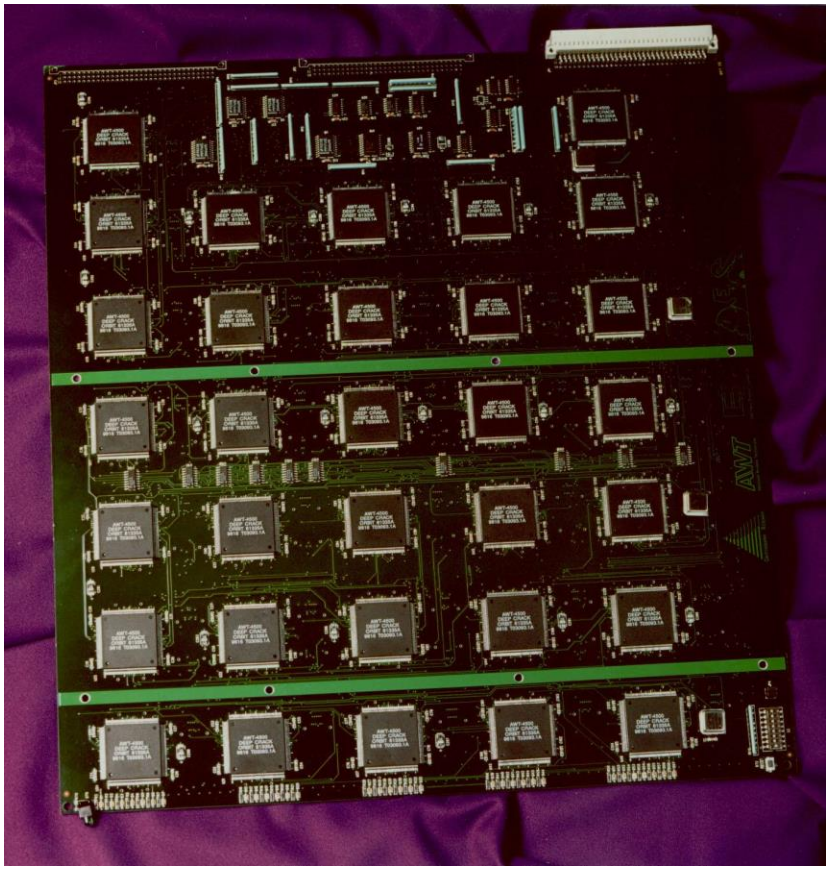
Prolomení DESu

- 1998 - **DES cracker** - projekt EFF (Electronic Frontier Foundation)
- útok hrubou silou na DES
- hrubý výpočetní výkon $9 \cdot 10^9$ klíčů/s
- cena $250.000
  - odměna za prolomení ale, pouze $10.000 !!!
- 29 desek plošných spojů
- na každé desce 64 čipů
- celkem 1856 ASIC čipů
- spočítá 1 DES klíč do 5 dnů

DES Cracker

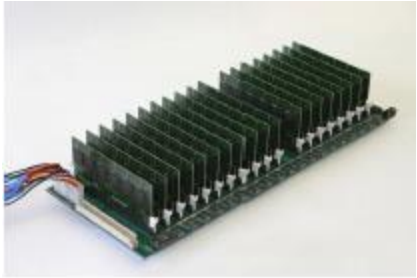
- DES Challenge II byl vyřešen po 56 hodinách pomocí stroje EFF DES Cracker
- OT: "The secret message is: It's time for those 128-, 192-, and 256-bit keys."

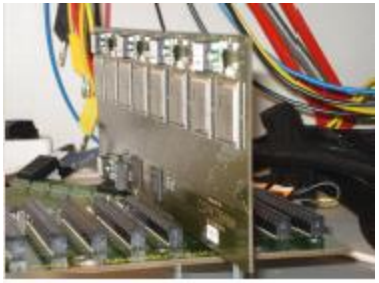
- DES Challenge III byl vyřešen za 22 hodin a 15 minut kombinace DES Crackeru a distribuovaných výpočtů
- OT: "See you in Rome (second AES Conference, March 22-23, 1999)."



Prolomení DES

- 2006 – nový stroj založený na FPGA (Field-Programmable Gate Array)
- COPACOBANA (COst-optimized PArallerl COdeBreaker)
- cena 10.000€
- průměrná doba nalezení klíče – 7 dní
- 2008 - COPACOBANA RIVYERA
  - zdokonalená verze
  - průměrná doba nalezení klíče – 24 hodin





Triple DES (3-DES)

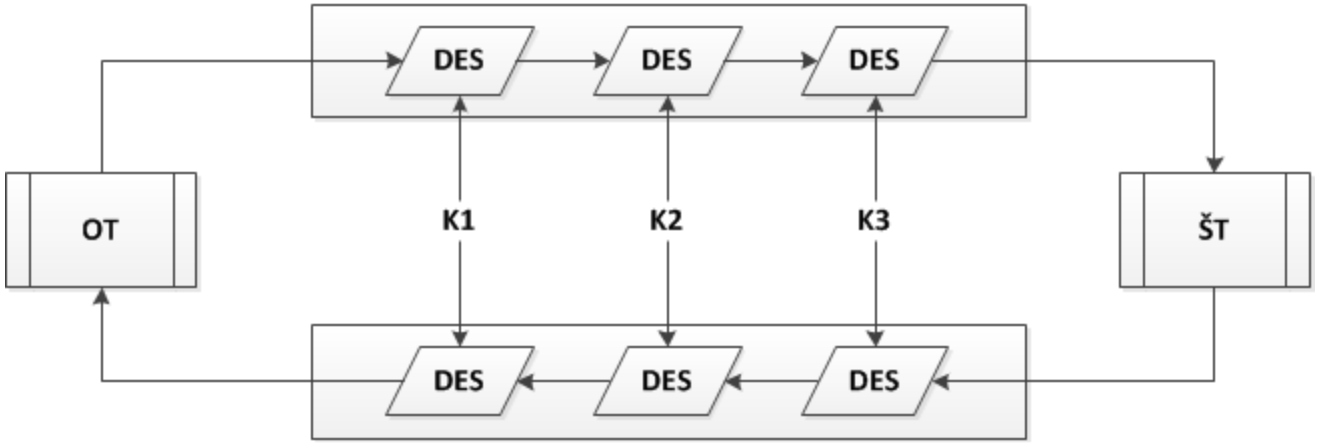
- Klíč o délce 56 bitů přestal v 90. letech postačovat
- DES byl široce rozšířen a nešlo ho rychle nahradit něčím zcela novým

Triple DES

- 3-DES-EDE2 byl standardizován v normách ANSI X9.17 a ISO 8732.

- Délka klíče 3DESu je 168 bitů (3x 56 bitů), ale díky možnosti tzv. meet-in-the-middle útoku (luštění současně z obou stran) je efektivní délka pouze 112 bitů.

Triple DES (3-DES)



Triple DES (3-DES)

- Nejčastější varianta: **Triple DES-EDE2**
  - $C = E(D(E(P,K_1),K_2),K_1)$
  - $P = D(E(D(C,K_1),K_2),K_1)$

- Proč používat 3DES-EDE se 2 klíči?
  - Zpětná kompatibilita: $E(D(E(P,K),K),K) = E(P,K)$
  - Klíč délky 112 bitů stačí

- Praktické použití 3DES dnes
  - PKCS#8 - šifrované soubory s privátními klíči (součást .pfx/.p12 blobů)
  - 3DES-EDE3-CBC

Dotazy