* ad IV pro CBC a CFB:
 - IV nemusí být tajný, tj. je možné ho přenášet spolu se zašifrovanou zprávou
 - IV musí být nepredikovatelný, dva doporučené způsoby vytváření
 - první způsob
  . pro každou zprávu vytvořit jedinečné číslo ”nonce”
  . nonce zašifrovat se stejným klíčem, jaký bude použit pro zprávu, tj. IV = E(nonce)
 - druhý způsob - kryptograficky bezpečný HW generátor náhodných čísel

* mód OFB (Output Feedback)
 - DES je použit pouze jako silný generátor pseudonáhodných čísel X1, X2, ... - postup generování viz popis níže
 - při šifrování se provádí Ci=Pi xor Xi, kde Xi je výstup DESu
 - dešifrování Pi=Ci xor Xi
 - DES v OFB módu:
  . na počátku je na vstup zaveden IV
  . X1 = E(IV), X2=E(X1), ...


**OFB mode**

 - výhoda: zotavení z chyby Ci po 1 bitu (neztratí-li se synchronizace)
  . šifrovací proud X1, X2, ... si můžeme připravit ještě před dostupností dat
  . IV nemusí být nepredikovatelný
 - nevýhody:
  . pokud je použit stejný klíč a IV, je vytvořený proud stejný - problém popsán u jednorázového klíče => pokud je stejný klíč, je pro každou zprávu nutné zvolit nový IV
  . cyklus takto konstruovaného RNG je cca 2^{n-1}; pokud by se použil posuvný registr se vstupem pouze n bitů Xi, tak je cyklus pouze 2^{n/2}) - proto se silně doporučuje první varianta
  . pro mnoho aplikací je výhodnější mód CTR popsaný níže

* mód CTR (Counter Mode)
 - podobně jako u OFB se DES používá jako silný generátor pseudonáhodných čísel
 - na počátku je do čítače T zaveden IV, obsah T zašifrujeme X1 = E(T)
 - pak T:=T+1, X2=E(T) atd., tj. v každém kroku se T zvětší o 1
 - šifrování a dešifrování opět C1 = P1 xor X1, P1 = C1 xor X1


**CTR mode**

 - řeší výše zmíněný problém krátkého cyklu RNG
 - má navíc vlastnost náhodného přístupu: je možné dešifrovat libovolný požadovaný blok aniž bychom museli dešifrovat n-1 blok
 - dokonce můžeme šifrovat více bloků paralelně
 - místo T:=T+1 můžeme použít jakoukoli fci, která zajistí jedinečnost všech T
 - problém - hodnota IV musí být taková, abychom zajistili jedinečnost obsahu čítače T přes všechny bloky šifrované stejným klíčem
  . tj. je to jako kdybychom spojili všechny zprávy šifrované stejným klíčem do jedné zprávy => celkový počet všech bloků nesmí překročit 2^m, kde m je počet bitů čítače
  . musíme si pamatovat stav čítače po zašifrování posledního bloku atd.
 - alternativní možnost:
  . každá zprávě přiřadit jedinečné číslo ”nonce” velikosti m/2 bitů, vložit na začátek T, inkrementovalo by se pouze druhých m/2 bitů čítače

Vlastnosti DESu
...............

- komplementační vlastnost

$$\text{jestliže } y = E_K(x), \text{ pak } \bar{y} = E_{\bar{K}}(\bar{x})$$

 . to Oskarovi moc nepomůže.
- má čtyři slabé a šest párů semislabých klíčů
 . slabé klíče: z klíče K vytvořené podklíče K1...K16 jsou stejné
 . pro slabý klíč platí: E_K(E_K(x)) = x
 . pro semislabý pár klíčů E_K1, E_K2 platí: E_K1(E_K2(x)) = x
 . slabé a semislabé klíče mají další nepěkné vlastnosti (32 pevných
   bodů pro slabé klíče E_K(x)=x, anti-pevné body pro semislabé klíče)
 . slabé a semislabé klíče bychom měli detekovat a nepoužívat

Útoky proti DESu:

* diferenciální kryptoanalýza - Biham a Shamir, 1991
* lineární kryptoanalýza - Matsui 1993 (včetně experimentálního ověření)
* různá další rozšíření lineární a diferenciální kryptoanalýzy,
  stále ještě nepraktické oproti hrubé síle, vyžadují příliš mnoho
  otevřených textů

| | otevřených textů | výpočetní složitost |
|---|---|---|
| hrubá síla | 1 | 2^{55} |
| lineární kryptoanalýza | 2^{43} nebo 2^{38} | 2^{43} nebo 2^{50} |
| diferenciální kryptoanalýza | 2^{55} | 2^{55} |
| | 2^{47} vybraných | 2^{47} |

Porovnání pouze hrubé, výpočet nemá stejnou cenu pro jednotlivé typy
útoků.

Kontraverze DESu
................

* DES byl už od svého zavedení provázen kontraverzí
 - DES založen na šifře IBM nazvané Lucifer která měla klíč 128 bitů
 - vláda doporučila konzultovat s NSA (National Security Agency)
 - na žádost NSA klíč zkrácen na 56 bitů a nezveřejněny principy návrhu
 - S-boxy navrženy NSA, podezření že NSA zabudovala do S-boxů ”zadní vrátka”

* ve skutečnosti autoři DESu znali diferenciální kryptoanalýzu
  (podle [Coppersmith 1994]), ale asi neznali lineární kryptoanalýzu
* podezření že NSA zabudovala do S-boxů ”zadní vrátka” se nepodařilo
  potvrdit; S-boxy od NSA pravděpodobně kvalitnější než původní od IBM
* asi jediné oslabení krátký klíč

* prostor klíčů 2^56 malý, existují návrhy strojů pro prohledávání hrubou silou

1977 návrh: Diffie a Hellman - stroj za 20 mil.$, který by prohledal prostor
     klíčů za < 1 den
1991 návrh: Čínská loterie (Quisquater a Girault)
     - předpokládejme že cca 1.2*10^9 lidí v Číně má rádio nebo televizi
     - každé rádio nebo TV by bylo vybaveno čipem který 10^6 op/sec
     - pokud by vláda chtěla zjistit klíč, odvysílala by pár (C,P)
     - všechna rádia a TV by začaly prohledávat část prostoru klíčů
     - do 60 sec prohledán, nálezci by se zobrazilo: ”Gratulujeme,
       právě jste vyhráli v čínské loterii! Pro získání ceny volejte 123456”.
1993 návrh: Wienerův stroj
        $100 000     35 hod
      $1 000 000     3,5 hod
     $10 000 000     21 min
1998 EFF DES Cracker (Kocher et al.) - za $250 000 včetně designu
     - skutečně postaven
     - za 56 hodin našel klíč i bez předchozí znalosti otevřeného textu
1999 distribuované hledání klíče, nalezen za 22h 15min
     - Deep Crack + cca 100 000 PC na internetu
     - lidé na internetu si nainstalují speciální klientský program

- zeptá se serveru na množinu klíčů, pak jí prohledá

* zřejmé, že DES už není bezpečný
* proto 1993 EES (Escrowed Encryption Standard) vytvořený NSA
 - algoritmus nepublikovat, ale dodat čipy v pouzdře odolném proti analýze
 - čip "Clipper", původně tajný algoritmus SKIPJACK 80 bitový klíč
 - každý čip pevný jedinečný klíč, rozdělený na poloviny mají dvě vládní organizace, vydají po soudním příkazu
* odpověď veřejnosti negativní, přesto schváleno v 1994 jako "dobrovolný standard", prakticky se neujalo.

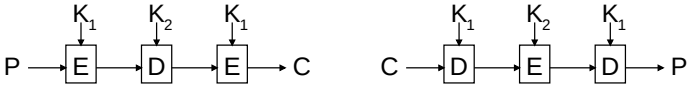
* přes výše uvedené je DES stále v mnoha aplikacích dodnes používán, např. bankomaty

3DES
....

* krátký klíč DESu už od počátku inspiroval snahu najít variantu s delším klíčem
* téměř všechny modifikace DESu se časem ukázaly jako horší než DES (GDES, RDES, ...) => šifru je zapotřebí navrhovat jako celek

* co takhle zesílit dvojitým šifrováním, tj. DES_K2(DES_K1(x))?
 - pak by místo 2^56 bylo 2^112 možných klíčů, v Čínské loterii byste mohli vyhrát cca po 10^11 letech
 - Merkle a Hellman 1981 ale přišli na metodu, kterou by se dalo hledání urychlit - meet-in-the-middle attack
 - redukuje z 2^{2k} na 2^k
  . Oskar má známý pár (c, p), c = E_K2(E_K1(p))
  . spočte všechny m = E_Ki(p) a zapamatuje (m_i, K_i)
  . počítá m_j = D_Kj(c), trefa m_i = m_j pro pravděpodobné řešení (K_i, K_j)
  . další známý otevřený text eliminuje kandidáty
  . potřebuje čas 2^{56} a prostor 2^{56}
 - existují vylepšení základního meet-in-the-middle, která potřebují méně paměti za cenu většího výpočtu
 - proto dvojité šifrování není považováno za bezpečnější než jednoduché

* proto se prakticky používá trojité šifrování - tripple-DES, 3DES
 - zavedla IBM v 1979, bylo adoptováno do standardů ANSI (1986) i ISO (1988)
 - IBM zvolila trojité šifrování se 2 klíči:




 - důvodem dvou klíčů šetření ve správě klíčů, 2^112 považováno za dostatečné
 - důvodem E-D-E zpětná kompatibilita: pokud K_1 = K_2 = K_3, je to DES
 - existují také útoky, ale nejsou praktické; vyžadují O(t) prostoru a 2^{120-lg(t)} operací
 - varianta pro paranoidní: E-E-E se třemi klíči (tj. 168 bitů)

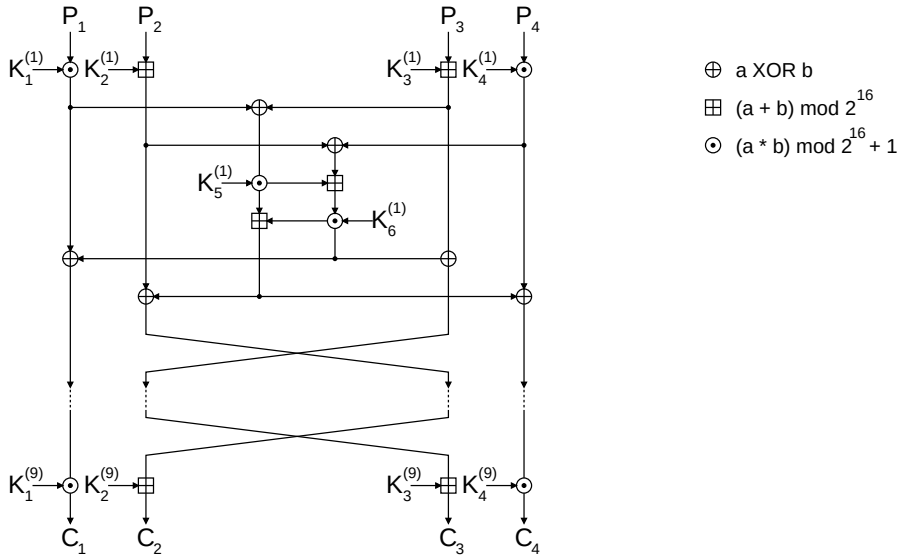
* otázka - pokud je DES tak slabý, 3DES je pomalý, tak proč nenavrhnout něco lepšího?
 - bylo navrženo mnoho dalších blokových šifer, asi nejdůležitější jsou IDEA (Lai a Massey 1990, Lai 1992), Blowfish (Schneier 1994) a SAFER (Massey 1994)
 - postupně se na ně podíváme

IDEA
----

* Lai a Massey 1991 PES (Proposed Encryption Standard, napadnutelný diferenciální kryptoanalýzou (2^{64} oproti 2^{128}) (Lai, Massey, Murphy)
* malá modifikace IPES (Improved PES), Massey a Lai
* komercionalizace pod jménem IDEA (International Data Encryption Algorithm), Lai 1992

* 64-bitový blok, 128-bitový klíč

* 8 iterací zobecněné Feistelovy struktury, následovány výstupní
  transformací, 16 bitové podklíče
* skládání operací ze tří pečlivě vybraných ”nekompatibilních” algebraických
  grup o 2^16 prvků, a to:
 - XOR 16 bitových podbloků
 - sčítání mod 2^16
 - modifikované násobení mod 2^{16}+1, nula je chápána jako 2^16




* výstup operace není nikdy použit jako vstup pro operaci stejného typu.
* funkce jedné iterace je úplná v tom smyslu, že každý bit otevřeného
  textu závisí na každém bitu šifrového textu a každém bitu podklíče

Nejdražší operací násobení modulo 2^{16}+1.

Dešifrování stejnou strukturu jako šifrování, dešifrovací podklíče
z šifrovacích jako příslušnou aditivní nebo multiplikativní inverzi.

Útoky:
* Daemen 1994, 1995 našel několik tříd slabých klíčů, náhodně vybraný klíč
  je slabý s p = 2{-77}
* žádné jiné dosud publikované útoky nejsou lepší než prohledávání hrubou silou
* pravděpodobně největší slabost malá délka bloku (platí pro všechny
  šifry s délkou bloku 64 bitů)

* nevýhoda: IDEA je patentovaná (mezinárodní patent WO 91/18459)
* patentování šifry IDEA podnítilo vznik nepatentovaných šifer Blowfish
  a SAFER (obě 1994)

❇