Block Ciphers

AK Bhateja

Block Cipher

- A block cipher is an encryption scheme which breaks up the plaintext messages to be transmitted into strings (called blocks) of a fixed length t over an alphabet A, and encrypts one block at a time. e.g. DES, 3-DES, AES, IDEA, and Blowfish
- Two important classes of block ciphers are substitution ciphers and transposition ciphers
- Substitution Cipher
  - Simple substitution
  - Polyalphabetic Cipher
- Transposition Cipher: permutes the symbols in a block
  - Simple transposition cipher
  - Double transposition cipher

Transposition cipher

- Simple transposition cipher

  Example: Consider $e = (6\ 4\ 1\ 3\ 5\ 2)$, period $t = 6$.

  The message m = CAESAR is encrypted to c = RSCEAA.

  Decryption uses the inverse permutation $d = (3\ 6\ 4\ 2\ 5\ 1)$.

- Double transposition cipher

  Example: Plaintext: attack at four

  Let the two transformations be

  First: permute rows from (1, 2, 3) to (3, 2, 1)

  second: permute columns from (1, 2, 3, 4) to (4, 2, 1, 3)

$$\begin{matrix} a & t & t & a \\ c & k & a & t \\ f & o & u & r \end{matrix} \Rightarrow \begin{matrix} f & o & u & r \\ c & k & a & t \\ a & t & t & a \end{matrix} \Rightarrow \begin{matrix} r & o & f & u \\ t & k & c & a \\ a & t & a & t \end{matrix}$$

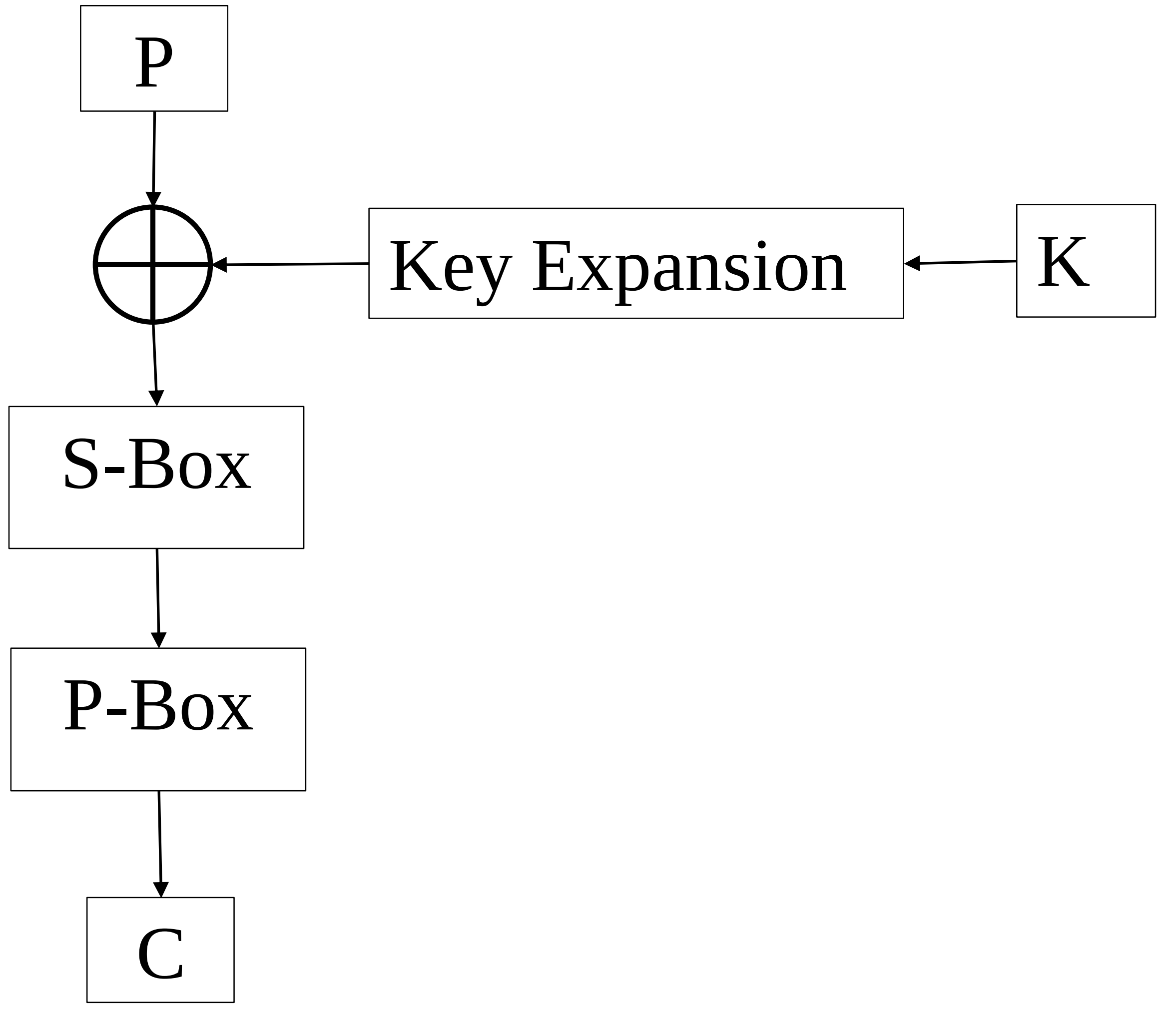
Ciphertext: rofutkcaatat

Product Cipher

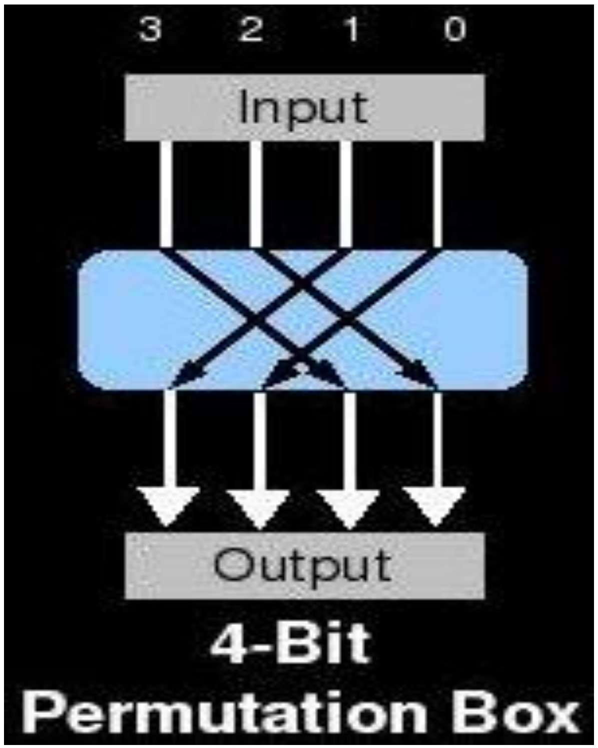
- Shannon introduced the idea of product ciphers (multiple encryption)
- Definition: A product cipher combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual components.

  i.e. The product of two ciphers is the result of applying one cipher followed by the other.
- This is composition of two ciphers or superencipherment
- A product cipher that uses only substitutions and permutations is called a SP-network.

Substitution-Permutation Networks (SPN)



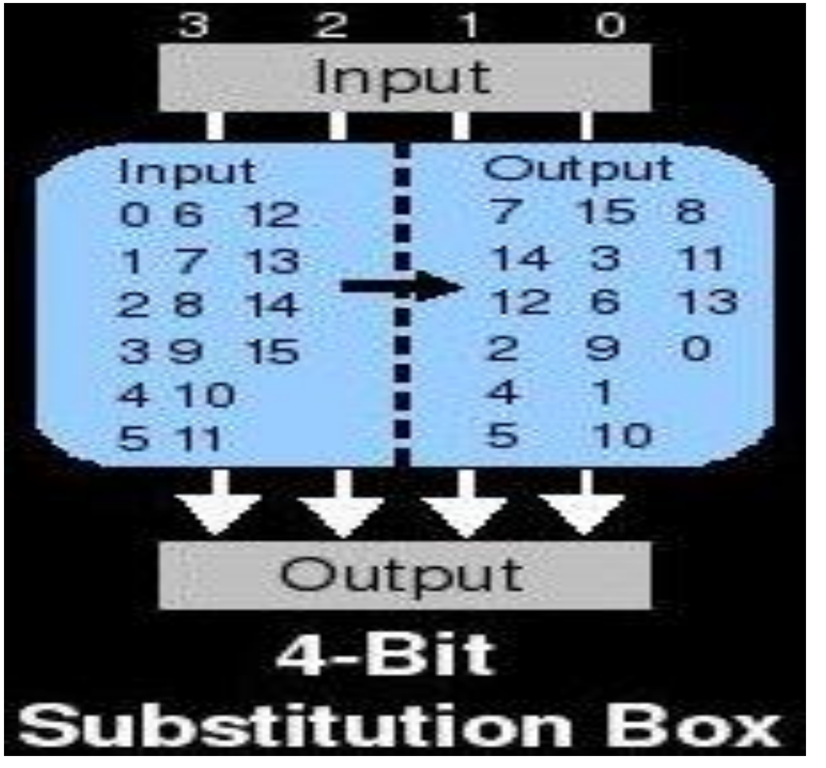
Permutation Boxes



- It is an element of ciphers that adds Diffusion to the algorithm.
- The objective of diffusion is to spread information around in the ciphertext.
- A group of techniques called frequency analysis take advantage of patterns in the input data, to help deduce the plaintext.
- Ciphers using only substitution are vulnerable to these attacks.

Substitution Boxes

- S-boxes add confusion to ciphers that employ them.
- Confusion is intended to make the relationship between the key and ciphertext as complex as possible.

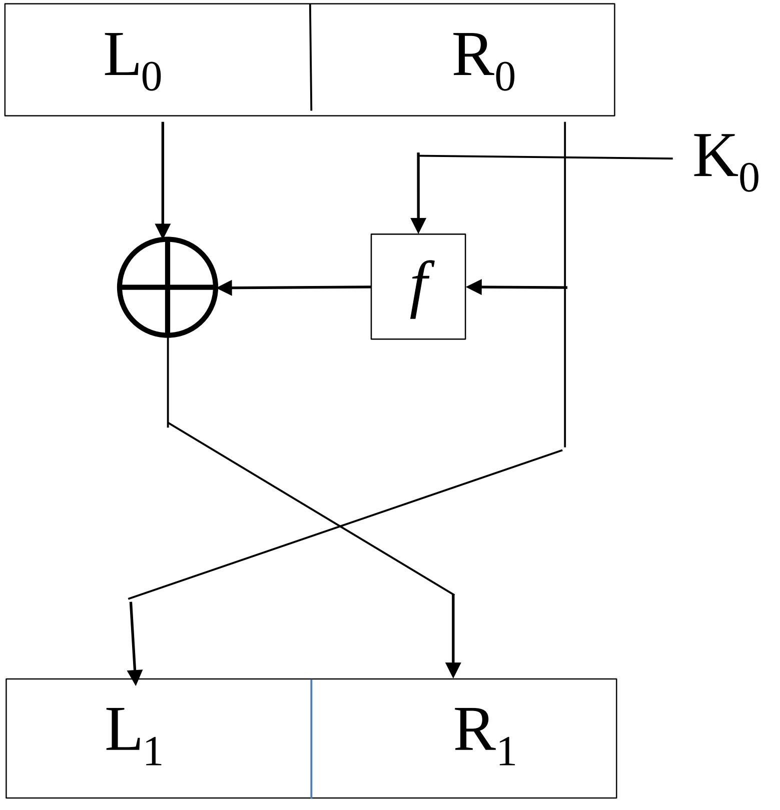


Feistel Cipher

- A Feistel cipher is an iterated cipher mapping a $2t$-bit plaintext (L_0, R_0), for t-bit blocks L_0 and R_0, to a ciphertext (R_r, L_r), through an r-round process where $r \geq 1$.
- For $1 \leq i \leq r$, round i maps $(L_{i-1}, R_{i-1}) \xrightarrow{K_i} (L_i, R_i)$ as follows:

  $L_i = R_{i-1}$, $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$,
  where each subkey K_i is derived from the cipher key K.

One round of a Feistel Cipher

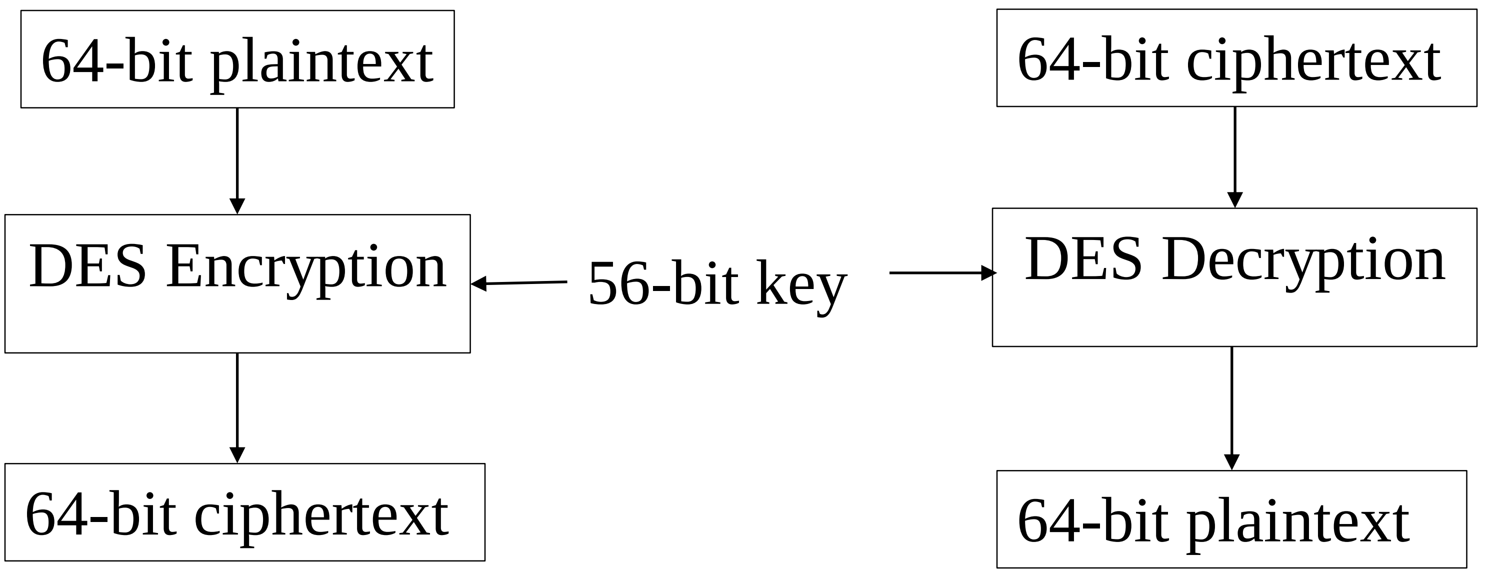


Data Encryption Standard (DES)

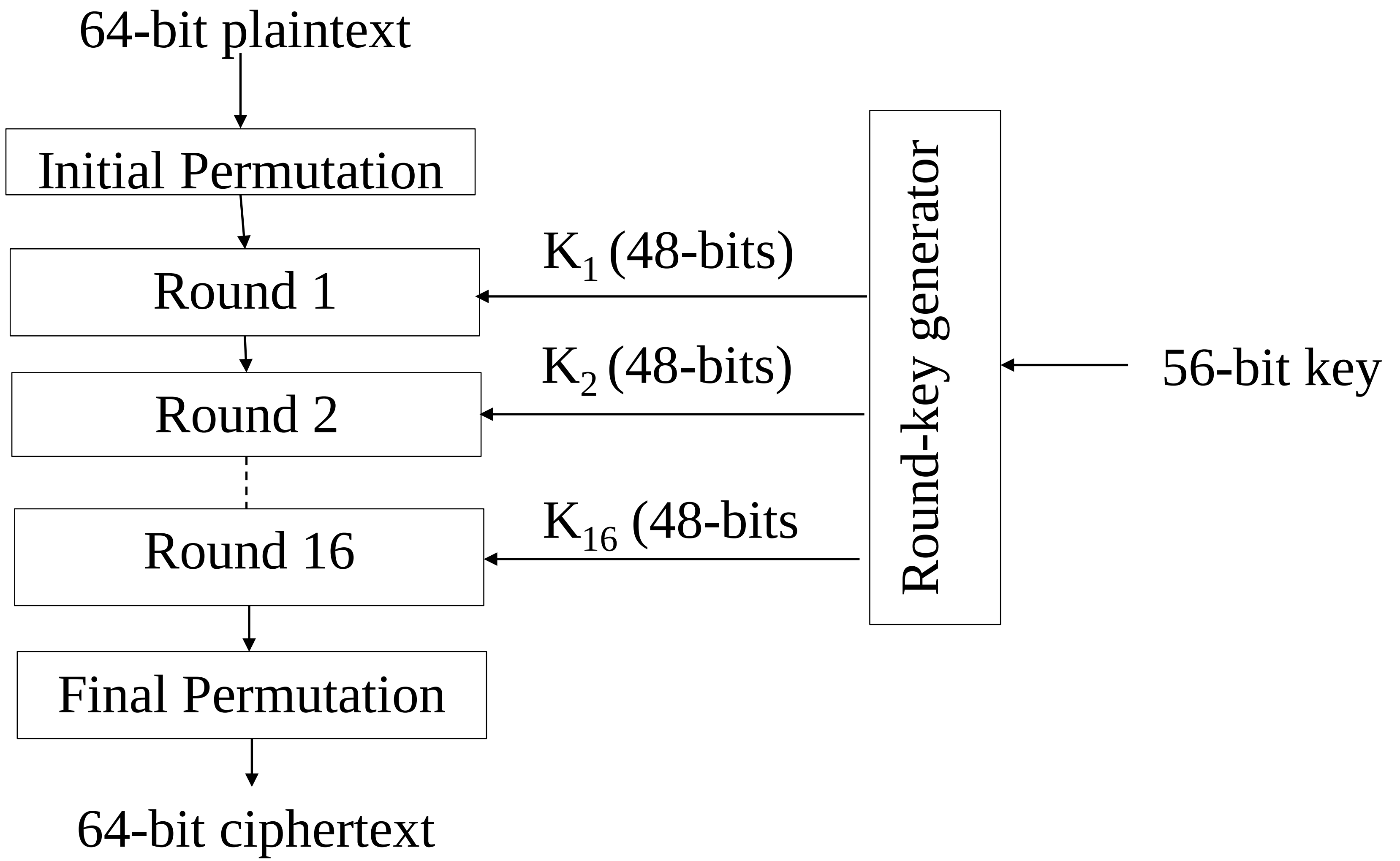
- It uses a Feistel structure.
- DES is probably the most studied algorithm in history and much research, and therefore ciphers, is based on it.
- It is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).
- It is the first commercial-grade modern algorithm with openly and fully specified implementation details.

Data Encryption Standard

- DES processes plaintext blocks of n = 64 bits, producing 64-bit ciphertext blocks.
- The effective size of the secret key K is 56 bits.
- The input key K is specified as a 64-bit key, 8 bits of which (bits 8, 16,. . . , 64) may be used as parity bits.



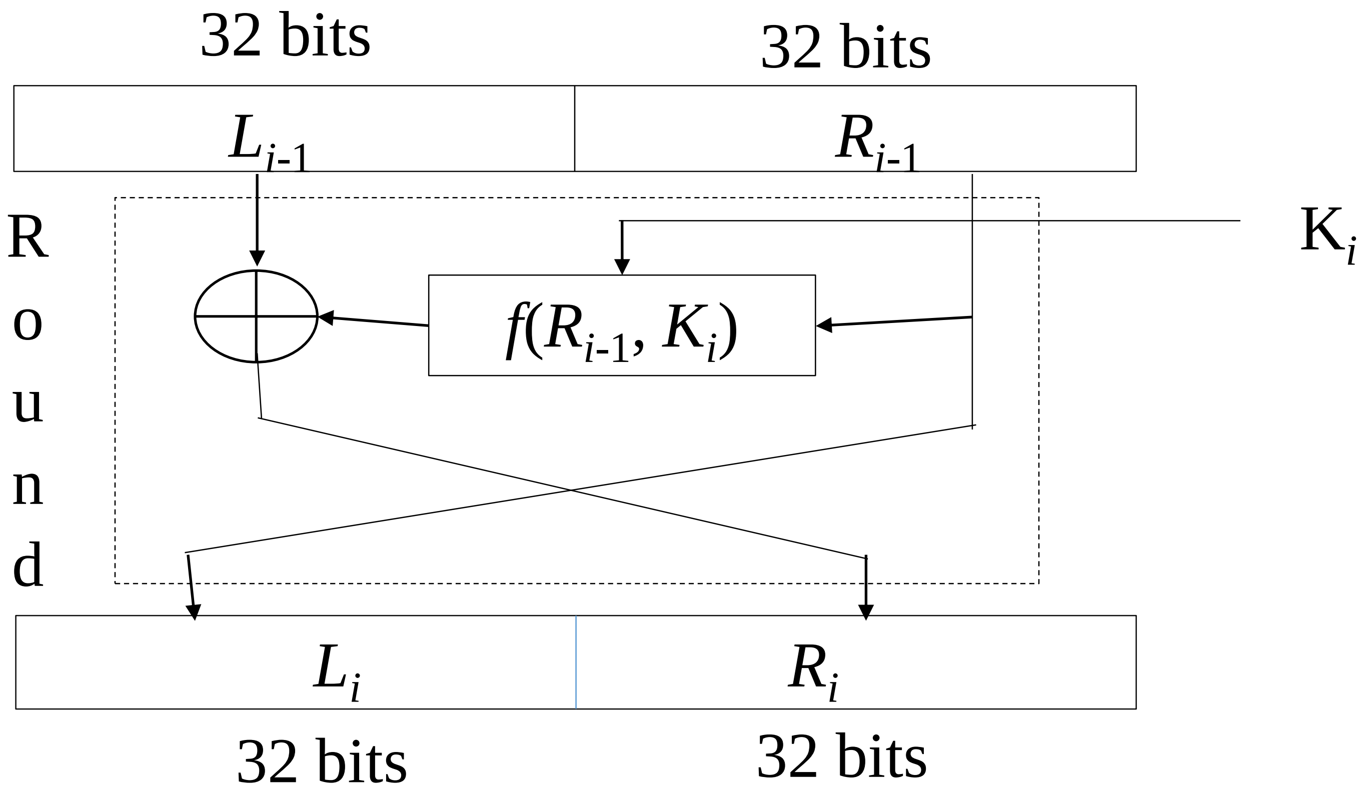
DES Encryption



Initial and final permutation tables

Initial Permutation	Final (Inverse) Permutation
58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25

DES Rounds



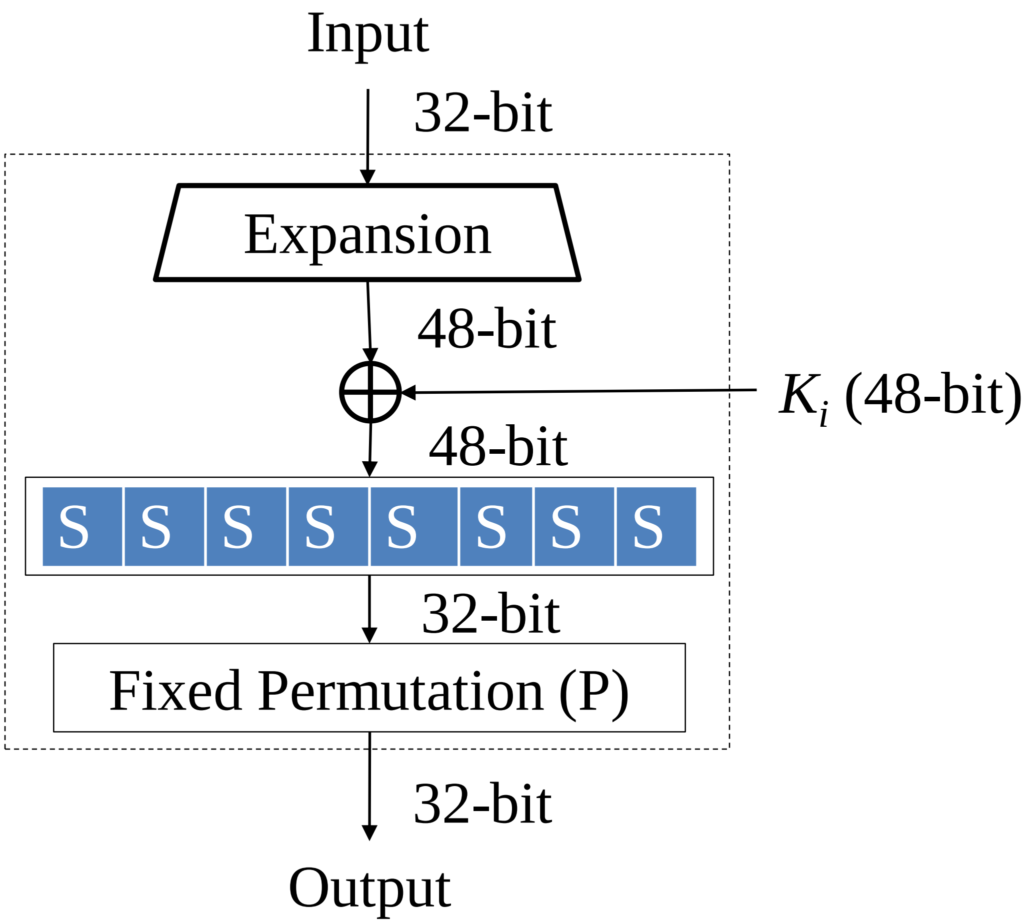
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$,

f-function (DES function)

$f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$

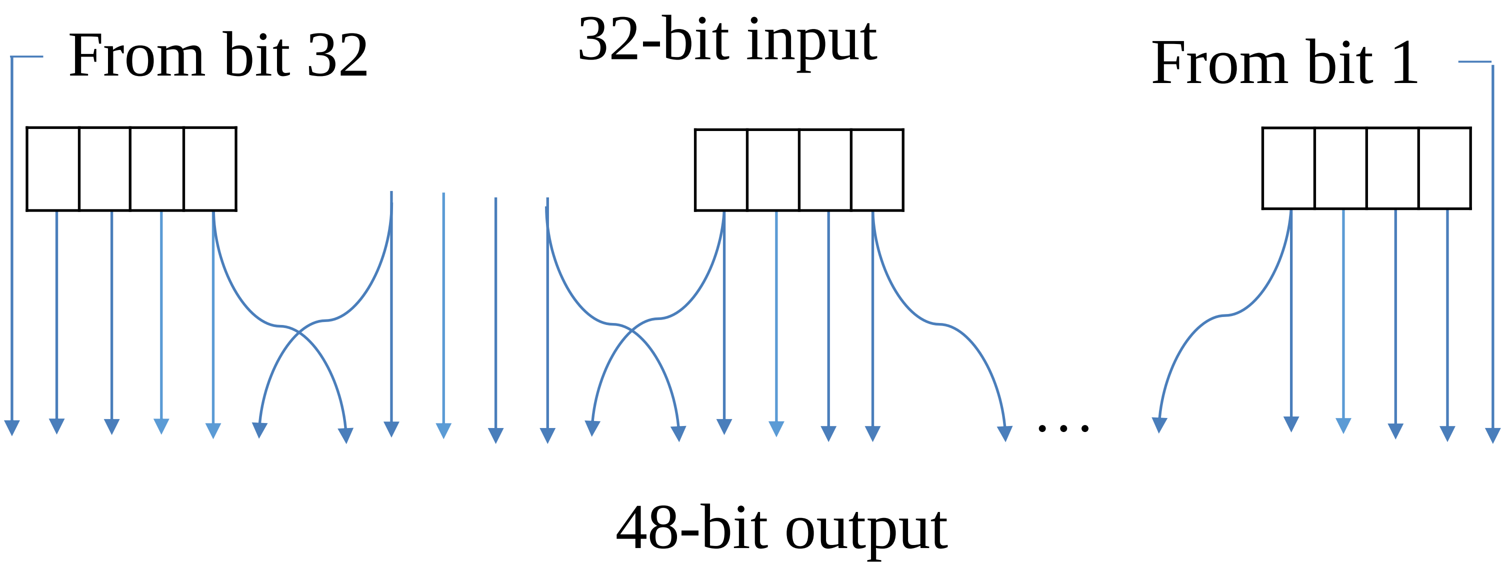
Here

- E is a fixed expansion permutation mapping R_{i-1} from 32 to 48 bits.
- P is another fixed permutation on 32 bits.
- Within each round, 8 fixed, carefully selected 6-to-4 bit substitution mappings (S-boxes) S_i, collectively denoted S, are used.



Expansion permutation mapping (E)

- A fixed expansion permutation mapping E, which maps $R_{i\text{-}1}$ from 32 to 48 bits (all bits are used once; some are used twice).



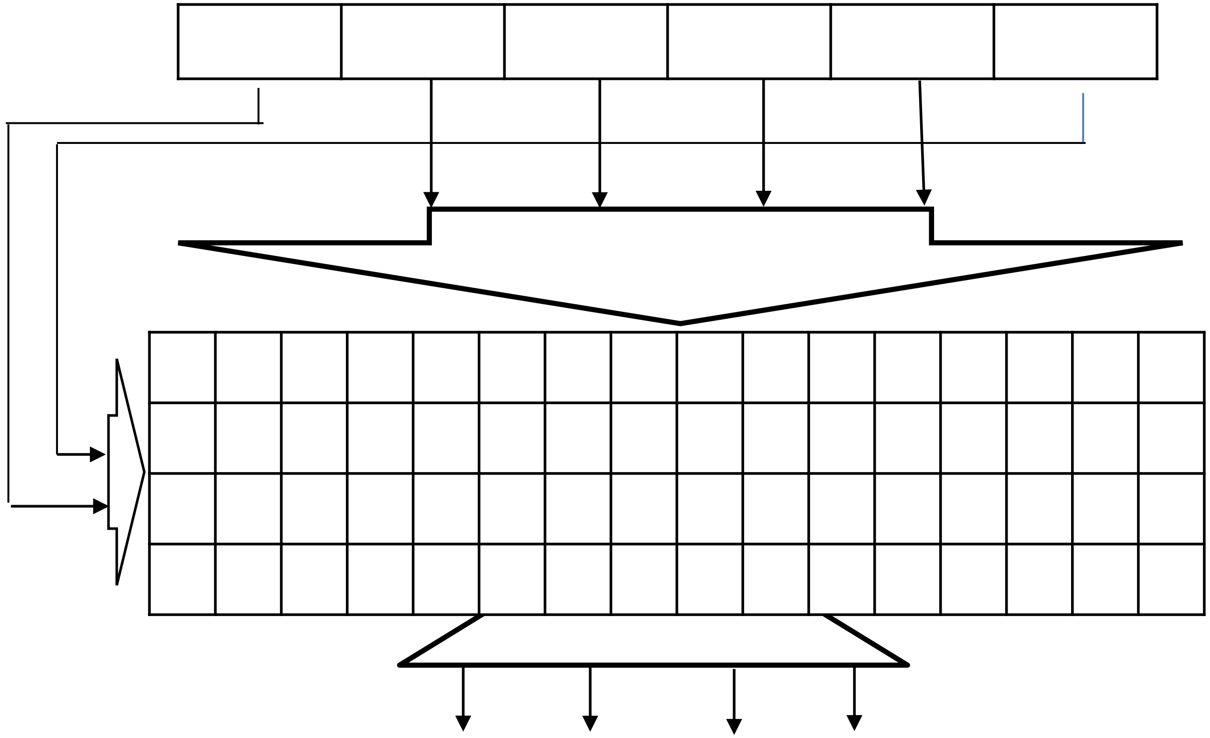
S-box in DES

- An S-box is a substitution box and it is the only non-linear component in the cipher.
- Its main purpose is to obscure the relationship between the key, the plaintext, and the ciphertext.
- DES consists of 8 different parallel S-boxes. Every S-box transforms 6 bits of input to an output of 4 bits:

$$S : \{0,1\}^6 \to \{0,1\}^4 \quad : x \to S(x)$$

- The 8 Standard DES S-boxes of IBM were published together with the algorithm in 1977, but the criteria were only disclosed 17 years after.

S-Boxes



- The combination of bits 1 and 6 of the input defines one of four rows.
- The combination of bits 2 through 5 defines one of the sixteen columns.

The S-box Design Criteria

- Each S-box has six bits of input and four bits of output.
- No output bit of an S-box should be too close to a linear function of the input bits.
- If we fix the leftmost and rightmost input bits of the S-box and vary the four middle bits, each possible 4-bit output is attained exactly once as the middle four input bits range over their 16 possibilities
- If two inputs to an S-box differ in exactly one bit, the outputs must differ in at least two bits. (i.e. if $h(\Delta I_{i,j}) = 1$, then $h(\Delta O_{i,j}) \geq 2$, where $h(x)$ is the Hamming weight of x.)

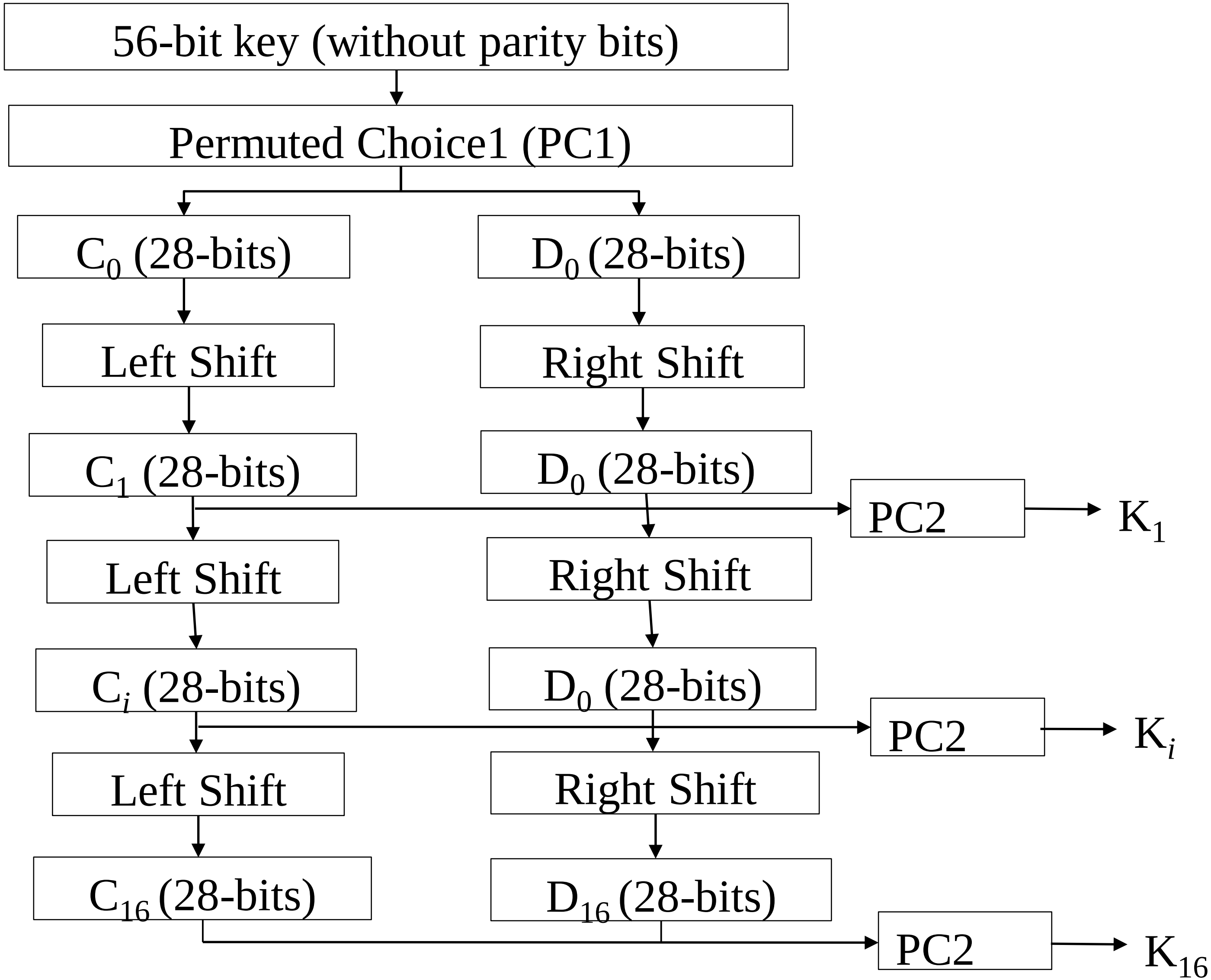
The S-box Design Criteria

- If two inputs to an S-box differ in the two middle bits exactly, the outputs must differ in at least two bits. (If $\Delta I_{i,j} = 001100$, then $h(\Delta O_{i,j}) \geq 2$.)
- If two inputs to an S-box differ in their first two bits and are identical in their last two bits, the two outputs must not be the same. (If $\Delta I_{i,j} = 11xy00$, where x and y are arbitrary bits, then $\Delta O_{i,j} \neq 0$.)
- For any nonzero 6-bit difference between inputs, $\Delta I_{i,j}$, no more than eight of the 32 pairs of inputs exhibiting $\Delta I_{i,j}$ may result in the same output difference $\Delta O_{i,j}$.

Fixed permutation (P) table

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

DES Key Generation ($K_1 – K_{16}$)



Permuted Choices & Left Shifts

PC1						
Left						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
Right						
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

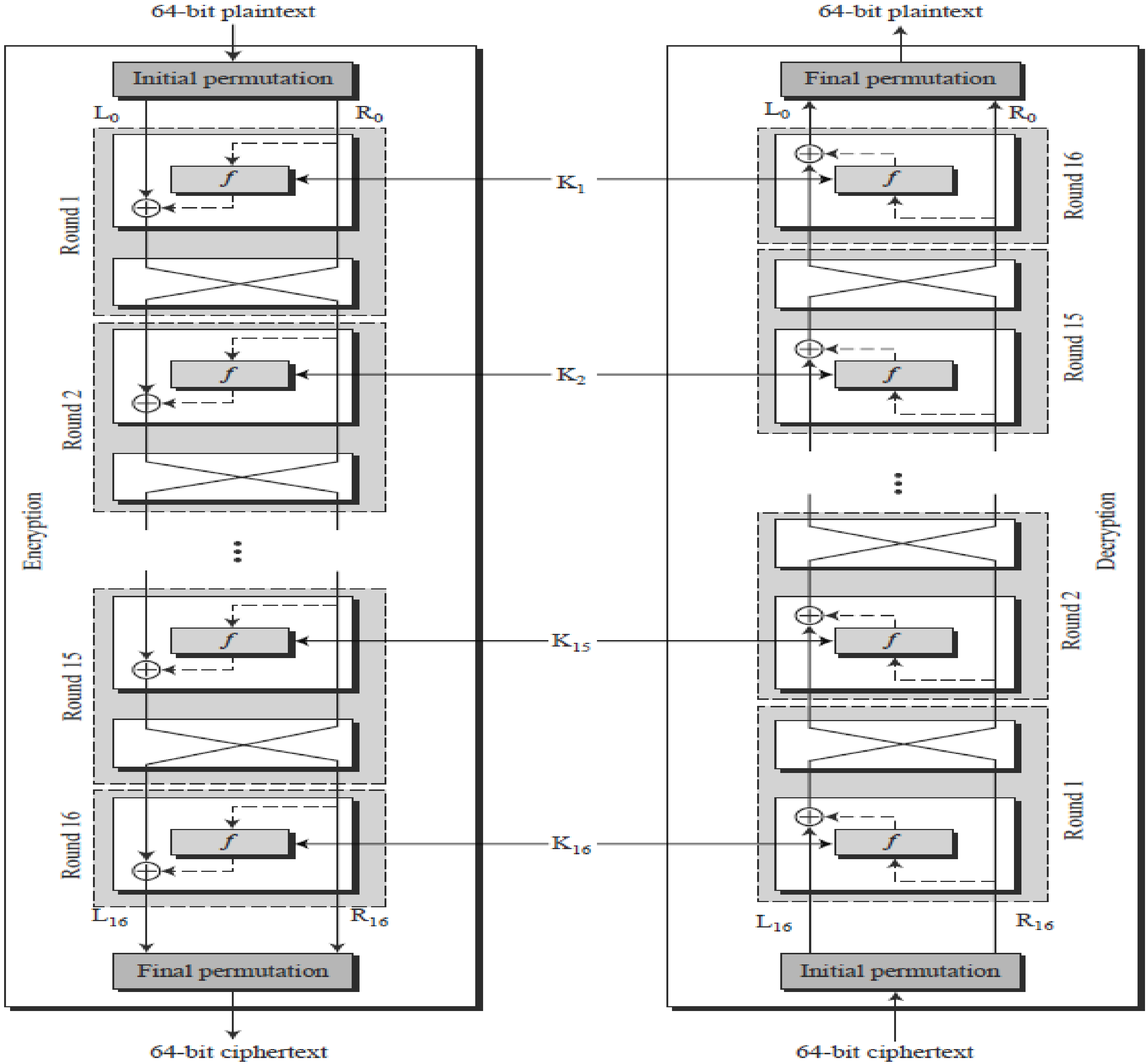
PC2							
14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Left shifts (number of bits to rotate) - r_1, r_2, ..., r_{16}

r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8	r_9	r_{10}	r_{11}	r_{12}	r_{13}	r_{13}	r_{15}	r_{16}
1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

DES Decryption

- DES decryption consists of the encryption algorithm with the same key but reversed key schedule, using in order $K_{16}, K_{15}, \ldots, K_1$.
- The effect of IP^{-1} is cancelled by IP in decryption, leaving (R_{16}, L_{16}); Consider applying round 1 to this input.
- The operation on the left half yields, rather than $L_0 \oplus f(R_0, K_1)$, now $R_{16} \oplus f(L_{16}, K_{16})$, which, since $L_{16} = R_{15}$ and $R_{16} = L_{15} \oplus f(R_{15}, K_{16})$, is equal to $L_{15} \oplus f(R_{15}, K_{16}) \oplus f(R_{15}, K_{16}) = L_{15}$.
- Thus round 1 decryption yields (R_{15}, L_{15}), i.e., inverting round 16.
- The remaining 15 rounds are likewise cancelled one by one in reverse order of application, due to the reversed key schedule.


64-bit plaintext
Initial permutation
L_0
R_0
f
K_1
K_2
K_{15}
K_{16}
Round 1
Round 2
Round 15
Round 16
Encryption
Decryption
L_{16}
R_{16}
Final permutation
64-bit ciphertext

DES properties and strength

- Each bit of the ciphertext depends on all bits of the key and all bits of the plaintext
- Complementation property
  - Let E denote DES, and $\bar{x}$ the bitwise complement of x. Then $y = E_K(x)$ implies $\bar{y} = E_{\bar{K}}(\bar{x})$.
- Weak keys, semi-weak keys, and possible weak keys
  - A DES weak key is a key K such that $E_K(E_K(x)) = x$ for all x, i.e., defining an involution.
  - A pair of DES semi-weak keys is a pair (K_1, K_2) with $E_{K_1}\left(E_{K_2}(x)\right) = x$.
  - DES has four weak keys and six pairs of semi-weak keys.

- DES Weak keys
  - 01010101 01010101
  - FEFEFEFE FEFEFEFE
  - E0E0E0E0 F1F1F1F1
  - 1F1F1F1F 0E0E0E0E
- DES semi-weak key pairs
  - 01FE 01FE 01FE 01FE, FE01 FE01 FE01 FE01
  - 1FE0 1FE0 0EF1 OEF1, E01F E01F F10E F10E
  - 01E0 01E0 01F1 01F1, E001 E001 F101 F101
  - 1FFE 1FFE 0EFE 0EFE, FE1F FE1F FE0E FE0E
  - 011F 011F 010E 010E, 1F01 1F01 0E01 0E01
  - E0FE E0FE F1FE F1FE, FEE0 FEE0 FEF1 FEF1
- Possible weak keys
  - A possible weak key is a key that creates only four distinct round keys; in other words, the sixteen round keys are divided into four groups and each group is made of four equal round keys.
  - There are also 48 possible weak keys.

Advanced Encryption Standard (AES)

- DES created by IBM was used successfully for close to 20 years.
- In 1999, distributed.net and the Electronic Frontier Foundation publicly break a DES key in 22 hours and 15 minutes.
- a 56-bit system was inadequate against brute force attacks.
- US govt announced a public competition to find a replacement system.
- In the first round of the competition 15 algorithms were accepted and this was narrowed to 5 in the second round.
- All five algorithms, commonly referred to as "AES finalists", were designed by cryptographers considered well-known and respected in the community.
- NIST finally chose **Rijndael**, named after the two Belgian cryptographers who developed and submitted it Vincent Rijmen and Joan Daemen.
- In 2002, it was renamed the Advanced Encryption Standard and published by the U.S. National Institute of Standards and Technology.

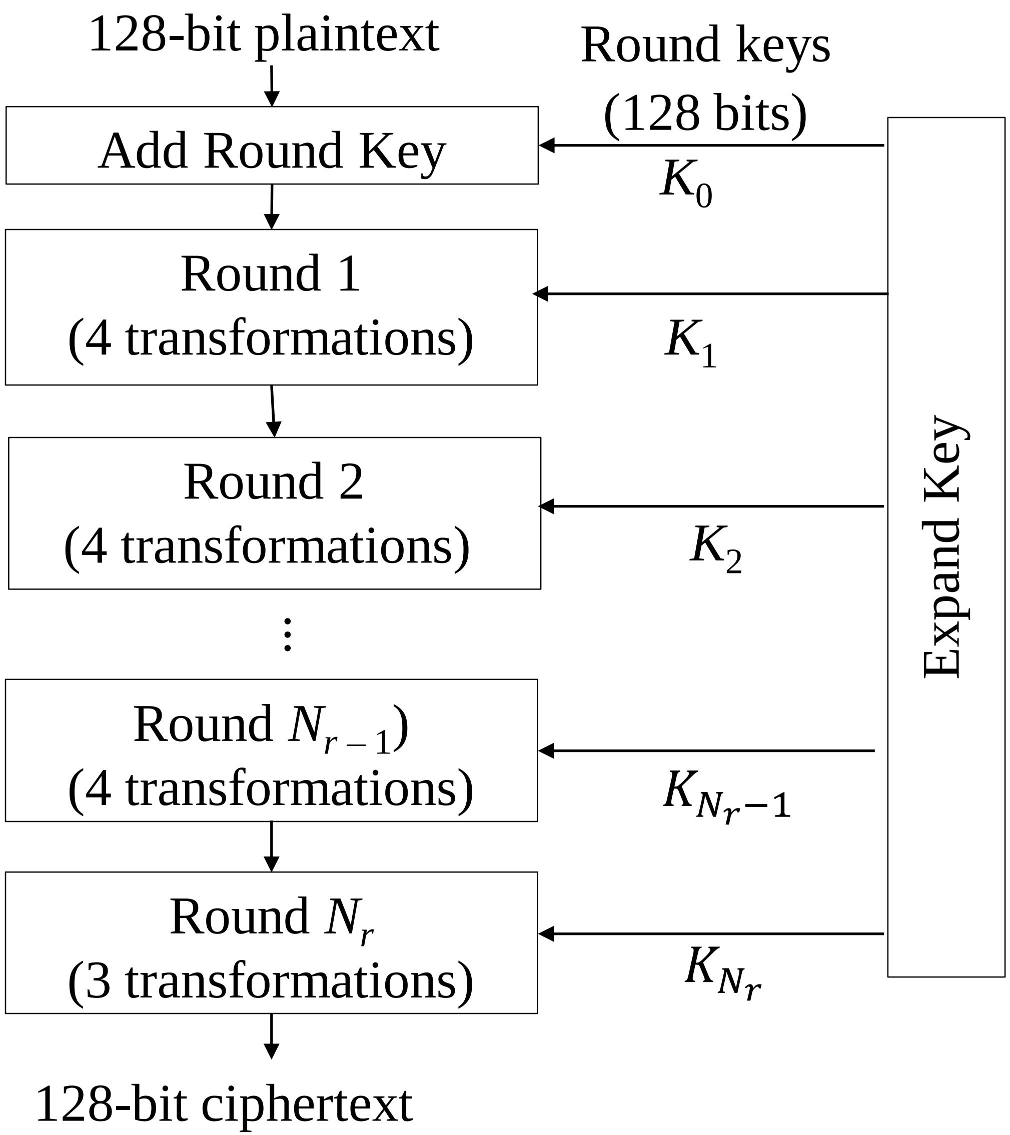
Rijndael - AES

- Rijndael was designed to have the following characteristics:
  - Resistance against all known attacks.
  - Speed and code compactness on a wide range of platforms.
  - Design Simplicity.
- The National Institute of Standards and Technology selected three "flavors" of AES: 128-bit, 192-bit, and 256-bit.
- Each type uses 128-bit blocks. The difference lies in the length of the key.
- The 256-bit key AES provides the strongest level of encryption.
- The three AES varieties are also distinguished by the number of rounds of encryption.
  - AES 128 uses 10 rounds,
  - AES 192 uses 12 rounds,
  - AES 256 uses 14 rounds.

Structure of AES

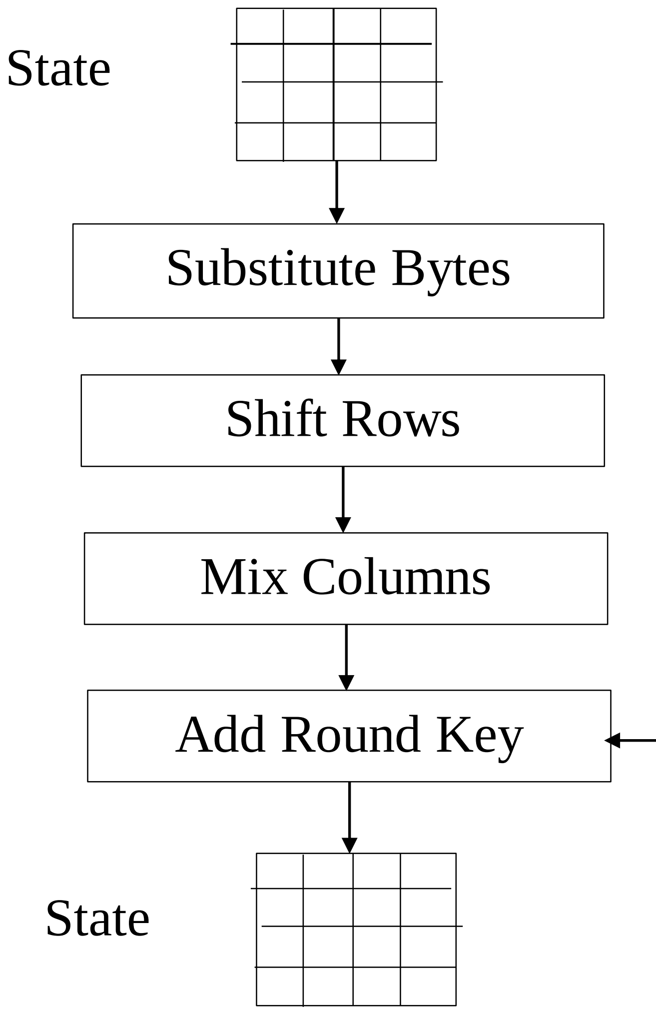
- The input is a single 128 bit block both for decryption and encryption and is known as the **in** matrix.
- This block is copied into a **state** array which is modified at each stage of the algorithm and then copied to an output matrix
- Both the plaintext and key are depicted as a square matrix of bytes.
- This key is expanded into an array of key schedule words.

AES Encryption



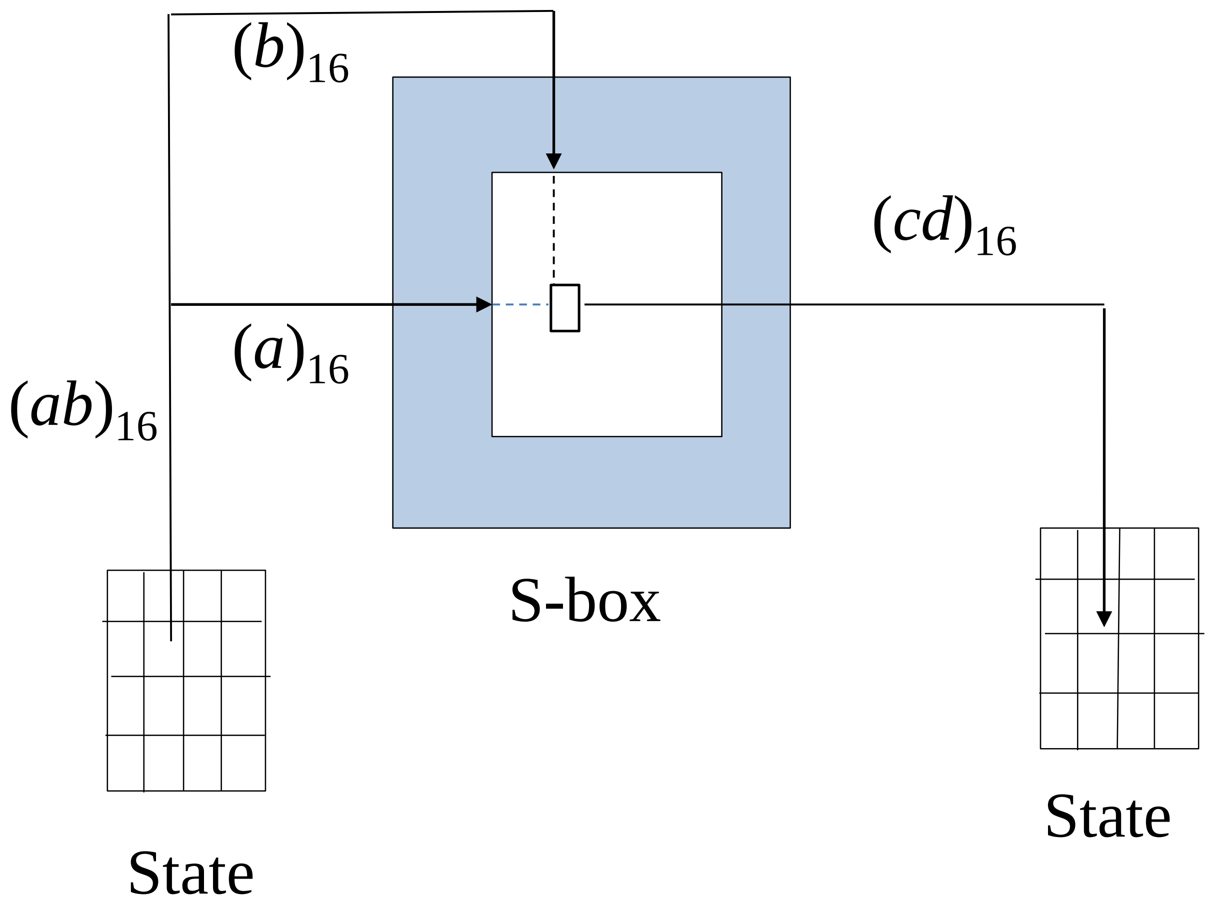
N_r	Key size
10	128
12	192
14	256

Structure of each Round



- One Add Round is applied before the first round
- In Add round key 128 bits of state are XORed with the 128 bits of round key
- Mix Columns transformation is not there in N_r^{th} round

Substitute Bytes transformation



Characteristics of S-box

- The s-box is designed to be resistant to known cryptanalytic attacks.
- Rijndael developers sought a design that has a low correlation between input bits and output bits, and the property that the output cannot be described as a simple mathematical function of the input.
- S-box has no fixed points (s-box(a) = a) and no opposite fixed points (s-box(a) = $\bar{a}$, where a is the bitwise compliment of a.
- The s-box must be invertible, so that decryption is possible

  (Is-box[s-box(a)]= a)

  however it should not be its self-inverse i.e. s-box(a) $\neq$ Is-box(a)
- The Inverse substitute byte transformation makes use of an inverse s-box.

Shift Row Transformation

- It is a simple permutation & works as follow:
- The first row of **state** is *not* altered.
- The second row is shifted 1 bytes to the left in a circular manner.
- The third row is shifted 2 bytes to the left in a circular manner.
- The fourth row is shifted 3 bytes to the left in a circular manner.

s_{00}	s_{01}	s_{02}	s_{03}
s_{10}	s_{11}	s_{12}	s_{13}
s_{20}	s_{21}	s_{22}	s_{23}
s_{30}	s_{31}	s_{32}	s_{33}

Shift Row →

← Inv Shift Row

s_{00}	s_{01}	s_{02}	s_{03}
s_{11}	s_{12}	s_{13}	s_{10}
s_{22}	s_{23}	s_{20}	s_{21}
s_{33}	s_{30}	s_{31}	s_{32}

Mix Column Transformation

- It is a substitution
- Each byte of a column is mapped into a new value that is a function of all four bytes in the column.
- The transformation is matrix multiplication in GF(2^8) with irreducible polynomial $x^8 + x^4 + x^3 + x + 1$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} = \begin{bmatrix} s'_{00} & s'_{01} & s'_{02} & s'_{03} \\ s'_{10} & s'_{11} & s'_{12} & s'_{13} \\ s'_{20} & s'_{21} & s'_{22} & s'_{23} \\ s'_{30} & s'_{31} & s'_{32} & s'_{33} \end{bmatrix}$$

i.e. AS = S′

Elements of the j^{th} column of the product matrix is

$s'_{0j} = (2 \cdot s_{0j}) \oplus (3 \cdot s_{1j}) \oplus s_{2j} \oplus s_{3j}$

$s'_{1j} = s_{0j} \oplus (2 \cdot s_{1j}) \oplus (3 \cdot s_{2j}) \oplus s_{3j}$

$s'_{2j} = s_{0j} \oplus s_{1j} \oplus (2 \cdot s_{2j}) \oplus (3 \cdot s_{3j})$

$s'_{3j} = (3 \cdot s_{0j}) \oplus s_{1j} \oplus s_{2j} \oplus (2 \cdot s_{3j})$

'•'denotes multiplication over the finite field $GF(2^8)$.

Let $s_{00} = (87)_{16}$, $s_{10} = (6E)_{16}$, $s_{20} = (46)_{16}$, $s_{30} = (A6)_{16}$

Represent each Hex number by a polynomial:

$(02)_{16} = x$, $(87)_{16} = x^7 + x^2 + x + 1$

Multiply these two together, we get:

$x \cdot (x^7 + x^2 + x + 1) \bmod (x^8 + x^4 + x^3 + x + 1) = x^4 + x^2 + 1$

This is equal to 0001 0101 in binary. i.e.

$(2 \cdot s_{00}) = 0001\ 0101$, $(3 \cdot s_{10}) = 1011\ 0010$, $s_{2j} = 0100\ 0110$, $s_{3j} = 1010\ 0110$

$s'_{00} = (2 \cdot s_{00}) \oplus (3 \cdot s_{10}) \oplus s_{20} \oplus s_{30} = 0100\ 0111 = (47)_{16}$

For Inv Mix Columns $S = A^{-1} S'$

Key Expansion of AES 128

- The AES key expansion algorithm takes as input a 4-word key and produces a linear array of 44 words.
- Each subkey is 128 bits (4-word) long.
- Design criteria
  - Efficient
  - resistant to known cryptanalytic attacks
  - Non-symmetric : ensured by round constants
  - Efficient diffusion properties of secret key into round keys

```
KeyExpansion (byte key[16],word w[44])
  word temp
  for i = 0 to 4
      w[i] = (key[4*i], key[4*i + 1], key[4*i + 2], key[4*i + 3]);
  for i = 4 to 44
       temp = w[i – 1]
       if (i mod 4) = 0
           temp = SubWord (RotWord (temp)) ⊕ Rcon[i/4]
           w[i] = w[i – 4] ⊕ temp
```

RotWord performs a one-byte circular left shift on a word.

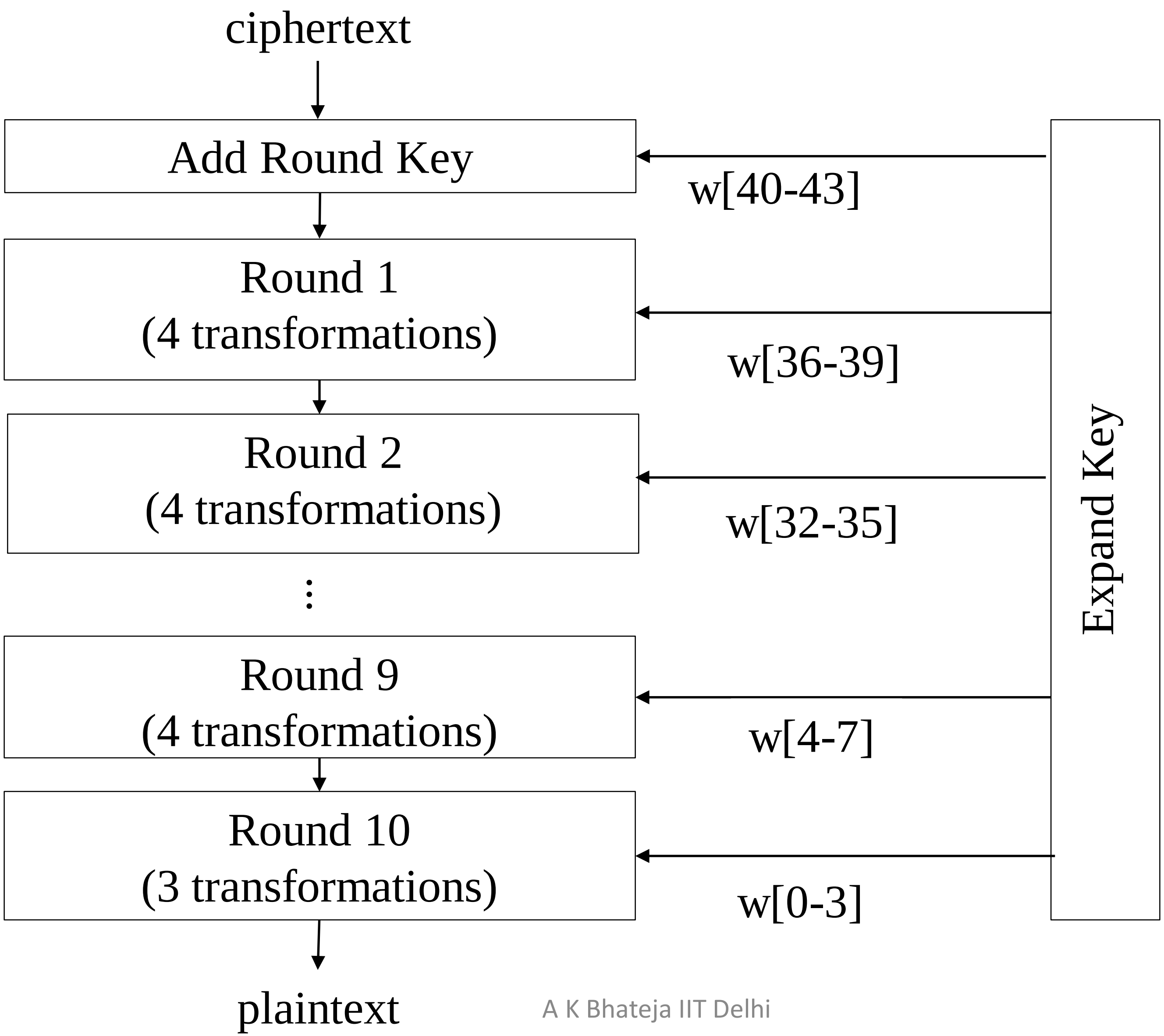
i.e. $[b_0, b_1, b_2, b_3] \rightarrow [b_1, b_2, b_3, b_0]$.

SubWord performs a byte substitution on each byte of its input word, using the S-box.

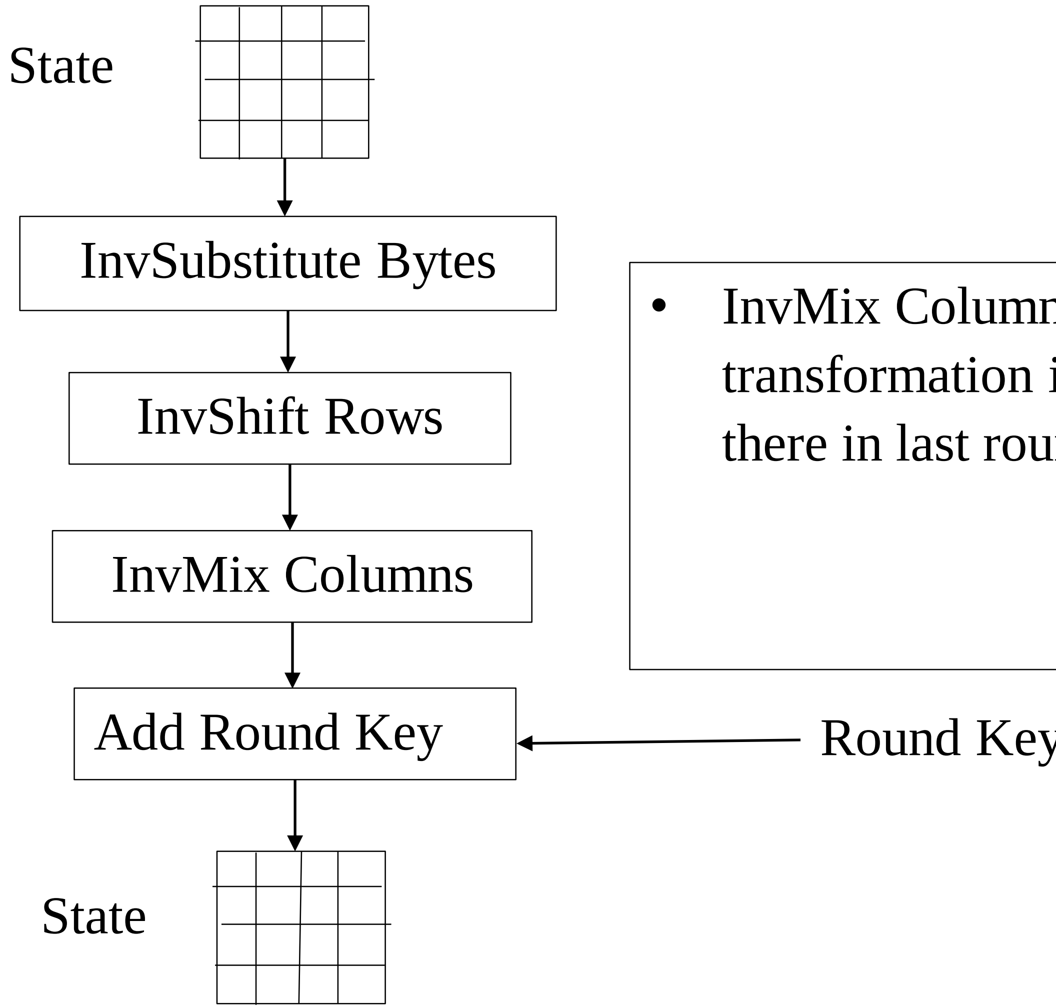
The result of steps 1 and 2 is XORed with round constant, Rcon[j].

$Rcon[j] = (RC[j], 0, 0, 0)$, with $RC[1]= 1$, $RC[j]= 2\bullet RC[j-1]$ and with multiplication defined over the field $GF(2^8)$.

AES Decryption



Structure of a round in AES Decryption



- InvMix Columns transformation is not there in last round

Security & Implementation of AES

- **Security**
  - AES was designed after DES. Most of the known attacks on DES were already tested on AES.
  - **Brute-Force Attack**
    - AES is definitely more secure than DES due to the larger-size key.
  - **Statistical Attacks**
    - Numerous tests have failed to do statistical analysis of the ciphertext.
  - **Differential and Linear Attacks**
    - AES resists differential and linear cryptanalysis.
- **Implementation**
  - AES can be implemented in software, hardware, and firmware. The implementation can use table lookup process or routines that use a well-defined algebraic structure.
  - The algorithms used in AES are so simple that they can be easily implemented using cheap processors and a minimum amount of memory.