Blokové šifry

přednáška pro Úvod do kryptografie, verze $\pi + \varepsilon$

Michal Havlíček

KM FJFI ČVUT

1. dubna 2010

Prolomení šifry DES

- **DES**: 56-bit klíč $= 2^{56} = 72\ 057\ 594\ 037\ 927\ 936$ možností

Prolomení šifry DES

- **DES**: 56-bit klíč $= 2^{56} = 72\ 057\ 594\ 037\ 927\ 936$ možností
- V době standardizace **DES** (1976) se věří, že stroj schopný prolomit šifru metodou hrubé síly by byl neúnosně nákladný a navíc by pracoval neúnosně dlouho...

Prolomení šifry DES

- **DES**: 56-bit klíč $= 2^{56} = 72\ 057\ 594\ 037\ 927\ 936$ možností
- V době standardizace **DES** (1976) se věří, že stroj schopný prolomit šifru metodou hrubé síly by byl neúnosně nákladný a navíc by pracoval neúnosně dlouho...
- 28.1.1997 - RSA Security vypisuje soutěž **DES Challenge** (finanční odměna 10.000$) na prolomení **DES**.

Prolomení šifry DES

- **DES**: 56-bit klíč $= 2^{56} = 72\ 057\ 594\ 037\ 927\ 936$ možností
- V době standardizace **DES** (1976) se věří, že stroj schopný prolomit šifru metodou hrubé síly by byl neúnosně nákladný a navíc by pracoval neúnosně dlouho...
- 28.1.1997 - RSA Security vypisuje soutěž **DES Challenge** (finanční odměna 10.000$) na prolomení **DES**.
- Cíl: najít klíč šifry **DES** metodou hrubé síly

Prolomení šifry DES

- **DES**: 56-bit klíč $= 2^{56} = 72\ 057\ 594\ 037\ 927\ 936$ možností
- V době standardizace **DES** (1976) se věří, že stroj schopný prolomit šifru metodou hrubé síly by byl neúnosně nákladný a navíc by pracoval neúnosně dlouho...
- 28.1.1997 - RSA Security vypisuje soutěž **DES Challenge** (finanční odměna 10.000$) na prolomení **DES**.
- Cíl: najít klíč šifry **DES** metodou hrubé síly = zkoušet rozšifrovat text všemi možnými klíči a tím prokázat nedostatečnost šifry (nedostatečnou délku klíče).

DES Challenge

- 18.6.1997 - první úspěšný pokus - **DESCHALL Project**.

DES Challenge

- 18.6.1997 - první úspěšný pokus - **DESCHALL Project**.
- Skupina vědců z oblasti informatiky (Rocke Verser, Justin Dolske, Matt Curtin a kol.) a tisíce dobrovolníků propojí pomocí internetu osobní počítače.

DES Challenge

- 18.6.1997 - první úspěšný pokus - **DESCHALL Project**.
- Skupina vědců z oblasti informatiky (Rocke Verser, Justin Dolske, Matt Curtin a kol.) a tisíce dobrovolníků propojí pomocí internetu osobní počítače.
- Client software: výkon 1M klíčů / s (maximum na dobovém 200MHz Pentium)

DES Challenge

- 18.6.1997 - první úspěšný pokus - **DESCHALL Project**.
- Skupina vědců z oblasti informatiky (Rocke Verser, Justin Dolske, Matt Curtin a kol.) a tisíce dobrovolníků propojí pomocí internetu osobní počítače.
- Client software: výkon 1M klíčů / s (maximum na dobovém 200MHz Pentium) $\Rightarrow$ jeden počítač by hledal klíč $\approx$ 2285 let!
- Připojeno celkem 78.000 strojů, s maximem během 24h periody 14.000.

DES Challenge

- 18.6.1997 - první úspěšný pokus - **DESCHALL Project**.
- Skupina vědců z oblasti informatiky (Rocke Verser, Justin Dolske, Matt Curtin a kol.) a tisíce dobrovolníků propojí pomocí internetu osobní počítače.
- Client software: výkon 1M klíčů / s (maximum na dobovém 200MHz Pentium) $\Rightarrow$ jeden počítač by hledal klíč $\approx$ 2285 let!
- Připojeno celkem 78.000 strojů, s maximem během 24h periody 14.000.
- Klíč nalezen po prohledání asi 1/4 prostoru klíčů za 96 dnů.

DES Challenge

- 18.6.1997 - první úspěšný pokus - **DESCHALL Project**.
- Skupina vědců z oblasti informatiky (Rocke Verser, Justin Dolske, Matt Curtin a kol.) a tisíce dobrovolníků propojí pomocí internetu osobní počítače.
- Client software: výkon 1M klíčů / s (maximum na dobovém 200MHz Pentium) $\Rightarrow$ jeden počítač by hledal klíč $\approx$ 2285 let!
- Připojeno celkem 78.000 strojů, s maximem během 24h periody 14.000.
- Klíč nalezen po prohledání asi 1/4 prostoru klíčů za 96 dnů.
- Majitel počítače, který nalezl klíč získal odměnu 4000$.

DES Challenge II-1

- Únor 1998 - využití **distributed.net**

DES Challenge II-1

- Únor 1998 - využití **distributed.net** = distribuované řešení rozsáhlých numerických problémů využívající výkonu málo vytížených CPU/GPU zapojených do systému.
- Prolomeno za 41 dnů.

DES Challenge II-1

- Únor 1998 - využití **distributed.net** = distribuované řešení rozsáhlých numerických problémů využívající výkonu málo vytížených CPU/GPU zapojených do systému.
- Prolomeno za 41 dnů.
- Otevřený text: "The secret message is: Many hands make light work."

DES Challenge II-2

- 17.7.1998 - Stroj **Deep Crack** (**DES Cracker**) dešifruje text za 56 hodin (přijatelný důkaz slabosti **DES**, v té době už publikovány i nějaké kryptoanalytické postupy, **Deep Crack** ale prokázal praktičnost metody hrubé síly).

DES Challenge II-2

- 17.7.1998 - Stroj **Deep Crack** (**DES Cracker**) dešifruje text za 56 hodin (přijatelný důkaz slabosti **DES**, v té době už publikovány i nějaké kryptoanalytické postupy, **Deep Crack** ale prokázal praktičnost metody hrubé síly).
- Otevřený text: "The secret message is: It's time for those 128-, 192-, and 256-bit keys."

DES Cracker

- **EFF DES Cracker** (přezdívaný **Deep Crack**) sestavený **Electronic Frontier Foundation** (**EFF**) v roce 1998 (**EFF** - nezisková organizace zabývající se digitálním právem) ve spolupráci s **Cryptography Research Inc.**, **Advanced Wireless Technologies**, hlavní designer: Paul Kocher (prezident **CR**).

DES Cracker

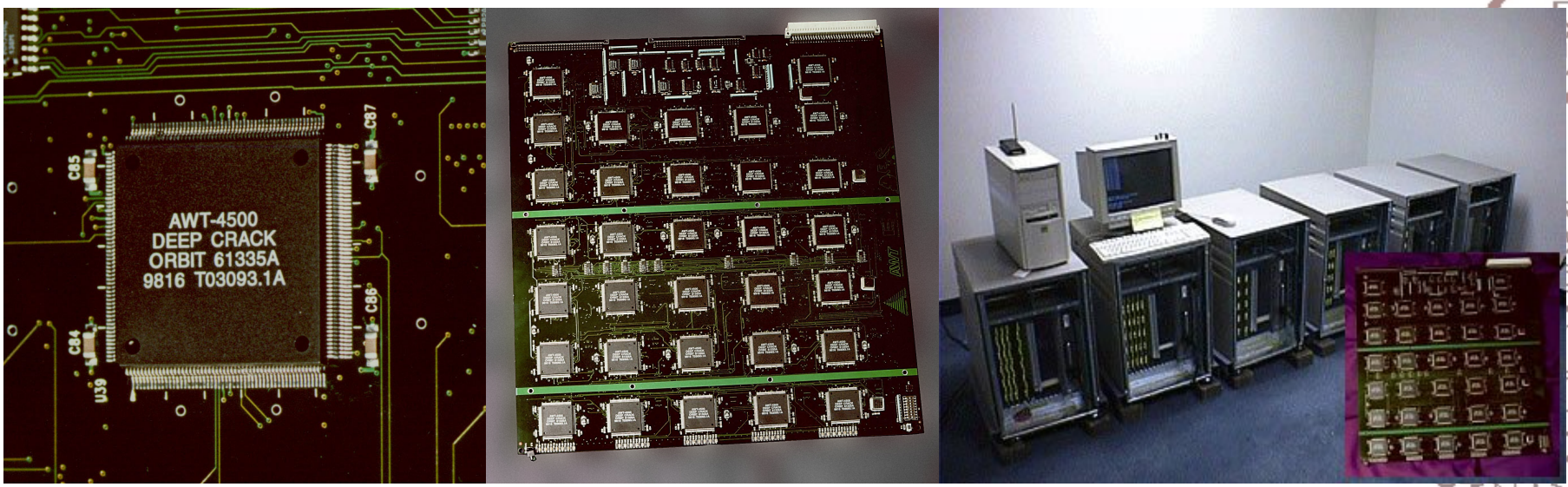
- **EFF DES Cracker** (přezdívaný **Deep Crack**) sestavený **Electronic Frontier Foundation** (**EFF**) v roce 1998 (**EFF** - nezisková organizace zabývající se digitálním právem) ve spolupráci s **Cryptography Research Inc.**, **Advanced Wireless Technologies**, hlavní designer: Paul Kocher (prezident **CR**).
- Náklady 250.000$ (přitom výhra **DES Challenge** činila 10.000$**!**)

DES Cracker

- **EFF DES Cracker** (přezdívaný **Deep Crack**) sestavený **Electronic Frontier Foundation** (**EFF**) v roce 1998 (**EFF** - nezisková organizace zabývající se digitálním právem) ve spolupráci s **Cryptography Research Inc.**, **Advanced Wireless Technologies**, hlavní designer: Paul Kocher (prezident **CR**).
- Náklady 250.000$ (přitom výhra **DES Challenge** činila 10.000$**!**)
- Výkon: test 90 miliard klíčů / s = 9 dnů k otestování všech možných (v průměru stačí polovina této doby).

Deep Crack

- 1856 čipů **ASIC** (**A**pplication **S**pecific **I**ntegrated **C**ircuit).
- Zasazeno do 29 desek (na každé 64 čipů) (sestaveno v **AWT**).
- Zamontováno do 6 skříní (Sun-4/470) (běžně používané pro servery), vše napojeno na PC.



DES Challenge III

- 19.1.1999 - **Deep Crack** ve spolupráci s **distributed.net** dešifruje **DES** za 22h 15m.

DES Challenge III

- 19.1.1999 - **Deep Crack** ve spolupráci s **distributed.net** dešifruje **DES** za 22h 15m.
- Otevřený text: "See you in Rome (second AES Conference, March 22-23, 1999)."

DES Challenge III

- 19.1.1999 - **Deep Crack** ve spolupráci s **distributed.net** dešifruje **DES** za 22h 15m.
- Otevřený text: "See you in Rome (second AES Conference, March 22-23, 1999)."
- Důsledky: navržen nový standard **Triple DES** (Říjen 1999),

DES Challenge III

- 19.1.1999 - **Deep Crack** ve spolupráci s **distributed.net** dešifruje **DES** za 22h 15m.
- Otevřený text: "See you in Rome (second AES Conference, March 22-23, 1999)."
- Důsledky: navržen nový standard **Triple DES** (Říjen 1999), výpočetní náročnost a nedokonalost klíče nakonec vedou k zavedení **AES** (26.5.2002).

COPACOBANA

- 2006 - sestaven jiný stroj založen na **FPGA** (**F**ield-**P**rogrammable **G**ate **A**rray) **COPACOBANA** (**CO**st-optimized **PA**rallerl **CO**de**B**reaker).

COPACOBANA

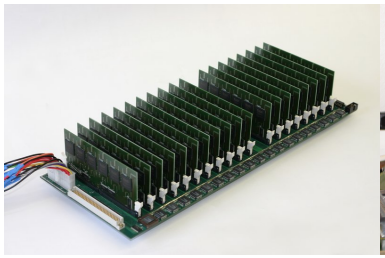
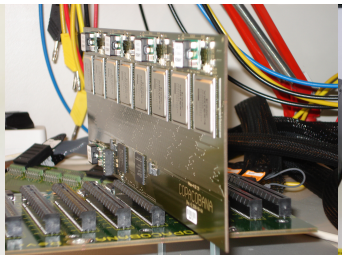
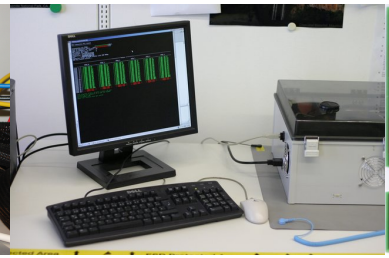
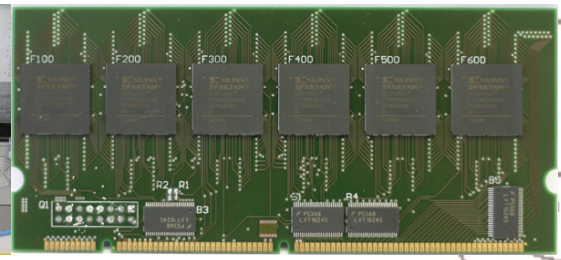
- 2006 - sestaven jiný stroj založen na **FPGA** (**F**ield-**P**rogrammable **G**ate **A**rray) **COPACOBANA** (**CO**st-optimized **PA**rallerl **CO**de**B**reaker).
- Podobný výkon jako **Deep Craker**, ale méně nákladný (způsobeno rozvojem v IC technologiích).

COPACOBANA

- 2006 - sestaven jiný stroj založen na **FPGA** (**F**ield-**P**rogrammable **G**ate **A**rray) **COPACOBANA** (**CO**st-optimized **PA**rallerl **CO**de**B**reaker).
- Podobný výkon jako **Deep Craker**, ale méně nákladný (způsobeno rozvojem v IC technologiích).
- 2008 - **COPACOBANA RIVYERA** (vylepšená verze) najde klíč v průměru za den!

COPACOBANA

- 2006 - sestaven jiný stroj založen na **FPGA** (**F**ield-**P**rogrammable **G**ate **A**rray) **COPACOBANA** (**CO**st-optimized **PA**rallerl **CO**de**B**reaker).
- Podobný výkon jako **Deep Craker**, ale méně nákladný (způsobeno rozvojem v IC technologiích).
- 2008 - **COPACOBANA RIVYERA** (vylepšená verze) najde klíč v průměru za den!

Triple DES

- Šifra odvozená z **DES**.

Triple DES

- Šifra odvozená z **DES**.
- Někdy pod názvy: **TDES**, **3DES**, **TDEA** (**T**riple **D**ata **E**ncryption **A**lgorithm).

Triple DES

- Šifra odvozená z **DES**.
- Někdy pod názvy: **TDES**, **3DES**, **TDEA** (**T**riple **D**ata **E**ncryption **A**lgorithm).
- Trojnásobná aplikace **DES** algoritmu na každý blok.

Triple DES

- Šifra odvozená z **DES**.
- Někdy pod názvy: **TDES**, **3DES**, **TDEA** (**T**riple **D**ata **E**ncryption **A**lgorithm).
- Trojnásobná aplikace **DES** algoritmu na každý blok.
- Výhoda: zvýšení odolnosti vůči útokům hrubou silou bez nutnosti vytvoření úplně nového algoritmu.

Triple DES

- Šifra odvozená z **DES**.
- Někdy pod názvy: **TDES**, **3DES**, **TDEA** (**T**riple **D**ata **E**ncryption **A**lgorithm).
- Trojnásobná aplikace **DES** algoritmu na každý blok.
- Výhoda: zvýšení odolnosti vůči útokům hrubou silou bez nutnosti vytvoření úplně nového algoritmu.
- Nevýhoda: pomalejší šifrování.

Triple DES

- Šifra odvozená z **DES**.
- Někdy pod názvy: **TDES**, **3DES**, **TDEA** (**T**riple **D**ata **E**ncryption **A**lgorithm).
- Trojnásobná aplikace **DES** algoritmu na každý blok.
- Výhoda: zvýšení odolnosti vůči útokům hrubou silou bez nutnosti vytvoření úplně nového algoritmu.
- Nevýhoda: pomalejší šifrování.
- Místo jednoho klíče - balík klíčů (skládá se z 3 **DES** klíčů: K1, K2, K3 - každý 56-bitový + bity kontroly parity).

Triple DES

Šifrování (po 64-bitových blocích):

- Šifrování textu s klíčem K1
- Dešifrování s klíčem K2
- Šifrování s klíčem K3

Dešifrování (inverzní operace):

- Dešifrování s klíčem K3
- Šifrování s klíčem K2
- Dešifrování s klíčem K1

Triple DES

Standard dále definuje tři možnosti použití:

- **1**: všechny klíče jsou na sobě nezávislé (nejsilnější verze).

Triple DES

Standard dále definuje tři možnosti použití:

- **1**: všechny klíče jsou na sobě nezávislé (nejsilnější verze).
- **2**: K1 a K2 na sobě nezávisí, ale: K3 = K1 (slabší, ale silnější než pouhá dvojnásobná aplikace **DES**, odolné vůči tzv. meet-in-the-middle útokům).

Triple DES

Standard dále definuje tři možnosti použití:

- **1**: všechny klíče jsou na sobě nezávislé (nejsilnější verze).
- **2**: K1 a K2 na sobě nezávisí, ale: K3 = K1 (slabší, ale silnější než pouhá dvojnásobná aplikace **DES**, odolné vůči tzv. meet-in-the-middle útokům).
- **3**: K1 = K2 = K3 (ekvivalentní **DES**, zpětná kompatibilita)

Bezpečnost Triple DES

- **1**: díky meet-in-the-middle atakům efektivní délka klíče = 112-bitů.
- **2**: náchylné k útokům pomocí chosen-plaintext/known-plaintext = 80-bitů efektivní klíč.
- Použití: Outlook 2007, elektronické bankovnictví (vylepšená verze)

Bezpečnost Triple DES

- **1**: díky meet-in-the-middle atakům efektivní délka klíče = 112-bitů.
- **2**: náchylné k útokům pomocí chosen-plaintext/known-plaintext = 80-bitů efektivní klíč.
  (known-plaintext = jsou k dispozici nějaké vzorky otevřeného textu a jejich zašifrované verze)
  (chosen-plaintext = předpoklad: je možnost získat libovolný otevřený text a je možnost ho zašifrovat a získat tak šifrový, viz "Zahradničení" za 2. světové války)

- Použití: Outlook 2007, elektronické bankovnictví (vylepšená verze)

Meet-in-the-middle

- Diffie, Hellman, 1977.

Meet-in-the-middle

- Diffie, Hellman, 1977.
- Idea: dva nezávislé klíče délky **n** $\Rightarrow$ hrubá síla $= 2^{2n}$ (všechny možné kombinace obou klíčů)

Meet-in-the-middle

- Diffie, Hellman, 1977.
- Idea: dva nezávislé klíče délky **n** $\Rightarrow$ hrubá síla $= 2^{2n}$ (všechny možné kombinace obou klíčů) (v případě jednoho klíče: 2^n).
- Šifrování s dvěma nezávislými klíči: $C = E_{K_2}(E_{K_1}(P))$, kde C - šifrový text, P - otevřený text, K_1,K_2 - klíče, E - šifrování

Meet-in-the-middle

- Diffie, Hellman, 1977.
- Idea: dva nezávislé klíče délky **n** $\Rightarrow$ hrubá síla $= 2^{2n}$ (všechny možné kombinace obou klíčů) (v případě jednoho klíče: 2^n).
- Šifrování s dvěma nezávislými klíči: $C = E_{K_2}(E_{K_1}(P))$, kde C - šifrový text, P - otevřený text, K_1,K_2 - klíče, E - šifrování
- Pokud zkoušíme kódovat z jednoho konce a dekódovat z druhého (postupně se kódování a dekodování k sobě přibližuje až se setká uprostřed = meet-in-the-middle) lze klíč najít za 2×2^n!

Meet-in-the-middle

- Diffie, Hellman, 1977.
- Idea: dva nezávislé klíče délky **n** $\Rightarrow$ hrubá síla $= 2^{2n}$ (všechny možné kombinace obou klíčů) (v případě jednoho klíče: 2^n).
- Šifrování s dvěma nezávislými klíči: $C = E_{K_2}(E_{K_1}(P))$, kde C - šifrový text, P - otevřený text, K_1,K_2 - klíče, E - šifrování
- Pokud zkoušíme kódovat z jednoho konce a dekódovat z druhého (postupně se kódování a dekodování k sobě přibližuje až se setká uprostřed = meet-in-the-middle) lze klíč najít za 2×2^n!
- Postup: spočteme $E_K(P)$ pro všechny možné klíče a výsledky uložíme do paměti, pak je provedeno dešifrování $D_K(C)$ pro všechny možné klíče, případné shody pak odhalují původní klíče.

DES-X

- Ron Rivest, Květen 1984.

DES-X

- Ron Rivest, Květen 1984.
- Varianta **DES** vytvořená za účelem znesnadnění útoku metodou hrubé síly (aniž by bylo nutné podstatněji zasahovat do původního algoritmu) přidáním key whiteningu.

DES-X

- Ron Rivest, Květen 1984.
- Varianta **DES** vytvořená za účelem znesnadnění útoku metodou hrubé síly (aniž by bylo nutné podstatněji zasahovat do původního algoritmu) přidáním key whiteningu.
- Metoda key whitening: kombinování dat s částí klíče pomocí nějaké operace (nejčastěji **XOR**) před prvním krokem šifrování a po posledním.

DES-X

- Ron Rivest, Květen 1984.
- Varianta **DES** vytvořená za účelem znesnadnění útoku metodou hrubé síly (aniž by bylo nutné podstatněji zasahovat do původního algoritmu) přidáním key whiteningu.
- Metoda key whitening: kombinování dat s částí klíče pomocí nějaké operace (nejčastěji **XOR**) před prvním krokem šifrování a po posledním.
- První bloková šifra, která tuto metodu použila (později například šifra **Twofish**).

DES-X

- Ron Rivest, Květen 1984.
- Varianta **DES** vytvořená za účelem znesnadnění útoku metodou hrubé síly (aniž by bylo nutné podstatněji zasahovat do původního algoritmu) přidáním key whiteningu.
- Metoda key whitening: kombinování dat s částí klíče pomocí nějaké operace (nejčastěji **XOR**) před prvním krokem šifrování a po posledním.
- První bloková šifra, která tuto metodu použila (později například šifra **Twofish**).
- Vyžaduje navíc další dva 64-bitové klíče (pro whitening) - jeden k otevřenému textu před vlastním šifrováním **DES** a druhý k aplikaci po zašifrování.

DES-X

- Ron Rivest, Květen 1984.
- Varianta **DES** vytvořená za účelem znesnadnění útoku metodou hrubé síly (aniž by bylo nutné podstatněji zasahovat do původního algoritmu) přidáním key whiteningu.
- Metoda key whitening: kombinování dat s částí klíče pomocí nějaké operace (nejčastěji **XOR**) před prvním krokem šifrování a po posledním.
- První bloková šifra, která tuto metodu použila (později například šifra **Twofish**).
- Vyžaduje navíc další dva 64-bitové klíče (pro whitening) - jeden k otevřenému textu před vlastním šifrováním **DES** a druhý k aplikaci po zašifrování.
- Velikost klíče: 56+2x64=184-bitů.

DES-X

- Ron Rivest, Květen 1984.
- Varianta **DES** vytvořená za účelem znesnadnění útoku metodou hrubé síly (aniž by bylo nutné podstatněji zasahovat do původního algoritmu) přidáním key whiteningu.
- Metoda key whitening: kombinování dat s částí klíče pomocí nějaké operace (nejčastěji **XOR**) před prvním krokem šifrování a po posledním.
- První bloková šifra, která tuto metodu použila (později například šifra **Twofish**).
- Vyžaduje navíc další dva 64-bitové klíče (pro whitening) - jeden k otevřenému textu před vlastním šifrováním **DES** a druhý k aplikaci po zašifrování.
- Velikost klíče: 56+2x64=184-bitů.
- Bezpečnost: differental cryptanalysis: 2^{61} chosen plaintext (**DES** 2^{47}), linear cryptanalysis: 2^{60} (**DES** 2^{43}).

Advanced Encryption Standard Process

- 1.2.1997 - zahájen proces (první tři měsíce: návrhy na požadavky na nový algoritmus).

Advanced Encryption Standard Process

- 1.2.1997 - zahájen proces (první tři měsíce: návrhy na požadavky na nový algoritmus).
- 12.9.1997 - zahájen výběr kandidátů, požadavky: blokové šifrování, 128-bit bloky, 128, 192, 256-bit klíč

Advanced Encryption Standard Process

- 1.2.1997 - zahájen proces (první tři měsíce: návrhy na požadavky na nový algoritmus).
- 12.9.1997 - zahájen výběr kandidátů, požadavky: blokové šifrování, 128-bit bloky, 128, 192, 256-bit klíč $\leftarrow$ v té době takových šifer málo (nejznámější: **Square**).
- Během 9 měsíců vybráno 15 kandidátů.

Advanced Encryption Standard Process

- 1.2.1997 - zahájen proces (první tři měsíce: návrhy na požadavky na nový algoritmus).
- 12.9.1997 - zahájen výběr kandidátů, požadavky: blokové šifrování, 128-bit bloky, 128, 192, 256-bit klíč $\leftarrow$ v té době takových šifer málo (nejznámější: **Square**).
- Během 9 měsíců vybráno 15 kandidátů.
- Srpen 1998, Březen 1999 - konference **AES1**, **AES2** (kandidáti zkoumáni nejen z hlediska bezpečnosti ale také výkonu a možnosti implementace na různém hardware/software).

Advanced Encryption Standard Process

- 1.2.1997 - zahájen proces (první tři měsíce: návrhy na požadavky na nový algoritmus).
- 12.9.1997 - zahájen výběr kandidátů, požadavky: blokové šifrování, 128-bit bloky, 128, 192, 256-bit klíč $\leftarrow$ v té době takových šifer málo (nejznámější: **Square**).
- Během 9 měsíců vybráno 15 kandidátů.
- Srpen 1998, Březen 1999 - konference **AES1**, **AES2** (kandidáti zkoumáni nejen z hlediska bezpečnosti ale také výkonu a možnosti implementace na různém hardware/software).
- Srpen 1999 - vybráno pět finalistů: **Rijndael**, **Serpent**, **Twofish**, **RC6**, **MARS**.

Advanced Encryption Standard Process

- 1.2.1997 - zahájen proces (první tři měsíce: návrhy na požadavky na nový algoritmus).
- 12.9.1997 - zahájen výběr kandidátů, požadavky: blokové šifrování, 128-bit bloky, 128, 192, 256-bit klíč $\leftarrow$ v té době takových šifer málo (nejznámější: **Square**).
- Během 9 měsíců vybráno 15 kandidátů.
- Srpen 1998, Březen 1999 - konference **AES1**, **AES2** (kandidáti zkoumáni nejen z hlediska bezpečnosti ale také výkonu a možnosti implementace na různém hardware/software).
- Srpen 1999 - vybráno pět finalistů: **Rijndael**, **Serpent**, **Twofish**, **RC6**, **MARS**.
- Duben 2000 - konference **AES3** (mimo jiné s prezentacemi tvůrců).

Advanced Encryption Standard Process

- 1.2.1997 - zahájen proces (první tři měsíce: návrhy na požadavky na nový algoritmus).
- 12.9.1997 - zahájen výběr kandidátů, požadavky: blokové šifrování, 128-bit bloky, 128, 192, 256-bit klíč $\leftarrow$ v té době takových šifer málo (nejznámější: **Square**).
- Během 9 měsíců vybráno 15 kandidátů.
- Srpen 1998, Březen 1999 - konference **AES1**, **AES2** (kandidáti zkoumáni nejen z hlediska bezpečnosti ale také výkonu a možnosti implementace na různém hardware/software).
- Srpen 1999 - vybráno pět finalistů: **Rijndael**, **Serpent**, **Twofish**, **RC6**, **MARS**.
- Duben 2000 - konference **AES3** (mimo jiné s prezentacemi tvůrců).
- 2.10.2000 - vybrán **Rijndael** (a zahájen proces standardizace).

AES (Rijndael)

- Vincent Rijmen a Joan Daemen, publikováno 1998.

AES (Rijndael)

- Vincent Rijmen a Joan Daemen, publikováno 1998.
- Přijat za standard 26.11.2001.

AES (Rijndael)

- Vincent Rijmen a Joan Daemen, publikováno 1998.
- Přijat za standard 26.11.2001.
- Odvozeno z: **Square**.

AES (Rijndael)

- Vincent Rijmen a Joan Daemen, publikováno 1998.
- Přijat za standard 26.11.2001.
- Odvozeno z: **Square**.
- AES jako základ dalších šifer: **Anubis**, **Grand Cru** ...

AES (Rijndael)

- Vincent Rijmen a Joan Daemen, publikováno 1998.
- Přijat za standard 26.11.2001.
- Odvozeno z: **Square**.
- AES jako základ dalších šifer: **Anubis**, **Grand Cru** ...
- Velikost klíče: 128, 192, 256-bitů

AES (Rijndael)

- Vincent Rijmen a Joan Daemen, publikováno 1998.
- Přijat za standard 26.11.2001.
- Odvozeno z: **Square**.
- AES jako základ dalších šifer: **Anubis**, **Grand Cru** ...
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloků: 128-bitů (původní sada algoritmů **Rijndael**: velikost bloku: násobek-32 (max 256), klíč: násobek-32 (teoreticky neomezeno)

AES (Rijndael)

- Vincent Rijmen a Joan Daemen, publikováno 1998.
- Přijat za standard 26.11.2001.
- Odvozeno z: **Square**.
- AES jako základ dalších šifer: **Anubis**, **Grand Cru** ...
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloků: 128-bitů
- Princip: substitučně permutační (nepoužívá **Feistel síť** na rozdíl od **DES** a jeho zobecnění).

AES (Rijndael)

- Vincent Rijmen a Joan Daemen, publikováno 1998.
- Přijat za standard 26.11.2001.
- Odvozeno z: **Square**.
- AES jako základ dalších šifer: **Anubis**, **Grand Cru** ...
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloků: 128-bitů
- Princip: substitučně permutační (nepoužívá **Feistel síť** na rozdíl od **DES** a jeho zobecnění).
- Cyklů: 10, 12, 14 (v závislosti na velikosti klíče).

AES (Rijndael)

- Vincent Rijmen a Joan Daemen, publikováno 1998.
- Přijat za standard 26.11.2001.
- Odvozeno z: **Square**.
- AES jako základ dalších šifer: **Anubis**, **Grand Cru** ...
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloků: 128-bitů
- Princip: substitučně permutační (nepoužívá **Feistel síť** na rozdíl od **DES** a jeho zobecnění).
- Cyklů: 10, 12, 14 (v závislosti na velikosti klíče).
- Pracuje na 4x4 poli (matici) bajtů (tzv. state).

AES (Rijndael)

- Vincent Rijmen a Joan Daemen, publikováno 1998.
- Přijat za standard 26.11.2001.
- Odvozeno z: **Square**.
- AES jako základ dalších šifer: **Anubis**, **Grand Cru** ...
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloků: 128-bitů
- Princip: substitučně permutační (nepoužívá **Feistel síť** na rozdíl od **DES** a jeho zobecnění).
- Cyklů: 10, 12, 14 (v závislosti na velikosti klíče).
- Pracuje na 4x4 poli (matici) bajtů (tzv. state).
- Šifrování: několikerá aplikace transformací, každá se skládá z několika kroků, některé závisí na volbě klíče.

AES (Rijndael)

- Vincent Rijmen a Joan Daemen, publikováno 1998.
- Přijat za standard 26.11.2001.
- Odvozeno z: **Square**.
- AES jako základ dalších šifer: **Anubis**, **Grand Cru** ...
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloků: 128-bitů
- Princip: substitučně permutační (nepoužívá **Feistel síť** na rozdíl od **DES** a jeho zobecnění).
- Cyklů: 10, 12, 14 (v závislosti na velikosti klíče).
- Pracuje na 4x4 poli (matici) bajtů (tzv. state).
- Šifrování: několikerá aplikace transformací, každá se skládá z několika kroků, některé závisí na volbě klíče.
- Dešifrování = inverzní proces.

AES - šifrování

Operace prováděné pouze na začátku:

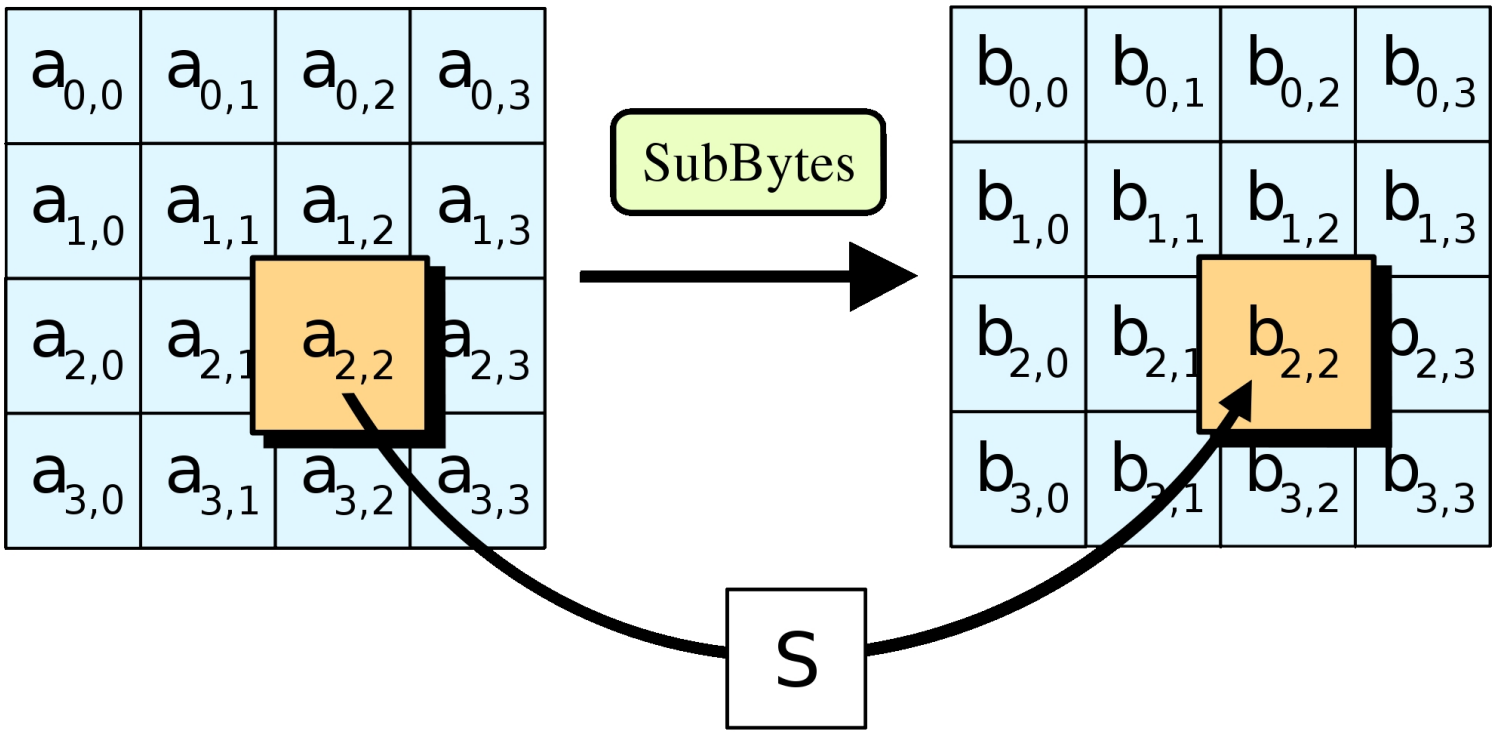
- **KeyExpansion** (rozklad klíče na několik sub-klíčů pro každou iteraci pomocí několika různých operací (cyklický posun bitů, n-tá mocnina dvou (n = počet iterací), S-box)).
- **InitialRound** (**AddRoundKey** - každý bajt stavové matice (state) je kombinován se sub-klíčem dané iterace (round key)).

Operace prováděné **n**-krát (**n** = počet iterací):

- **SubBytes** - nelineární substituce (každý bajt je nahrazen jiným dle vyhledávací tabulky - **Rijndael S-Box**).
- **ShiftRows** - na každý řádek stavové matice (state) je aplikován cyklický posun.
- **MixColumns** - zkombinování bajtů každého sloupce stavové matice (state).
- **AddRoundKey**

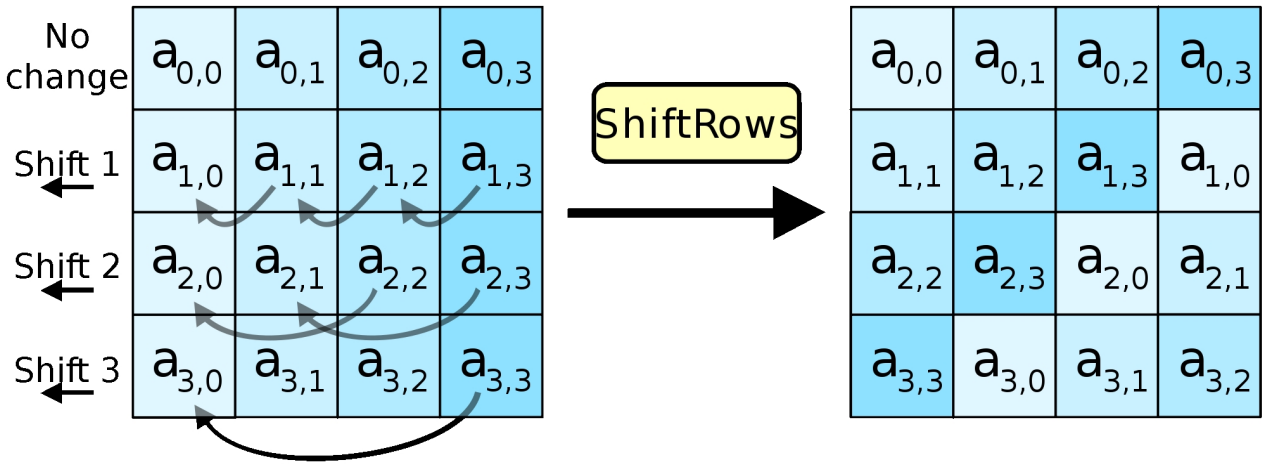
Operace prováděné pouze na konci: stejně jako předchozí ale bez operace **MixColumn**.

AES - SubBytes



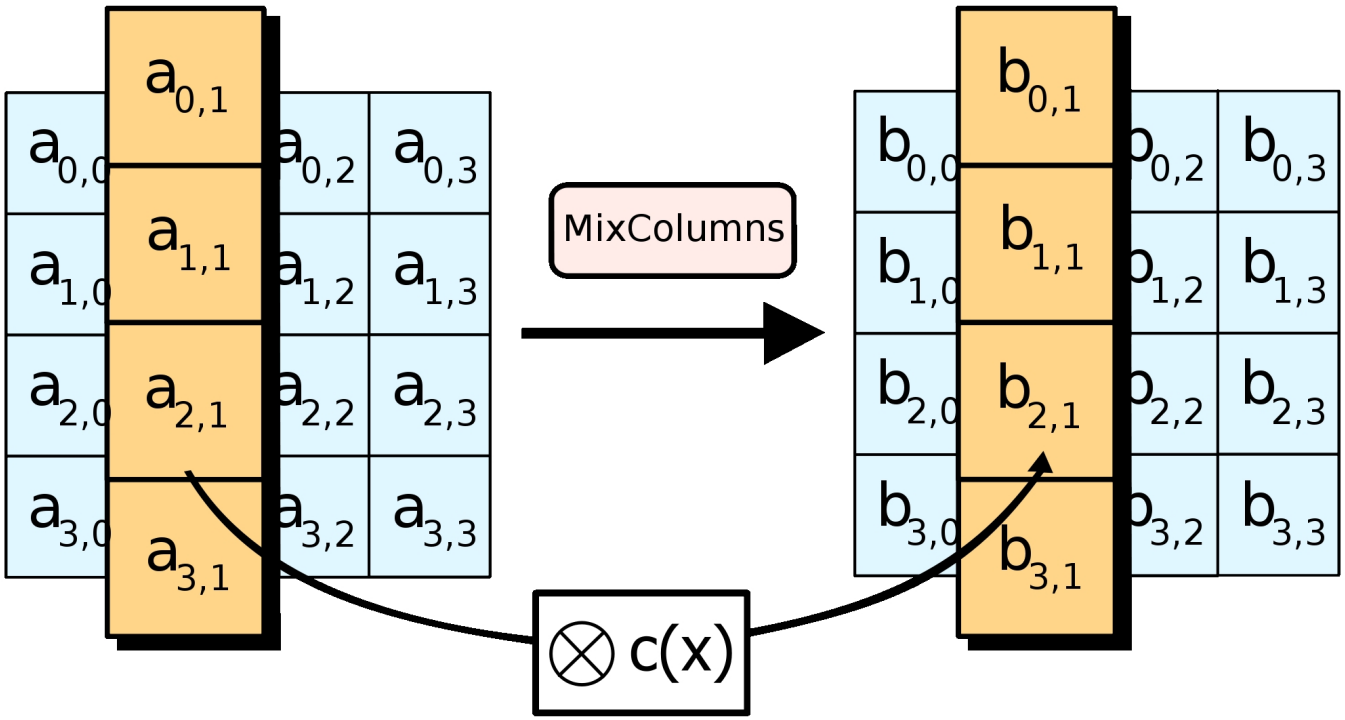
AES - ShiftRows

Bajty v každém řádku jsou posunuty doleva, v každém řádku je ovšem počet přesouvaných bajtů a délka posunu jiná.



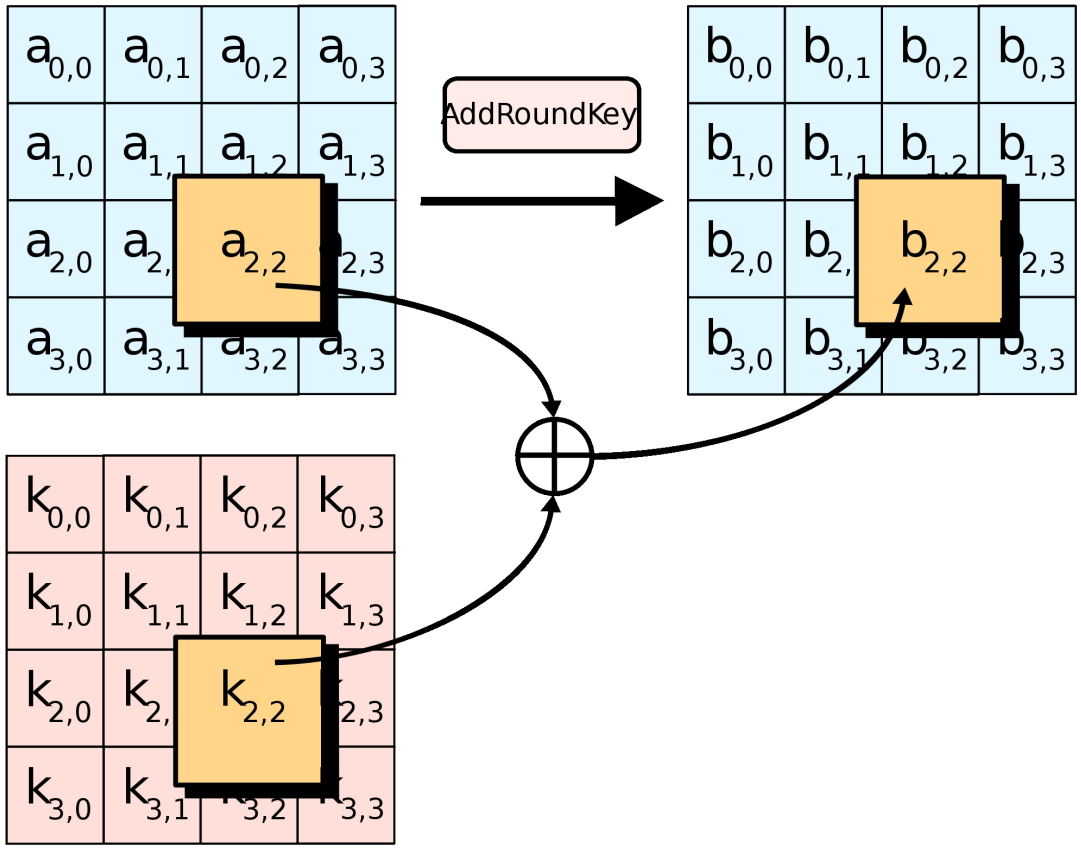
AES - MixColumns

Každý sloupec state matice je násoben pevně daným polynomem $c(x) = 3 \times x^3 + x^2 + x + 2$ (spolu s operacemi **ShiftRows** provádí difuzi šifry).



AES - AddRoundKey

Sub-klíč je kombinován s maticí stavu, pro každou iteraci je sub-klíč odvozen ze základního klíče (pomocí Rijndeal key schedule v kroku **KeyExpansion**), jednotlivé bajty klíče jsou bitově XORovány s odpovídajícími bajty sub-klíče.



AES - bezpečnost

- Květen 2009 - side-channel attack (neútočí na šifrování jako takové ale na konkrétní implementaci jejíž chybou uniknou data).

AES - bezpečnost

- Květen 2009 - side-channel attack (neútočí na šifrování jako takové ale na konkrétní implementaci jejíž chybou uniknou data).
- 2002 - **XSL** attack pro případ 128-bit klíče (2^{100} operací $\times$ hrubá síla: 2^{128}) $\leftarrow$ teoretický útok (Nicolas Courtois, Josef Pieprzyk) který měl za cíl poukázat na slabinu zapříčiněnou jednoduchým popisem systému (později se ukázalo, že nemohl fungovat).

AES - bezpečnost

- Květen 2009 - side-channel attack (neútočí na šifrování jako takové ale na konkrétní implementaci jejíž chybou uniknou data).
- 2002 - **XSL** attack pro případ 128-bit klíče (2^{100} operací $\times$ hrubá síla: 2^{128}) $\leftarrow$ teoretický útok (Nicolas Courtois, Josef Pieprzyk) který měl za cíl poukázat na slabinu zapříčiněnou jednoduchým popisem systému (později se ukázalo, že nemohl fungovat).
- 1.7.2009 related-key attack (192/256-bit verze)

AES - bezpečnost

- Květen 2009 - side-channel attack (neútočí na šifrování jako takové ale na konkrétní implementaci jejíž chybou uniknou data).
- 2002 - **XSL** attack pro případ 128-bit klíče (2^{100} operací $\times$ hrubá síla: 2^{128}) $\leftarrow$ teoretický útok (Nicolas Courtois, Josef Pieprzyk) který měl za cíl poukázat na slabinu zapříčiněnou jednoduchým popisem systému (později se ukázalo, že nemohl fungovat).
- 1.7.2009 related-key attack (192/256-bit verze) = útočník sleduje jak se mění šifrování v závislosti na změnách v klíči, kde klíč není celý znám ale jsou známy jeho jisté vlastnosti (například nějaké bity klíče jsou stejné).

XSL útok

- Nicolas Courtois, Josef Pieprzyk, 2002.

XSL útok

- Nicolas Courtois, Josef Pieprzyk, 2002.
- Založeno na soustavě kvadratických rovnic (pro 128-bit AES 8000 rovnic o 1600 neznámých).

XSL útok

- Nicolas Courtois, Josef Pieprzyk, 2002.
- Založeno na soustavě kvadratických rovnic (pro 128-bit AES 8000 rovnic o 1600 neznámých).
- Řešení soustavy odkrývá klíč.

XSL útok

- Nicolas Courtois, Josef Pieprzyk, 2002.
- Založeno na soustavě kvadratických rovnic (pro 128-bit AES 8000 rovnic o 1600 neznámých).
- Řešení soustavy odkrývá klíč.
- Výhoda: vyžaduje jen několik otevřených textů.

XSL útok

- Nicolas Courtois, Josef Pieprzyk, 2002.
- Založeno na soustavě kvadratických rovnic (pro 128-bit AES 8000 rovnic o 1600 neznámých).
- Řešení soustavy odkrývá klíč.
- Výhoda: vyžaduje jen několik otevřených textů.
- Nevýhoda: náročnost.

XSL útok

- Nicolas Courtois, Josef Pieprzyk, 2002.
- Založeno na soustavě kvadratických rovnic (pro 128-bit AES 8000 rovnic o 1600 neznámých).
- Řešení soustavy odkrývá klíč.
- Výhoda: vyžaduje jen několik otevřených textů.
- Nevýhoda: náročnost.

Na **AES4** konferenci (Bonn, 2004) V. Rijmen okomentoval **XSL**:
"*The XSL attack is not an attack. It is a dream.*"

XSL útok

- Nicolas Courtois, Josef Pieprzyk, 2002.
- Založeno na soustavě kvadratických rovnic (pro 128-bit AES 8000 rovnic o 1600 neznámých).
- Řešení soustavy odkrývá klíč.
- Výhoda: vyžaduje jen několik otevřených textů.
- Nevýhoda: náročnost.

Na **AES4** konferenci (Bonn, 2004) V. Rijmen okomentoval **XSL**:
"*The XSL attack is not an attack. It is a dream.*"
Načež mu N. Courtois pohotově odpověděl:
"*It will become your nightmare.*"

Serpent

- Finalista **AES**, *2.místo*.

Serpent

- Finalista **AES**, *2.místo*.
- Ross Anderson, Eli Biham, Lars Knudsen, publikováno 21.8.1998.

Serpent

- Finalista **AES**, *2.místo*.
- Ross Anderson, Eli Biham, Lars Knudsen, publikováno 21.8.1998.
- Odvozeno z **Square**.

Serpent

- Finalista **AES**, *2.místo*.
- Ross Anderson, Eli Biham, Lars Knudsen, publikováno 21.8.1998.
- Odvozeno z **Square**.
- Velikost klíče: 128, 192, 256-bitů

Serpent

- Finalista **AES**, *2.místo*.
- Ross Anderson, Eli Biham, Lars Knudsen, publikováno 21.8.1998.
- Odvozeno z **Square**.
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloku: 128-bitů (4 x 32-bitová slova).

Serpent

- Finalista **AES**, *2.místo*.
- Ross Anderson, Eli Biham, Lars Knudsen, publikováno 21.8.1998.
- Odvozeno z **Square**.
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloku: 128-bitů (4 x 32-bitová slova).
- Princip: substitučně-permutační síť.

Serpent

- Finalista **AES**, *2.místo*.
- Ross Anderson, Eli Biham, Lars Knudsen, publikováno 21.8.1998.
- Odvozeno z **Square**.
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloku: 128-bitů (4 x 32-bitová slova).
- Princip: substitučně-permutační síť.
- 32 cyklů (dle autorů zaručuje bezpečnost již 16 cyklů) + počáteční a konečná permutace.

Serpent

- Finalista **AES**, *2.místo*.
- Ross Anderson, Eli Biham, Lars Knudsen, publikováno 21.8.1998.
- Odvozeno z **Square**.
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloku: 128-bitů (4 x 32-bitová slova).
- Princip: substitučně-permutační síť.
- 32 cyklů (dle autorů zaručuje bezpečnost již 16 cyklů) + počáteční a konečná permutace.
- V každém z 32 cyklů je aplikován 1 z 8 4-bity-na-4-bity S-box (32-krát paralelně), (všechny operace lze provádět paralelně na 32 1-bitových řezech, maximální paralelizace) míchání klíče XORem (první a poslední fáze).

Serpent

Nepatentováno, volně k dispozici, lze bezplatně používat, bez omezení, možno implementovat do svého vlastního software/hardware řešení.

Bezpečnost:

- Obecně bezpečnější než **AES**.

Serpent

Nepatentováno, volně k dispozici, lze bezplatně používat, bez omezení, možno implementovat do svého vlastního software/hardware řešení.

Bezpečnost:

- Obecně bezpečnější než **AES**.
- Teoreticky napadnutelný pomocí **XSL**.

Serpent

Nepatentováno, volně k dispozici, lze bezplatně používat, bez omezení, možno implementovat do svého vlastního software/hardware řešení.

Bezpečnost:

- Obecně bezpečnější než **AES**.
- Teoreticky napadnutelný pomocí **XSL**.
- Věří se, že implementace **XSL** by byla náročnější než metoda hrubé síly!

Blowfish

- Bruce Schneier, 1993.

Blowfish

- Bruce Schneier, 1993.
- Velikost klíče: 32-448-bitů v 8-bit krocích (standardně 128-bit klíč).

Blowfish

- Bruce Schneier, 1993.
- Velikost klíče: 32-448-bitů v 8-bit krocích (standardně 128-bit klíč).
- Velikost bloku: 64-bitů

Blowfish

- Bruce Schneier, 1993.
- Velikost klíče: 32-448-bitů v 8-bit krocích (standardně 128-bit klíč).
- Velikost bloku: 64-bitů
- Princip: **Feistel síť**

Blowfish

- Bruce Schneier, 1993.
- Velikost klíče: 32-448-bitů v 8-bit krocích (standardně 128-bit klíč).
- Velikost bloku: 64-bitů
- Princip: **Feistel síť**
- Využívá na klíči závislých S-boxů.

Blowfish

- Bruce Schneier, 1993.
- Velikost klíče: 32-448-bitů v 8-bit krocích (standardně 128-bit klíč).
- Velikost bloku: 64-bitů
- Princip: **Feistel síť**
- Využívá na klíči závislých S-boxů.
- Cyklů: 16

Blowfish

- Bruce Schneier, 1993.
- Velikost klíče: 32-448-bitů v 8-bit krocích (standardně 128-bit klíč).
- Velikost bloku: 64-bitů
- Princip: **Feistel síť**
- Využívá na klíči závislých S-boxů.
- Cyklů: 16
- Efektivní softwareová implementace.

Blowfish

- Bruce Schneier, 1993.
- Velikost klíče: 32-448-bitů v 8-bit krocích (standardně 128-bit klíč).
- Velikost bloku: 64-bitů
- Princip: **Feistel síť**
- Využívá na klíči závislých S-boxů.
- Cyklů: 16
- Efektivní softwareová implementace.
- Navíc dodnes žádná účinná kryptoanalýza nalezena!

Blowfish

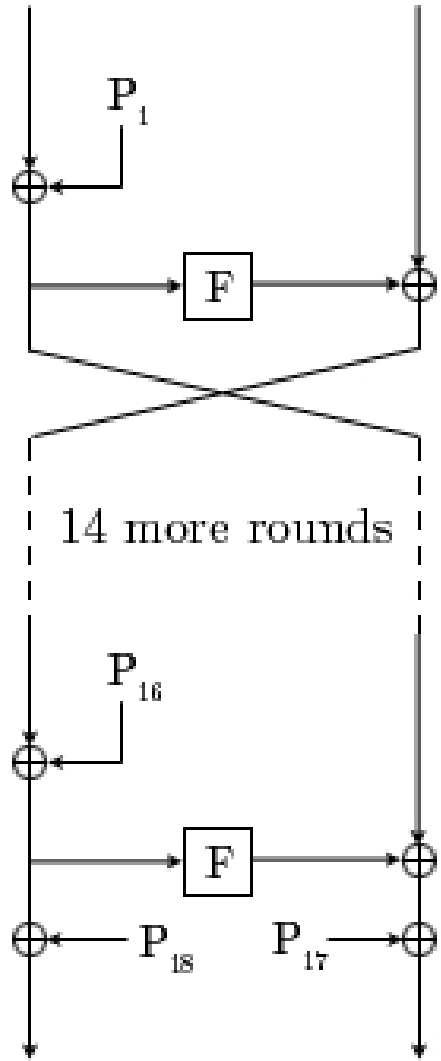
- Bruce Schneier, 1993.
- Velikost klíče: 32-448-bitů v 8-bit krocích (standardně 128-bit klíč).
- Velikost bloku: 64-bitů
- Princip: **Feistel síť**
- Využívá na klíči závislých S-boxů.
- Cyklů: 16
- Efektivní softwareová implementace.
- Navíc dodnes žádná účinná kryptoanalýza nalezena!
- Přesto **AES** standard není ani **Blowfish** ani jeho následovník **Twofish**...

Blowfish

- Bruce Schneier, 1993.
- Velikost klíče: 32-448-bitů v 8-bit krocích (standardně 128-bit klíč).
- Velikost bloku: 64-bitů
- Princip: **Feistel síť**
- Využívá na klíči závislých S-boxů.
- Cyklů: 16
- Efektivní softwareová implementace.
- Navíc dodnes žádná účinná kryptoanalýza nalezena!
- Přesto **AES** standard není ani **Blowfish** ani jeho následovník **Twofish**...
- Vše volně k dispozici (opět žádné patenty).

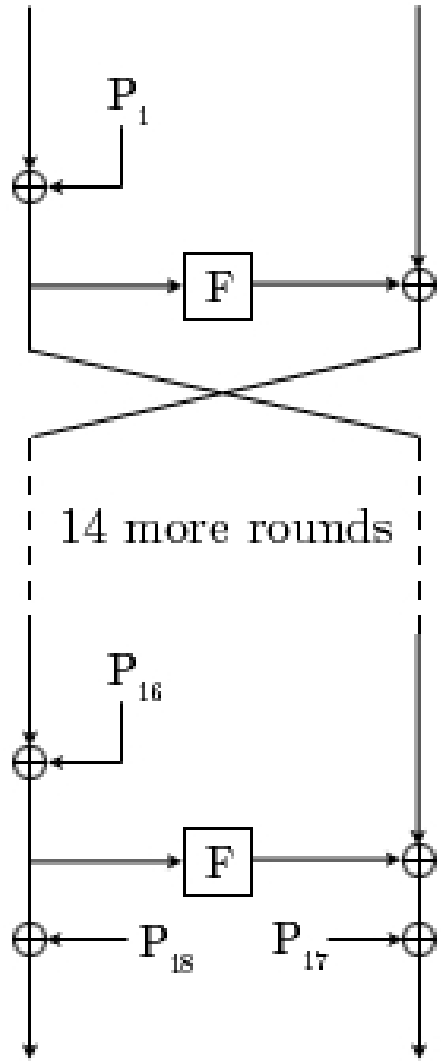
Blowfish - šifrování

- Každá řádka diagramu = 32bitů



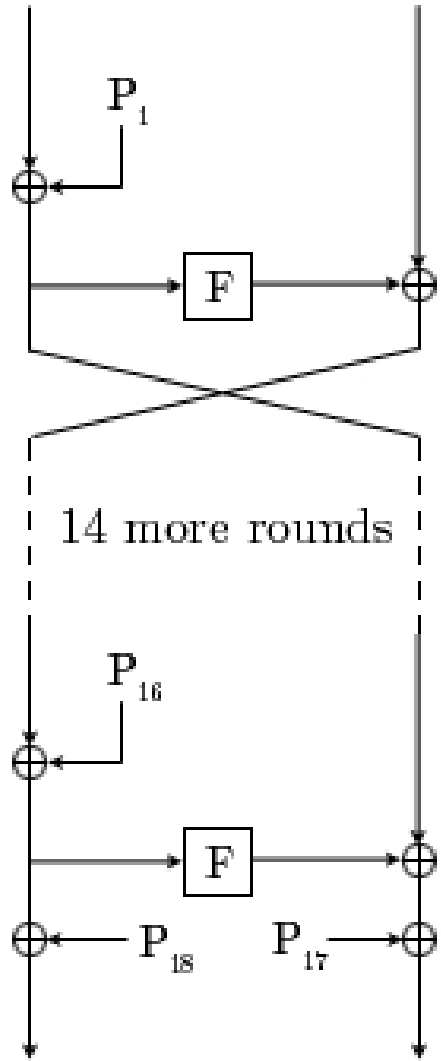
Blowfish - šifrování

- Každá řádka diagramu = 32bitů
- 2 sub-klíčová pole: **P**-array, S-box



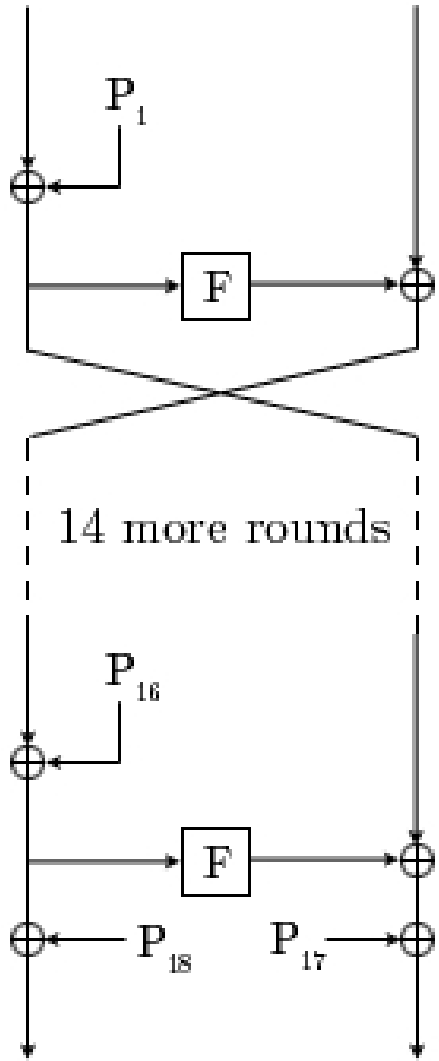
Blowfish - šifrování

- Každá řádka diagramu = 32bitů
- 2 sub-klíčová pole: **P**-array, S-box
- S-box: 8-bit vstup, 32-bit výstup

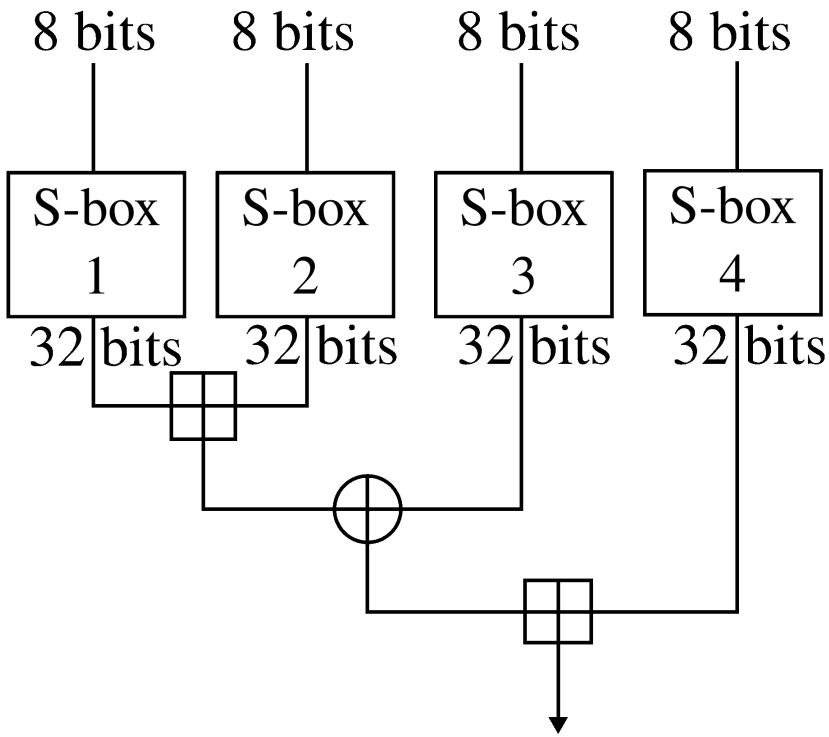


Blowfish - šifrování

- Každá řádka diagramu = 32bitů
- 2 sub-klíčová pole: **P**-array, S-box
- S-box: 8-bit vstup, 32-bit výstup
- **P**-array: 18-ti prvkové pole (jeden vstup použit na začátku, jeden na konci procesu a v každém kroku polovina nepoužitého prvku), prvky XORovány s daty



Blowfish - šifrování



F-funkce rozdělí 32-bit vstup na 4 8-bit části, které slouží jako vstup pro S-boxy, k výstupům je přičteno modulo 2^{32} a jsou XORovány čímž je získán 32-bit výstup.

Twofish

- Finalista **AES**, *3. místo*

Twofish

- Finalista **AES**, *3. místo*
- Bruce Schneier, 1998.

Twofish

- Finalista **AES**, *3. místo*
- Bruce Schneier, 1998.
- Odvozeno z: **Blowfish**, **SAFER**, **Square**

Twofish

- Finalista **AES**, *3. místo*
- Bruce Schneier, 1998.
- Odvozeno z: **Blowfish**, **SAFER**, **Square**
- Velikost klíče: 128, 192, 256-bitů

Twofish

- Finalista **AES**, *3. místo*
- Bruce Schneier, 1998.
- Odvozeno z: **Blowfish**, **SAFER**, **Square**
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloku: 128-bitů

Twofish

- Finalista **AES**, *3. místo*
- Bruce Schneier, 1998.
- Odvozeno z: **Blowfish**, **SAFER**, **Square**
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloku: 128-bitů
- Princip: **Feistel síť** (jako **DES**)

Twofish

- Finalista **AES**, *3. místo*
- Bruce Schneier, 1998.
- Odvozeno z: **Blowfish**, **SAFER**, **Square**
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloku: 128-bitů
- Princip: **Feistel síť** (jako **DES**)
- Cyklů: 16

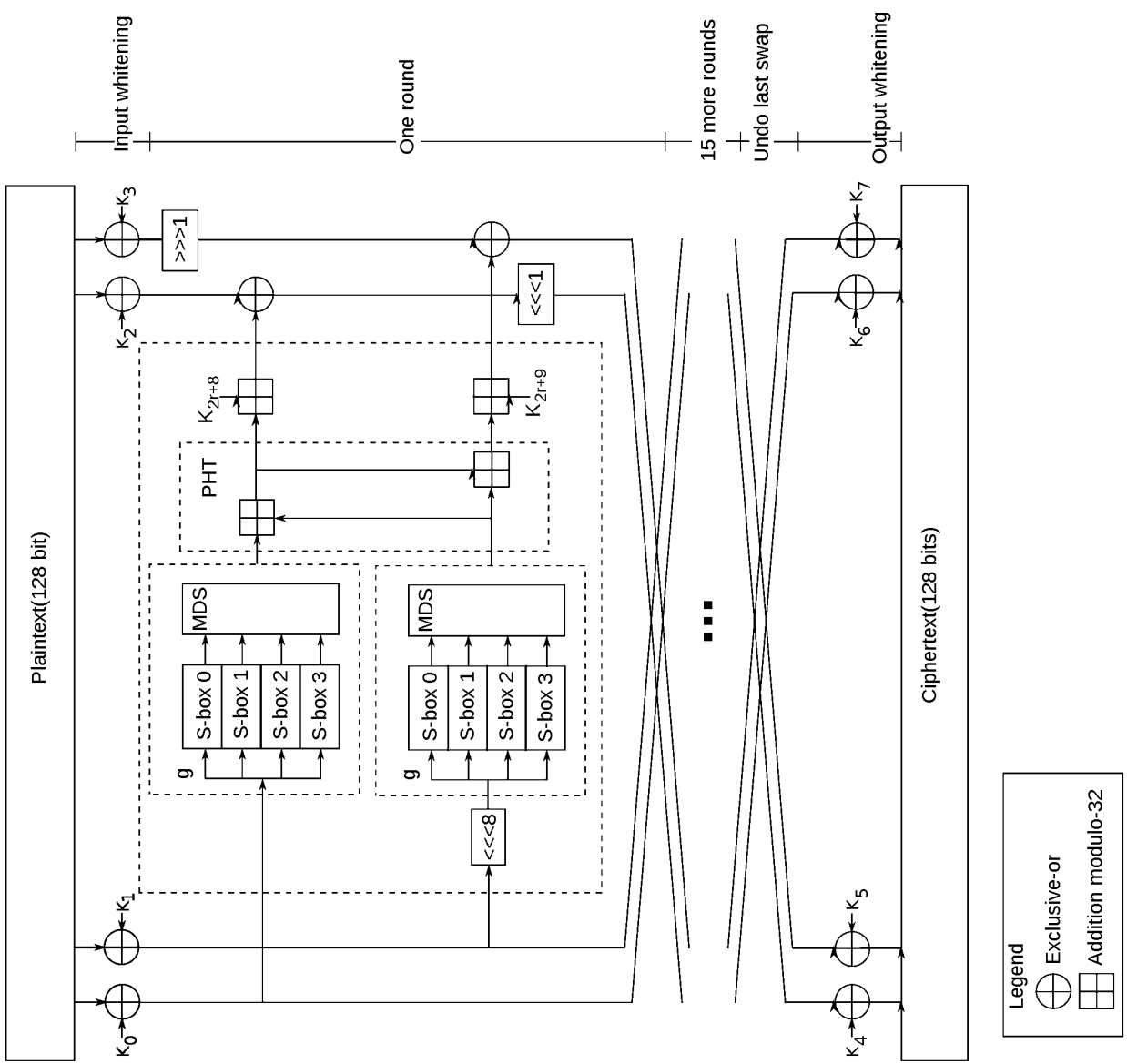
Twofish

- Finalista **AES**, *3. místo*
- Bruce Schneier, 1998.
- Odvozeno z: **Blowfish**, **SAFER**, **Square**
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloku: 128-bitů
- Princip: **Feistel síť** (jako **DES**)
- Cyklů: 16
- Předpočítané (na klíči závislé) S-boxy.

Twofish

- Finalista **AES**, *3. místo*
- Bruce Schneier, 1998.
- Odvozeno z: **Blowfish**, **SAFER**, **Square**
- Velikost klíče: 128, 192, 256-bitů
- Velikost bloku: 128-bitů
- Princip: **Feistel síť** (jako **DES**)
- Cyklů: 16
- Předpočítané (na klíči závislé) S-boxy.
- Polovina klíče slouží opravdu k šifrování, druhá k modifikaci šifrovacího algoritmu (S-boxů).

Twofish


Input whitening
One round
15 more rounds
Undo last swap
Output whitening
Plaintext(128 bit)
Ciphertext(128 bits)
PHT
MDS
S-box 0
S-box 1
S-box 2
S-box 3
g
>>>1
<<<1
<<<8
Legend
Exclusive-or
Addition modulo-32

Twofish

Poznámky ke schématu:

PHT - **P**seudo-**H**adamard transformace (**PHT**) (z šifrovacích algoritmů typu **SAFER**):
reversibilní transformace řetězce bitů (sloužící ke kryptografické difuzi), řetěz musí být sudé délky (je rozdělen na dvě stejně dlouhé části).
Transformace je pak dána:
$a^{'} = a + b(mod 2^n)$
$b^{'} = a + 2b(mod 2^n)$

MDS - Matice A ($m \times n$) je **MDS** (**M**aximum **D**istance **S**eparable) $\iff$ A je transformační maticí linearní transformace $f(x) : K^n \rightarrow K^m$ (K - konečné těleso) $f(x) = Ax$ taková, že:
žádné dvě rozdílné $n + m$-tice $(x, f(x))$ se neliší v n a více prvcích.

Kdo chce znát podrobnosti aneb odkazy

Něco málo zajímavých odkazů k dané problematice:

http://csrc.nist.gov/archive/aes/
http://gilchrist.ca/jeff/distrib-des2-2.html
http://www.cl.cam.ac.uk/ rja14/serpent.html
http://www.copacobana.org/
http://www.cryptography.com
http://www.cryptosystem.net/aes/
http://www.eff.org
http://www.interhack.net/projects/deschall/
http://www.quadibloc.com/crypto/co4514.htm
http://www.samiam.org/key-schedule.html
http://www.schneier.com/blowfish-products.html
http://www.schneier.com/twofish.html
http://www.usdsi.com/aes.html