Pseudorandom Permutations and Block Ciphers

Cryptography and Protocols

Andrei Bulatov

Pseudorandom Permutations

- A pseudorandom function $F = \{ f_s \}_{s \in \{0,1\}^*}$ is called a pseudorandom permutation if $f_s : \{0,1\}^m \to \{0,1\}^m$ is one-to-one for all s.

- The only exception is that when considering security we use random permutations rather than random functions

- An encryption scheme based on a PRP is called a block cipher

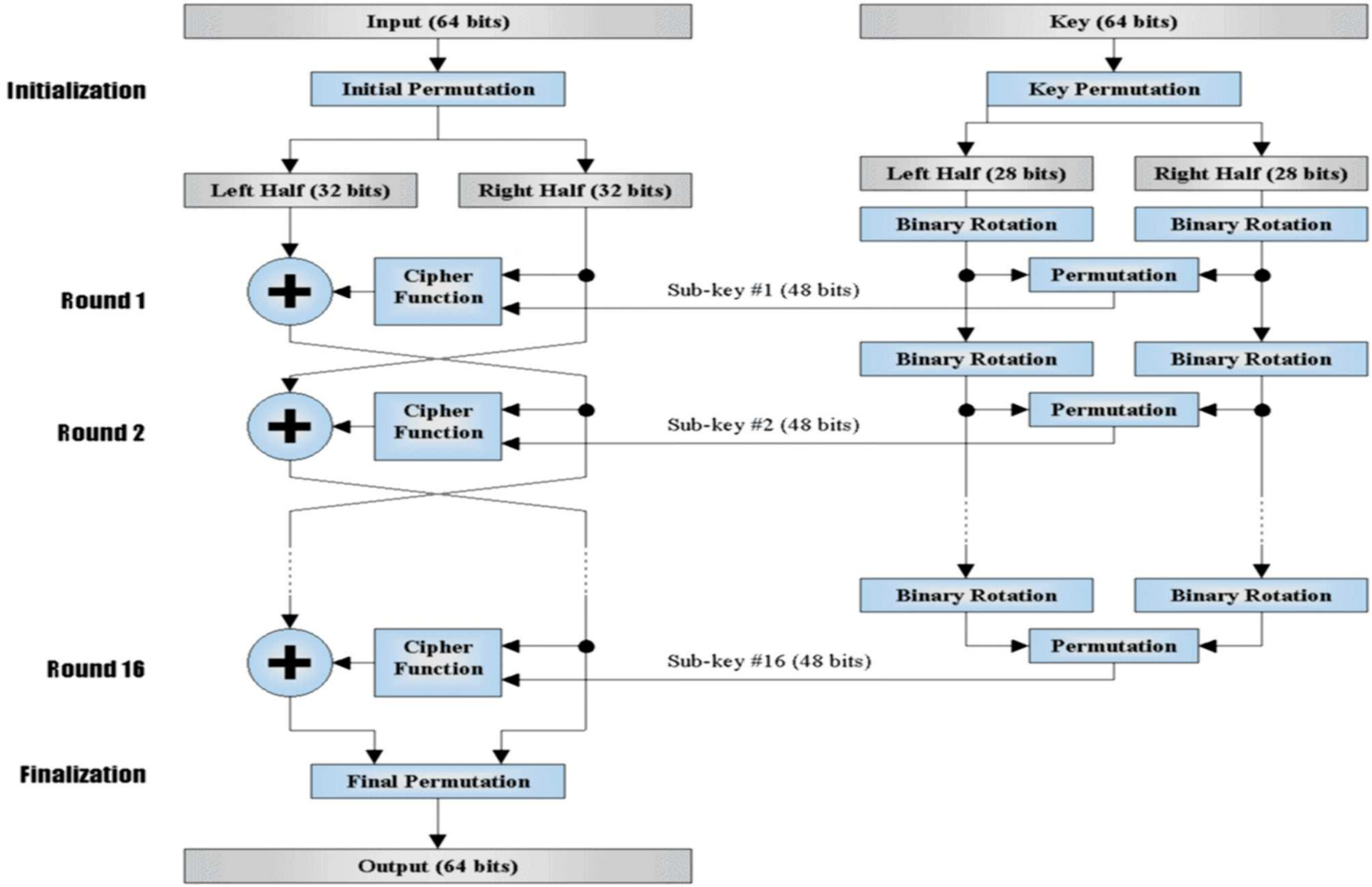
DES

- DES – Data Encryption Standard

- 1972 NIST (then NBS) called for encryption standards proposals
- 1974 IBM responded with Lucifer
- NSA tweaked Lucifer to get DES
- key size |s| = 56, block size 64 bit

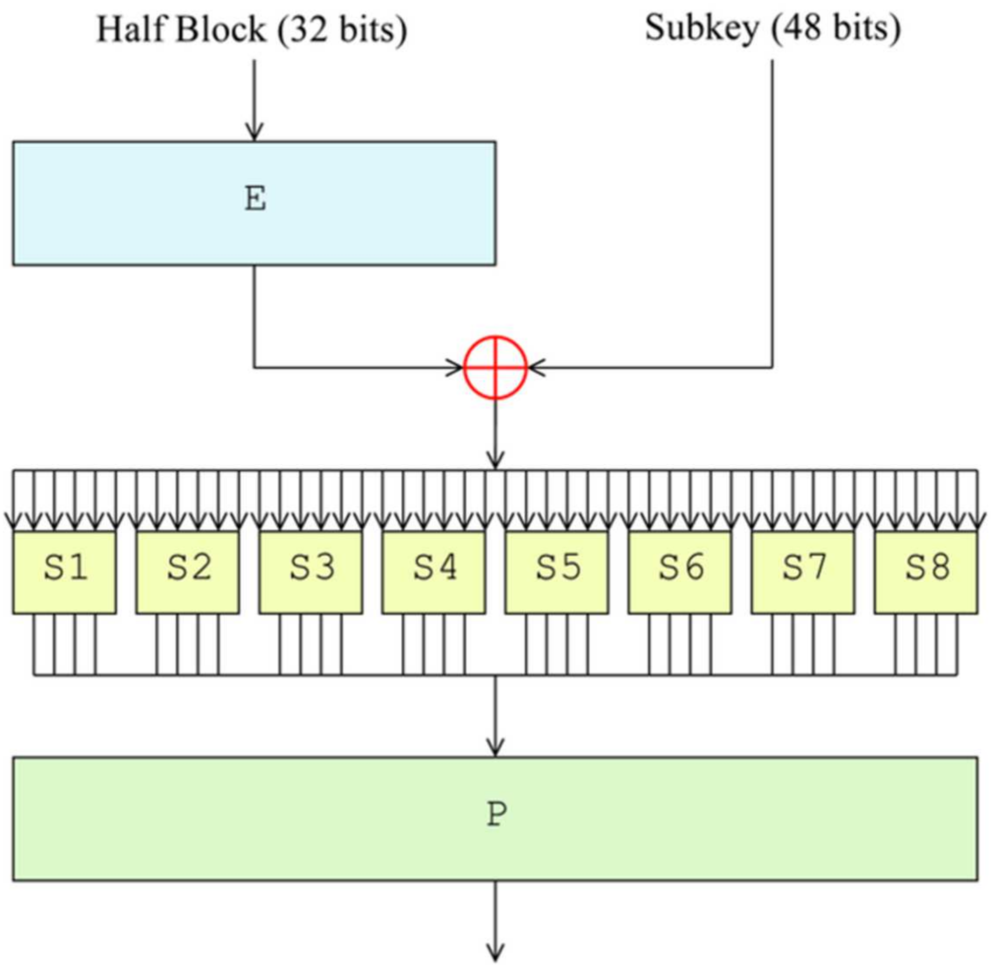
- 1970's Diffie & Hellman suggested a $20 million machine to find a key within a day
- 1990's Wiener suggests a $1 million to find a key in 3.5 hours
- 1997 over the Internet ~ $50K machines found a key in 90 days
- 1998 $210K machine Deep Crack finds a key in 56 hours

DES (cntd)


Input (64 bits)
Key (64 bits)
Initialization
Initial Permutation
Key Permutation
Left Half (32 bits)
Right Half (32 bits)
Left Half (28 bits)
Right Half (28 bits)
Binary Rotation
Binary Rotation
Round 1
Cipher Function
Permutation
Sub-key #1 (48 bits)
Binary Rotation
Binary Rotation
Round 2
Cipher Function
Permutation
Sub-key #2 (48 bits)
Binary Rotation
Binary Rotation
Round 16
Cipher Function
Permutation
Sub-key #16 (48 bits)
Finalization
Final Permutation
Output (64 bits)

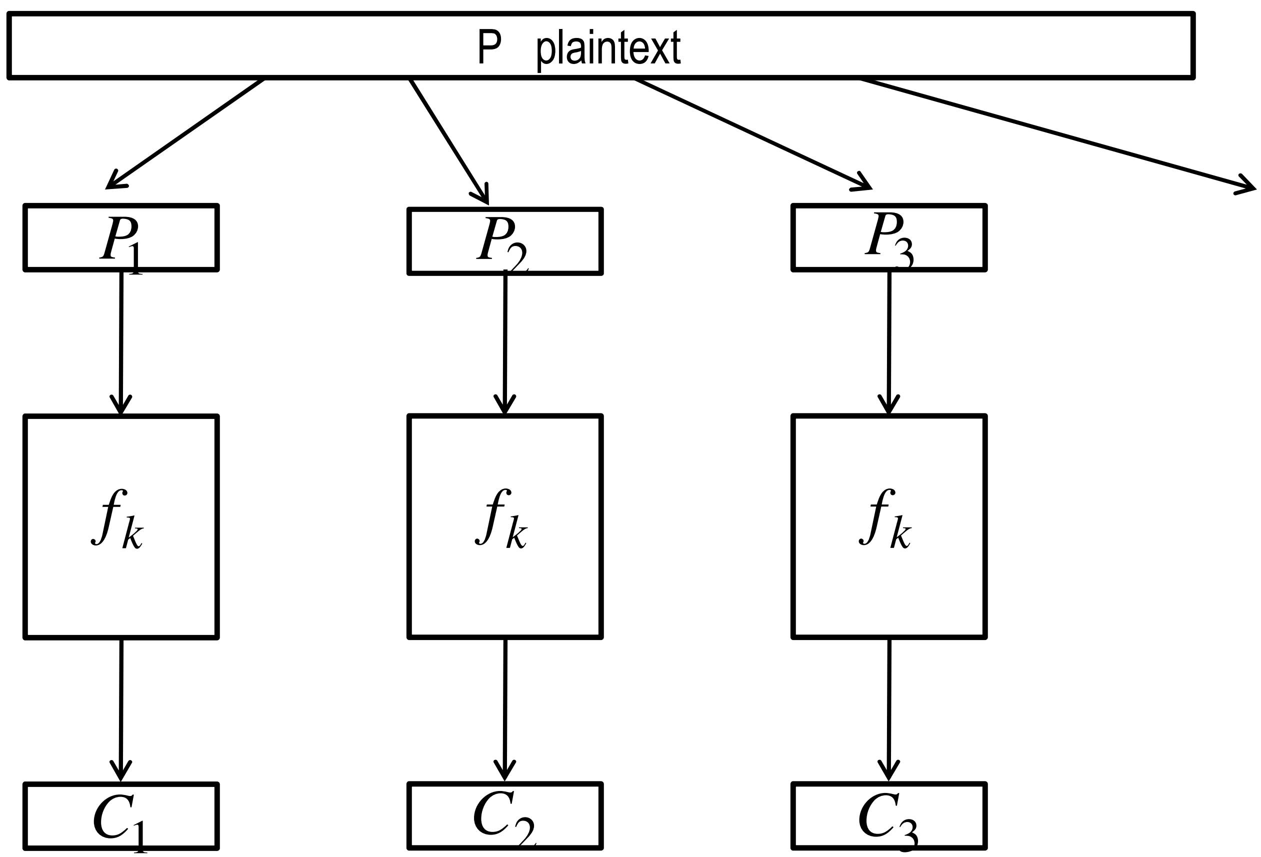
More on DES

- Cipher function and S-Boxes



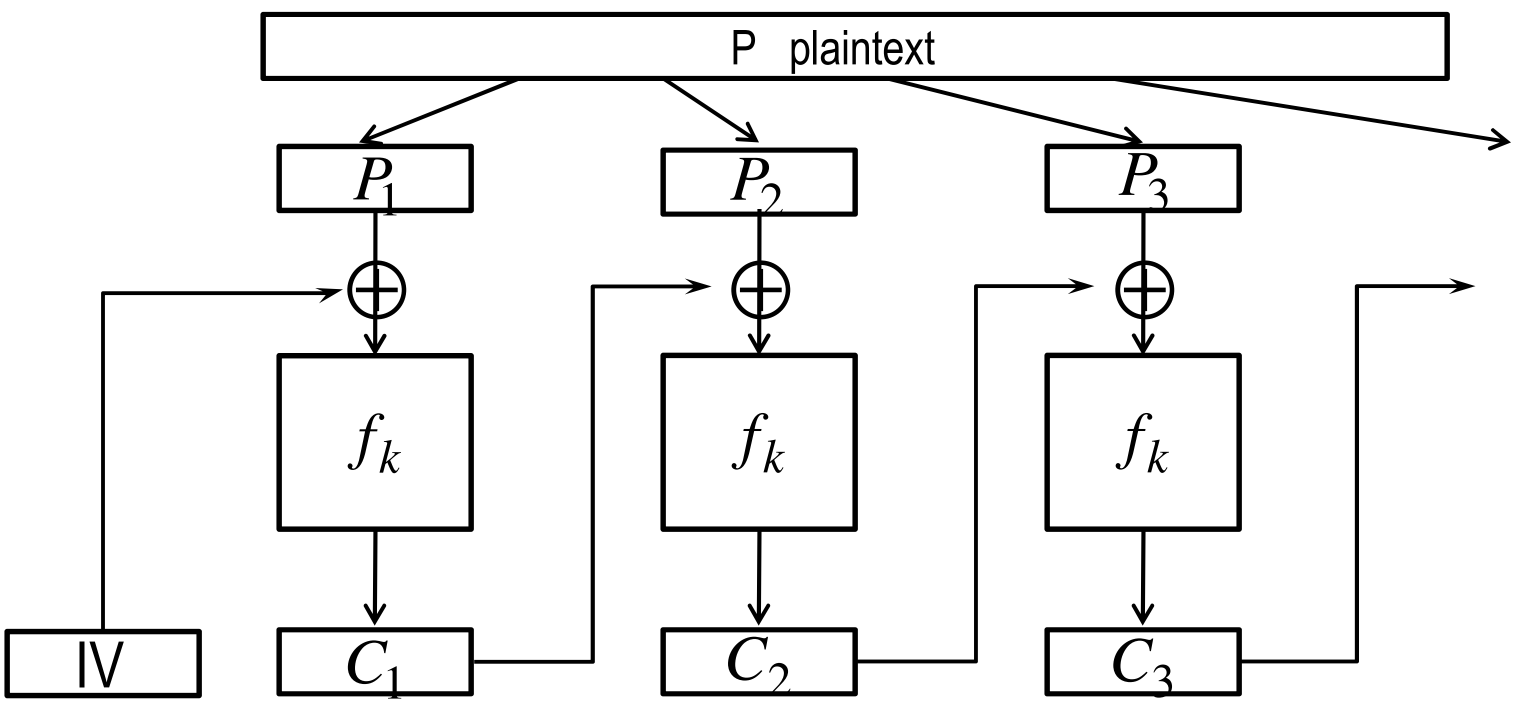
Modes of Block Ciphers – ECB

- ECB stands for Electronic CodeBook



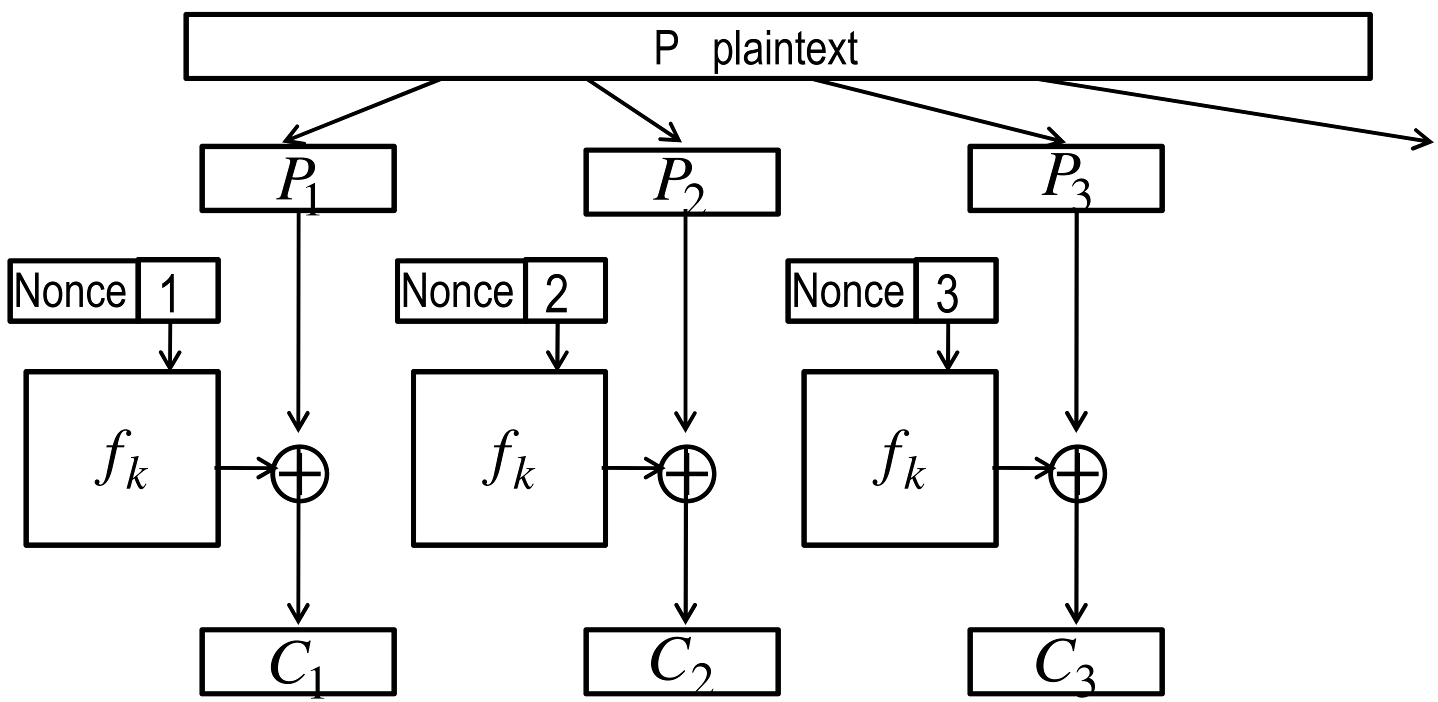
Modes of Block Ciphers – CBC

- CBC means Cipher Block Chaining
- Use IV (fixed, counter, random,…)
- Set $C_0 = \text{IV}, \quad C_1 = f_k(P_1 \oplus C_1), \quad C_2 = f_k(P_2 \oplus C_2), \ldots$



Modes of Block Ciphers – CTR

- CBC means CounTeR mode
- Convert a block cipher into a PRG and then use it for a stream cipher
- Set $C_1 = P_1 \oplus f_k(1), \quad C_2 = P_2 \oplus f_k(2), \ldots$



Modes of Block Ciphers – Security

- **Theorem**

  In the CBC mode, if IV is chosen at random, then the encryption scheme is CPA-secure

- **Theorem**

  In the CTR mode if Nonce is empty then the encryption scheme is CPA secure.

- **Idea of a Proof**

  If $\{f_s\}_{s\in\{0,1\}^*}$ is a pseudorandom function then for any k $g(k) = f_k(0)f_k(1)f_k(2)\ldots$ is a pseudorandom generator

More Block Ciphers

- Triple DES

  $$\mathrm{3DES2}(k_1, k_2, P) = \mathrm{DES}(k_2, \mathrm{DES}^{-1}(k_1, \mathrm{DES}(k_2, P)))$$
  $$\mathrm{3DES3}(k_1, k_2, k_3, P) = \mathrm{DES}(k_3, \mathrm{DES}^{-1}(k_2, \mathrm{DES}(k_1, P)))$$

- Skipjack and the Clipper chip

  - 1993 US govt suggests to give industry a chip (called Clipper) containing NSA developed cipher Skipjack
  - Clipper uses 3 keys

    family key hardwared and shared among all chips, secret

    unit key, one per chip, split among two federal agencies

    session key, chosen by user
  - Was not very popular, declassified in 1998
  - Biham, Biryukov, Shamir found a weakness in 1999

AES

- AES – Advanced Encryption Standard
- 1997 NIST called for replacement of DES
- Goals:

  use for ≥30 years, protect info for 100 years

  strong at least as 3DES, significantly more efficient
- Open competition
- Winner: Rijndael (Daeman, Rijmen from Belgium)
- Block length 128 bit, key length 128, 192, or 256 bit
- Efficiency:
  - hardware up to ~50 Gbit/sec
  - software 251 cycles/block (2 cycles/bit)

    ~ 1 Gbit/sec on 2Ghz processor

AES

- Block: 128bits = 16 bytes (4x4 square)
- function AES$_k(P)$

  $(k_0, \dots, k_{10})$:= expand (k)

  $s := P \oplus k_0$

  for r = 1 to 10 do

  s := S(s)

  s := shift_rows(s)

  if r ≤ 9 then s := mix_cols(s)

  $s := s \oplus k_r$

  endfor

  return s

AES: Key Expansion

- function expand (k)

  $k_0 := k$ /* split the key into four 4-byte parts $k_0[0], \ldots, k_0[3]$

  for i = 1 to 10 do

  $k_i[0] := k_{i-1}[0] \oplus S(k_{i-1}[3]$ left shifted by 8 bits$) \oplus C_i$

  $k_i[1] := k_{i-1}[1] \oplus k_i[0]$

  $k_i[2] := k_{i-1}[2] \oplus k_i[1]$

  $k_i[3] := k_{i-1}[3] \oplus k_i[2]$

  endfor

  return $(k_0, \ldots, k_{10})$

Coefficients C_i are carefully chosen

AES: S-boxes

- Function S acts byte-wise; it is a permutation on bytes

  S: {0, …, 255} $\rightarrow$ {0, …, 255}
- Implementation: table look-up
- Byte can be represented as a polynomial

  $$pol(a) = pol(a_0 a_1 \ldots a_7) = a_7 x^7 + \cdots + a_1 x + a_0$$
- Define multiplication

  $$a \cdot b = \mathrm{pol}(a) \cdot \mathrm{pol}(b) (\mathrm{mod}\, x^8 + x^4 + x^3 + x + 1)$$

  this is a byte again
- For each a $\neq$ 0 there is a^{-1} such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$
- Then $S(a) = a^{-1}$ and S(0) = 0

AES: Shft_Rows

- Arrange 16 bytes of the block into a matrix

$$\begin{pmatrix} s_1 & s_5 & s_9 & s_{13} \\ s_2 & s_6 & s_{10} & s_{14} \\ s_3 & s_7 & s_{11} & s_{15} \\ s_4 & s_8 & s_{12} & s_{16} \end{pmatrix}$$

- Shift_row:

$$\begin{pmatrix} s_1 & s_5 & s_9 & s_{13} \\ s_2 & s_6 & s_{10} & s_{14} \\ s_3 & s_7 & s_{11} & s_{15} \\ s_4 & s_8 & s_{12} & s_{16} \end{pmatrix} \longrightarrow \begin{pmatrix} s_1 & s_5 & s_9 & s_{13} \\ s_6 & s_{10} & s_{11} & s_2 \\ s_{11} & s_{15} & s_3 & s_7 \\ s_{16} & s_4 & s_8 & s_{12} \end{pmatrix}$$

- Mix_cols

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 02 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} s_1 & s_5 & s_9 & s_{13} \\ s_2 & s_6 & s_{10} & s_{14} \\ s_3 & s_7 & s_{11} & s_{15} \\ s_4 & s_8 & s_{12} & s_{16} \end{pmatrix}$$