Chapter 9: Symmetric Key Encryption

Information Security

Nguyễn Đăng Quang

Fall 2017

Goals

- Describe the components of block ciphers,
- Explain the operation of feistel function
- Explain the operation of Data Encryption Standard (DES),
- Explain the operation of Advanced Encryption Standard (AES),
- Encrypting large message

Symmetric Ciphers

- Use the same cryptographic keys for both encryption of plaintext and decryption of cipher text.
- Being faster than asymmetric ciphers and allow encrypting large sets of data.
- However, they require sophisticated mechanisms to securely distribute the secret keys to both parties.
- For every m (message), and k (key), the following equality holds:

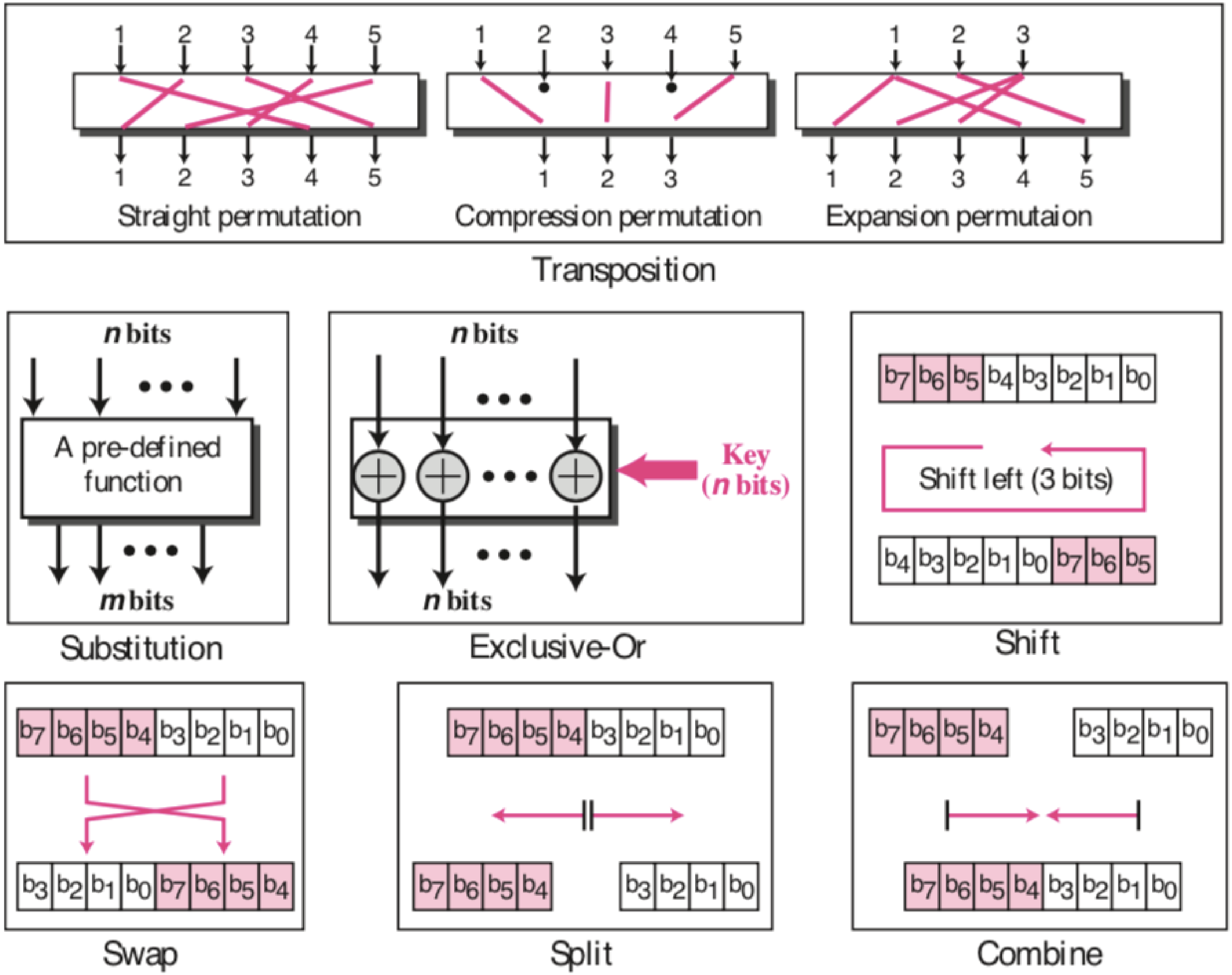
$$D(k, E(k, m)) = m$$

Components

To provide an attack-resistant cipher, a modern block cipher is made of a combination of:

- P-boxes – Transposition units
- S-boxes – Substitution units
- XOR operations, shifting, swapping, splitting, combining elements

Components



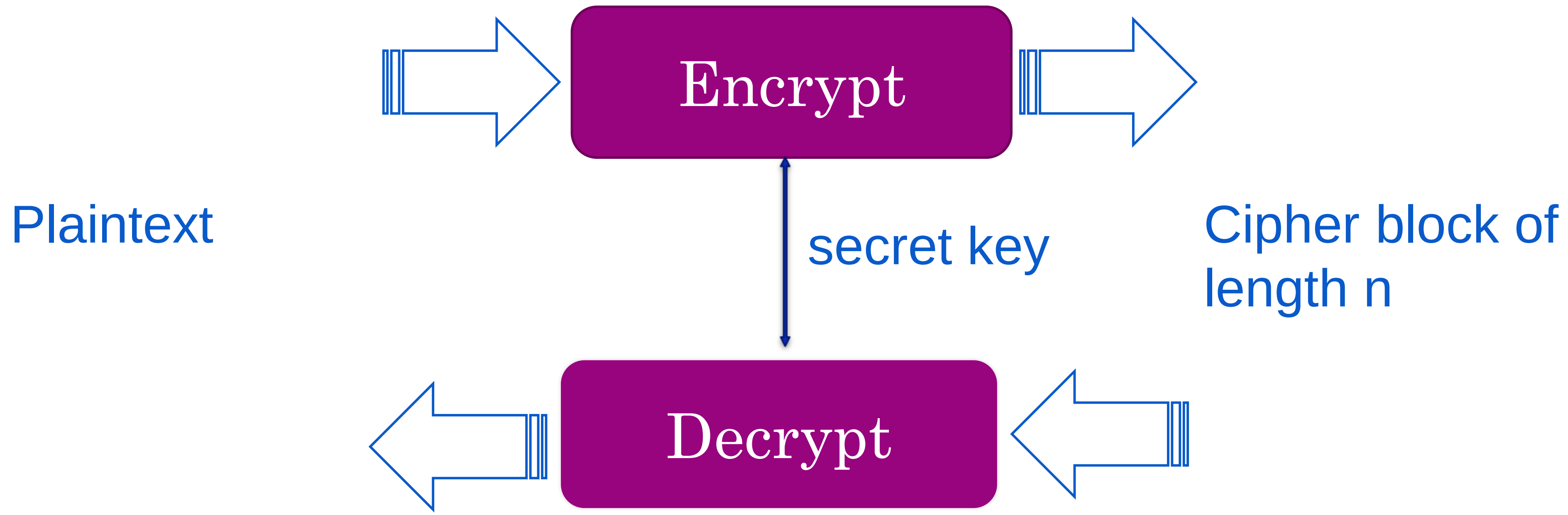
Straight permutation
Compression permutation
Expansion permutaion
Transposition
n bits
A pre-defined function
m bits
Substitution
n bits
Key (n bits)
n bits
Exclusive-Or
Shift left (3 bits)
Shift
Swap
Split
Combine

Block Cipher Primitives (Shannon)

- **Confusion**: obscure the relationship between a key and cipher text,
  - Achieved with substitution.
- **Diffusion**: plaintext bits are spread over many bits in a cipher text,
  - Achieved with permutation.
- **Round**: To enhanced the security by combining the substitution and permutation in multiple round.

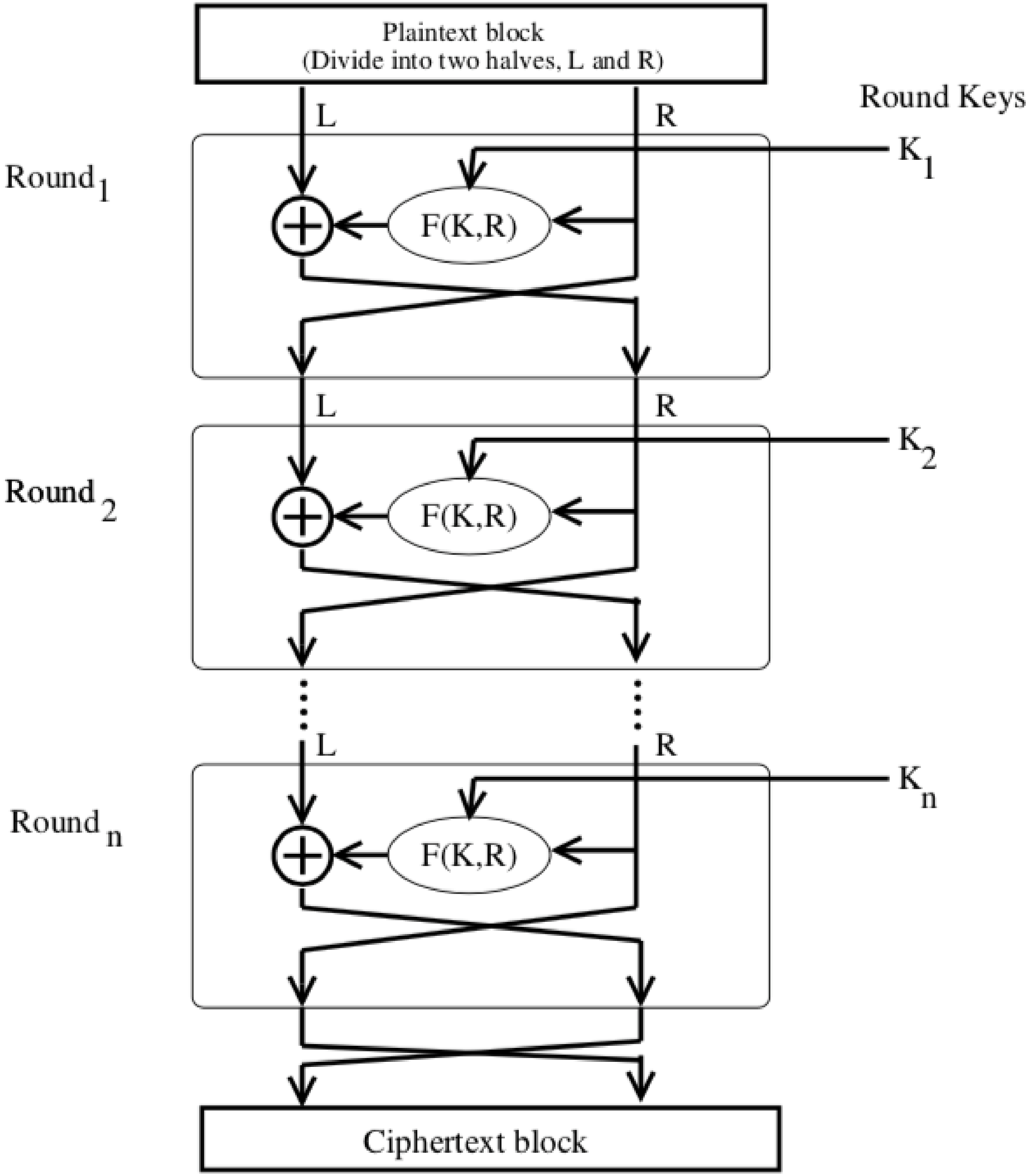
Block Cipher Scheme

- Most symmetric encryption schemes are blocked ciphers,
- Take input as fixed length plain text,



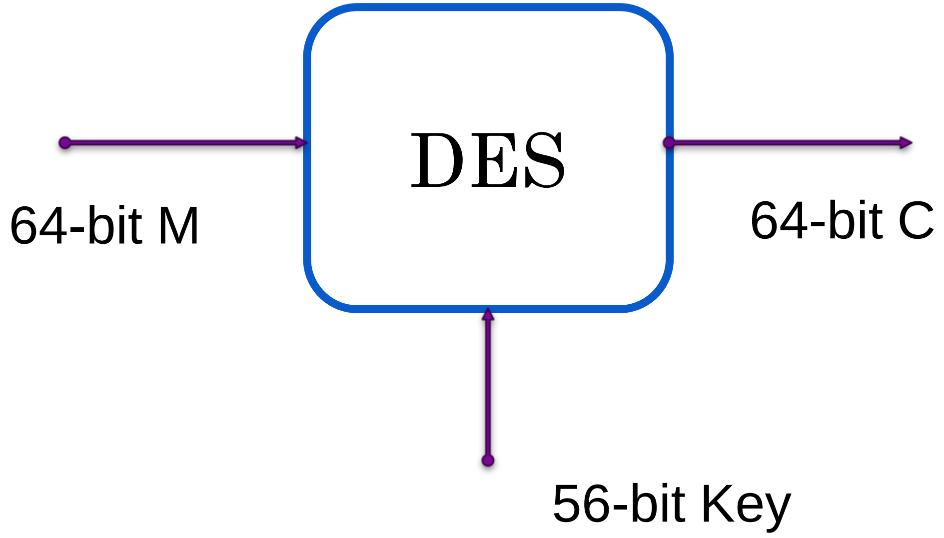
The Feistel Structure for Block Ciphers

- Named after the IBM cryptographer Horst Feistel and first implemented in the Lucifer cipher by Horst Feistel and Don Coppersmith.
- A cryptographic system based on Feistel structure uses the same basic algorithm for both encryption and decryption.

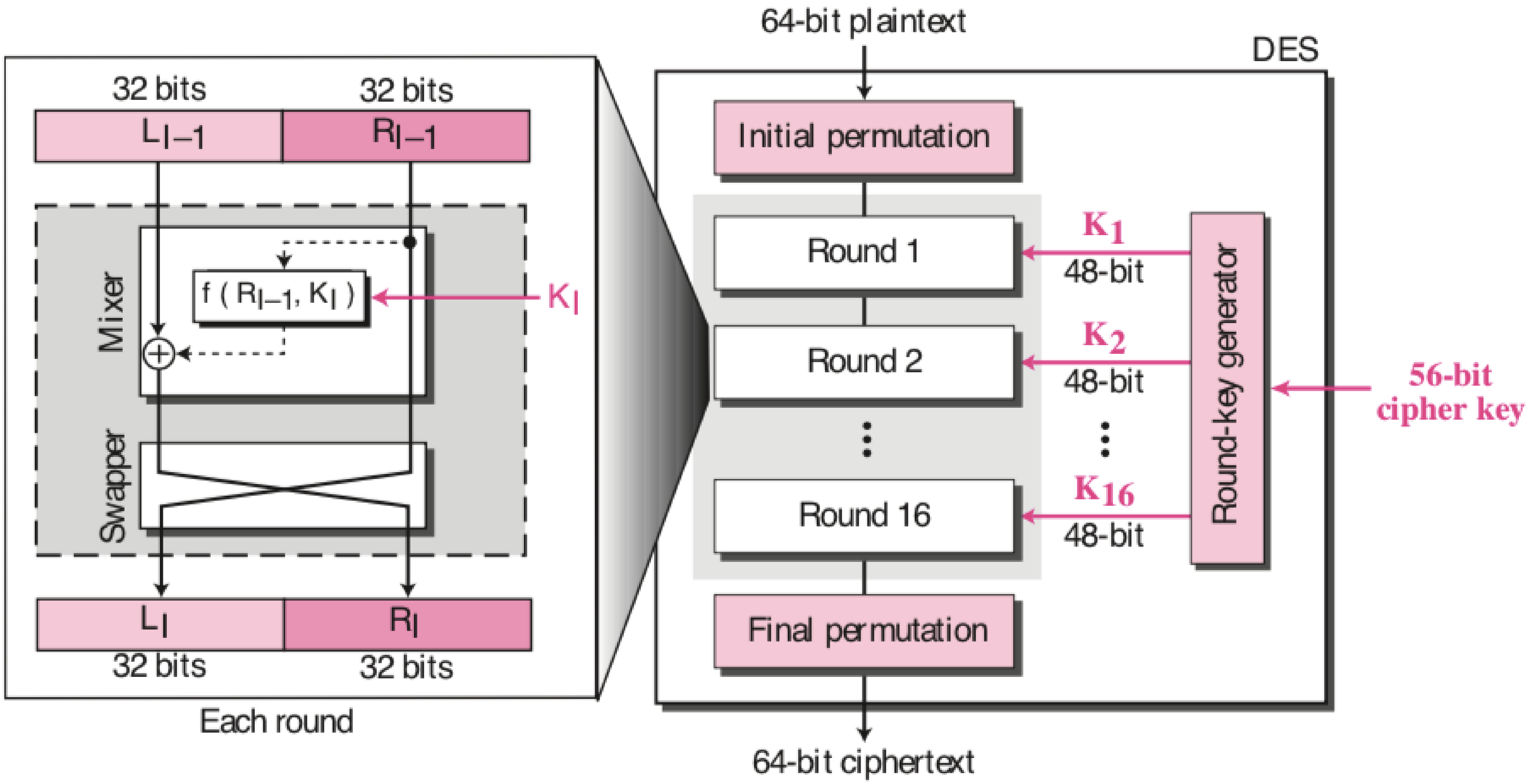


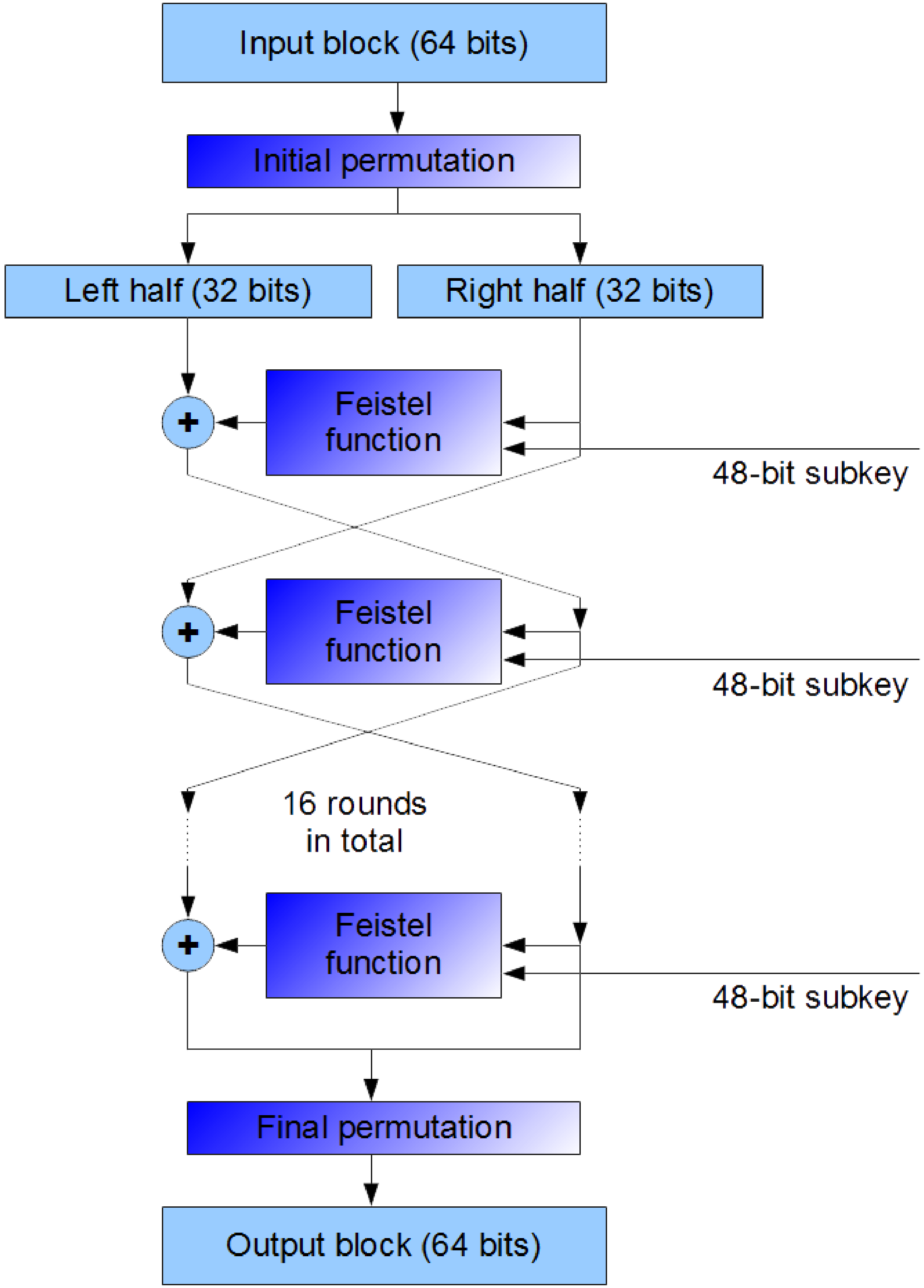
Data Encryption Standard (DES)

- The key is 64-bit length, the actual value is 56 bits plus 1 parity-bits for each byte.
- Input plaintext block message is 64-bit length.
- Output ciphertext block message is 64-bit length.



Structure of DES

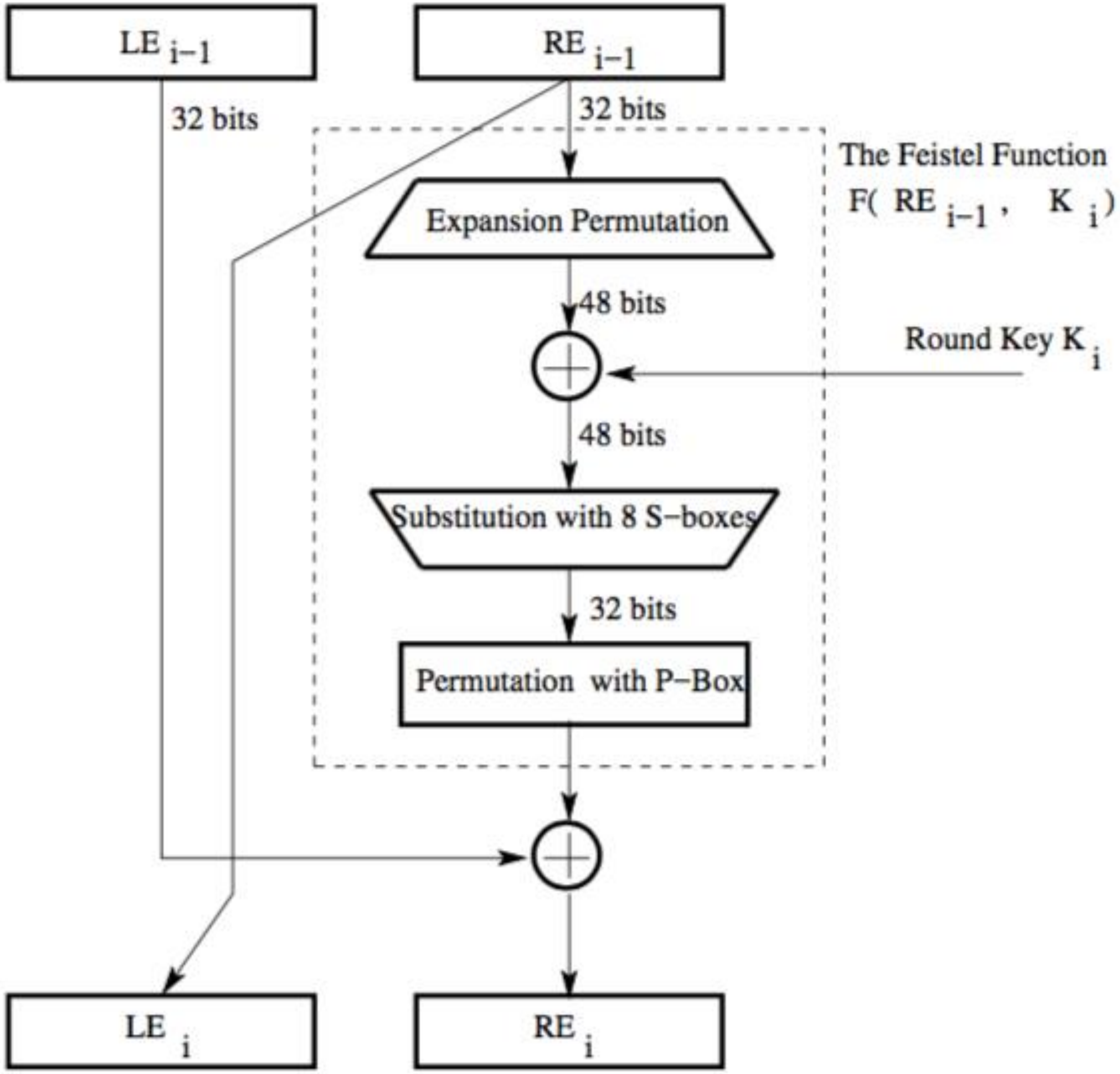




DES Algorithm

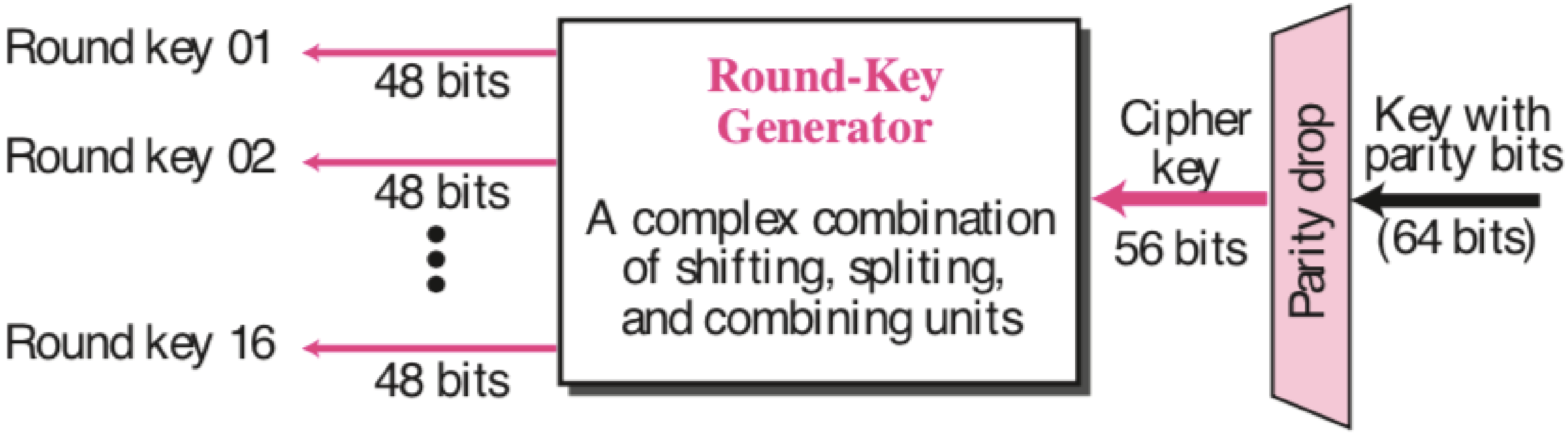
1. Initial permutation rearranges bits in a certain, predefined way.
2. The input data is divided into two 32-bit parts: the left one and the right one.
3. 56 bits are selected from the 64-bit key (Permutation PC-1). They are then divided into two 28-bit parts.
4. Sixteen rounds of the feistel function operations are performed.
5. After all sixteen rounds, the left and the right halves of data are combined using the XOR operation.
6. The Final Permutation is performed

A DES round



1. The 32-bit right half of input data block is expanded by into a 48-bit block.
2. The 56-bit key is divided into two halves, each half shifted separately, and permuted/contracted to yield a 48-bit round key (confusion)
3. The 48 bits of the expanded output are XORed with the round key (key mixing)
4. The output is broken into eight 6-bit words then goes through a substitution with an S-box (diffusion)
5. The 32-bits output then go through a P-box based permutation.
6. The output of the P-box is then XORed with the left half of the 64-bit block that we started out with.
7. Final XOR operation produces the right half block for the next round.

Key generation



Triple DES

- 3DES cipher is a popular block symmetric cipher, created based on DES.
- It was presented in 1998, and is also called Triple Data Encryption Algorithm (TDEA).
- Block length = 64 bits
- Key length = 56, 112, or 168 bits
- 3DES cipher was developed because DES encryption, invented in the early 1970s and protected by a 56-bit key, turned out to be too week and easy to break using modern computers of that time. The effective security which 3DES provides is 112 bits

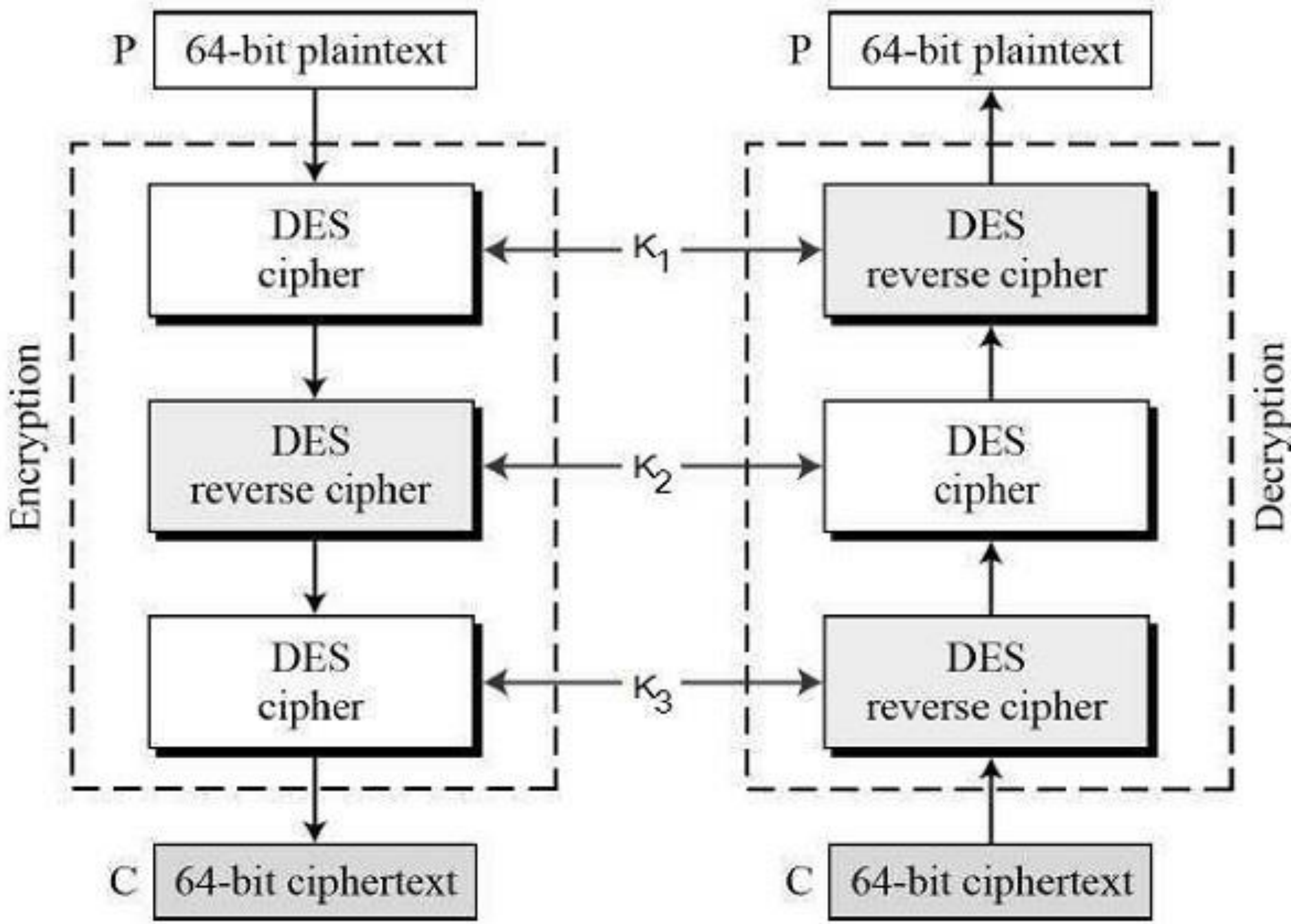
Triple DES

- Triple DES algorithm performs three iterations of a typical DES algorithm.
- In its strongest version, it uses a secret key which consists of 168 bits. The key is then divided into three 56-bit keys
- The encryption and decryption operations may be presented as mathematical equations:
- Encryption:
  $c = E_3(D_2(E_1(m)))$
- Decryption:
  $m = D_1(E_2(D_3(c)))$

3 DES Scheme

1. Encrypt the plaintext blocks using single DES with key K_1.
2. Now decrypt the output of step 1 using single DES with key K_2.
3. Finally, encrypt the output of step 2 using single DES with key K_3.
4. The output of step 3 is the ciphertext.

Decryption of a ciphertext is a reverse process. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1



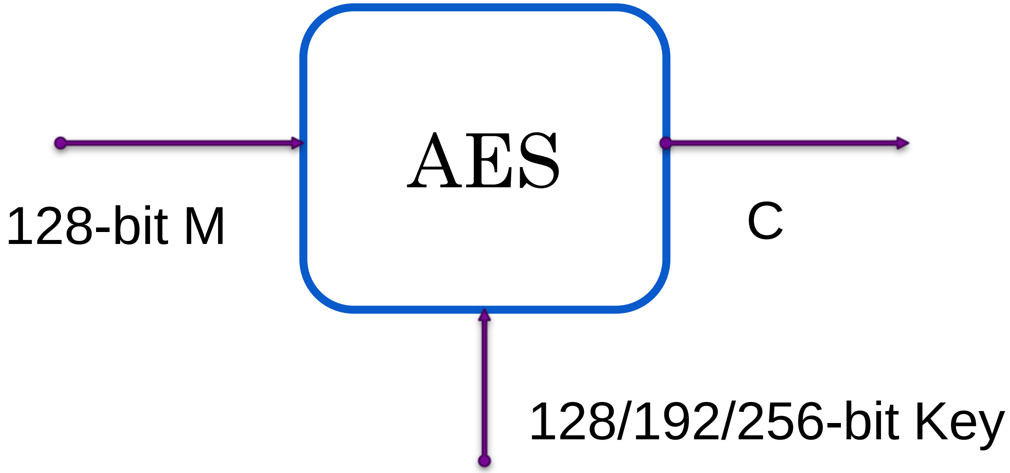
Advanced Encryption Standard (AES)

The History

- 1997: NIST called for a new encryption standard
- Five finalists: MARS, RC6, Rijndael, Serpent and Twofish
- Rijndael was selected as AES

Advanced Encryption Standard (AES)

- It was developed in 1997 by Vincent Rijmen and Joan Daemen (RijDael algorithm), and later approved as a federal encryption standard in the United States in 2002.
- AES is a modern block symmetric cipher, one of the most popular ciphers in the world. Block cipher with symmetric secret key.
- Block length = 128 bits
- Secret key in AES, for encryption and decryption, may be 128 or 192 or 256 bits. Based on the length of the key, a different number of encrypting cycles is performed

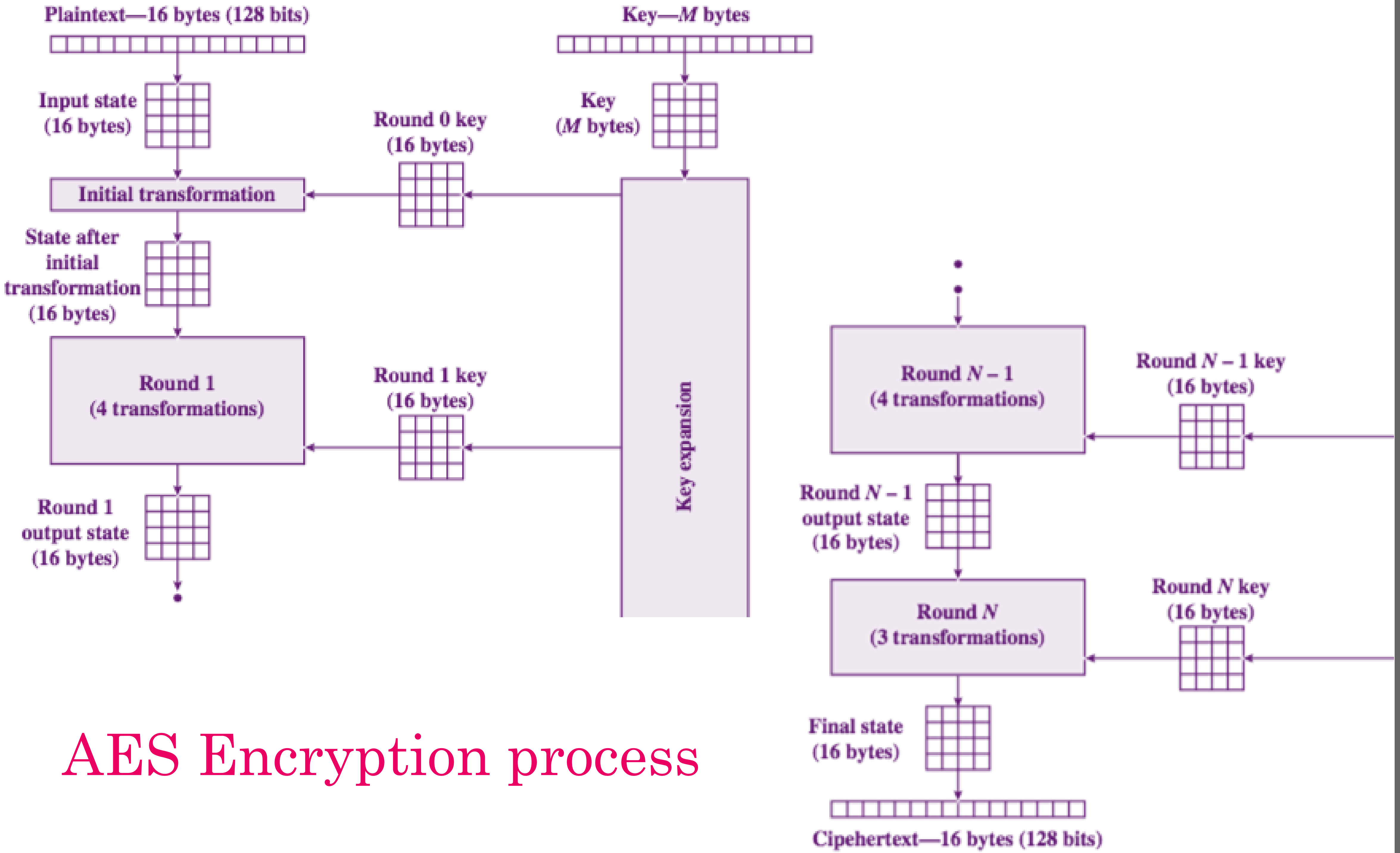


#-bit key
128 – 10 rounds
192 – 12 rounds
256 – 14 rounds

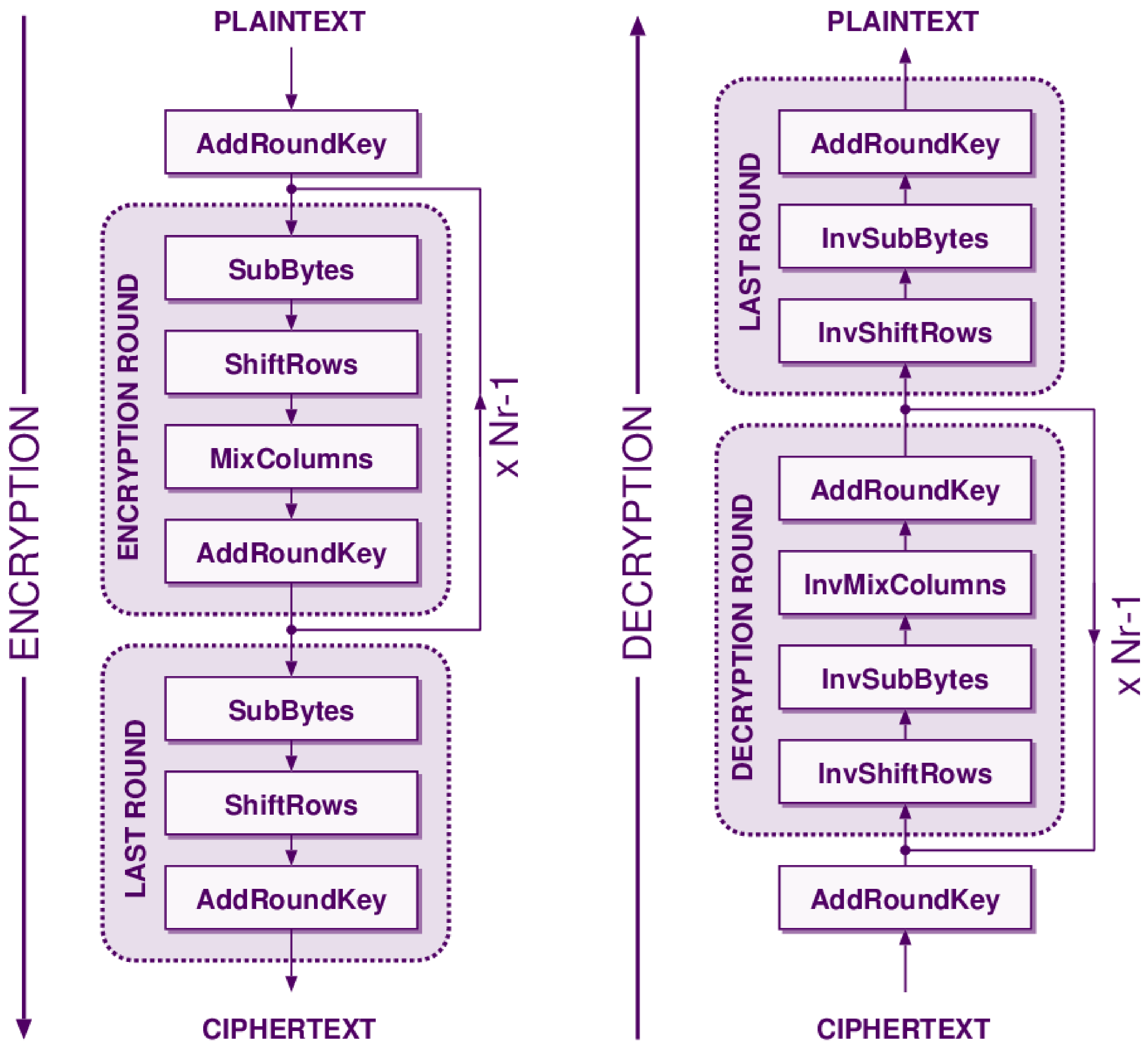
AES Parameter & Key

- **Nb**: is the number of 32-bit words in an encryption block.
  E.g., for AES-128: Nb = 4.
- **Nk**: is the number of 32-bit words in an encryption key.
  E.g., for AES-128: Nk = 4.
- **Nr:** is the number of rounds.
  It should be large enough to allow sufficient mixing so that each bit of a plain text block or a key has a complex effect on each bit of the resulting cipher text.
  Nr = 6 + Max (Nb, Nk),
  E.g., for AES-128: Nr = 10

- Cryptanalysis: With 128 bit: $2^{128} = 3.4x\ 10^{38}$ possible keys → A PC that tries 255 keys per second needs 149.000 billion years to break AES



AES Encryption process


ENCRYPTION
PLAINTEXT
AddRoundKey
ENCRYPTION ROUND
SubBytes
ShiftRows
MixColumns
AddRoundKey
x Nr-1
LAST ROUND
SubBytes
ShiftRows
AddRoundKey
CIPHERTEXT
DECRYPTION
PLAINTEXT
LAST ROUND
AddRoundKey
InvSubBytes
InvShiftRows
DECRYPTION ROUND
AddRoundKey
InvMixColumns
InvSubBytes
InvShiftRows
x Nr-1
AddRoundKey
CIPHERTEXT

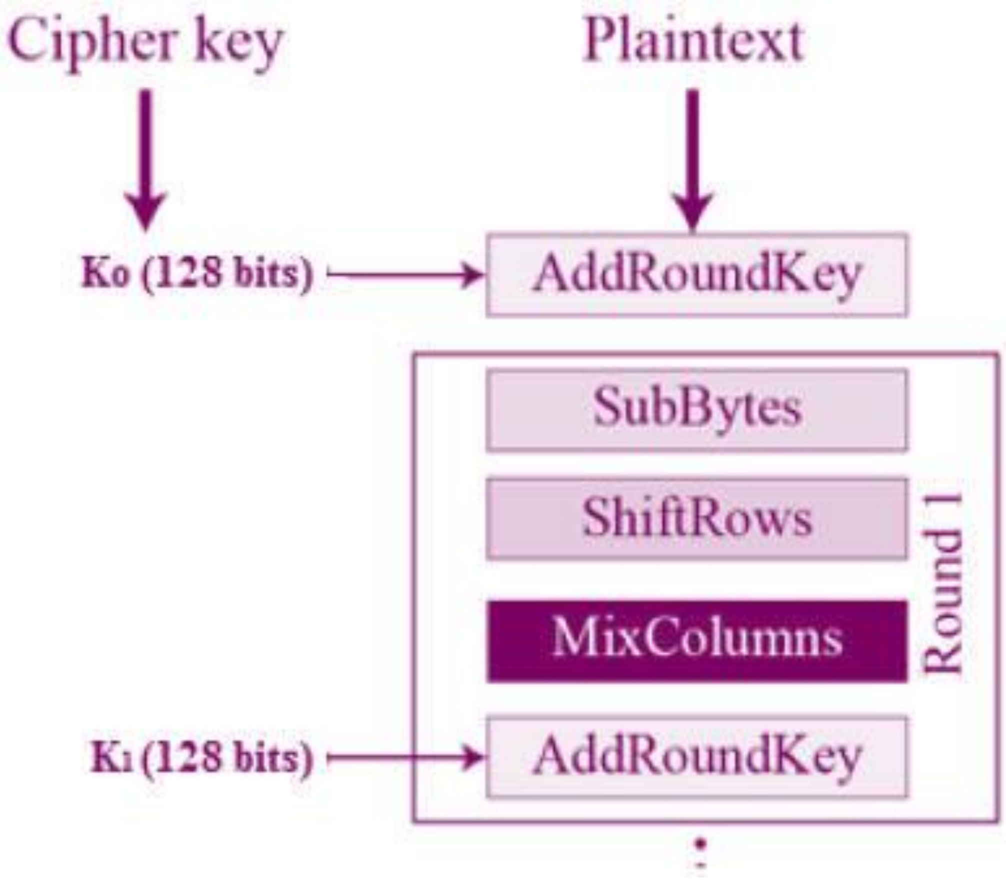
AES Algorithm

- **Key Expansion-** round keys are derived from the cipher key using Rijndael key schedule
  - Initial RoundAdd Round Key- each byte of the state is combined with the round key using bitwise xor
- **Rounds**:
  - SubBytes: a non-linear substitution step where each byte is replaced with another according to a lookup table.
  - ShiftRows: a transposition step where each row of the state is shifted cyclically a certain number of steps.
  - MixColumns: a mixing operation which operates on the columns of the state, combining the four bytes in each column.
  - AddRoundKey
- **Final Round** (no MixColumns)
  - SubBytes
  - ShiftRows
  - AddRoundKey

High-level Description

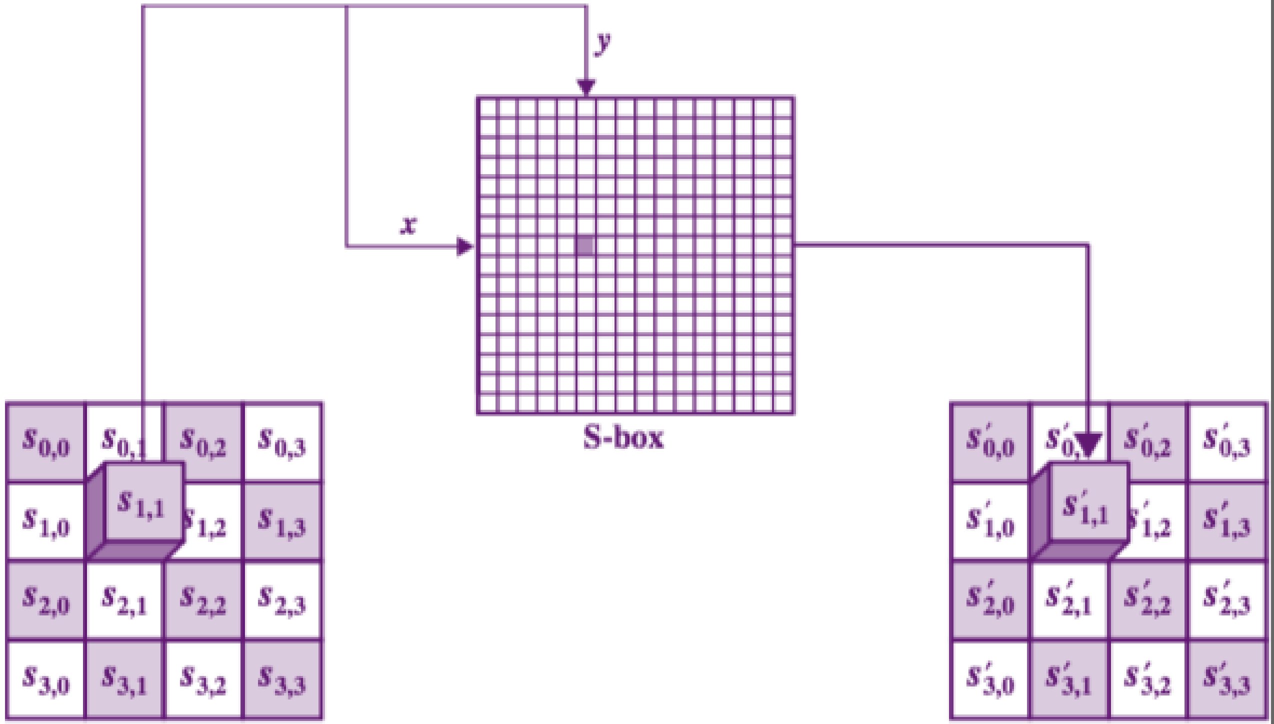
- Each round consists of 4 layers:
  1. SubBytes,
  2. ShiftRows,
  3. MixColumns
  4. AddRoundKey

  Remark:
  - The last round does not have MixColumns
  - Key Whitening is added at the beginning and end a sub-key



Substitute Byte Transformation

- Called SubBytes: simple table lookup.
- AES defines a 16 * 16 matrix of byte values, called an S-box, that contains a permutation of all possible 256 8-bit values.
- Each individual byte of *State* is mapped into a new byte:
  - Leftmost 4 bits of the byte are used as a row value; rightmost 4-bits used as a column value
  - these row and column values serve as indexes into the S-box to select a unique 8-bit output value



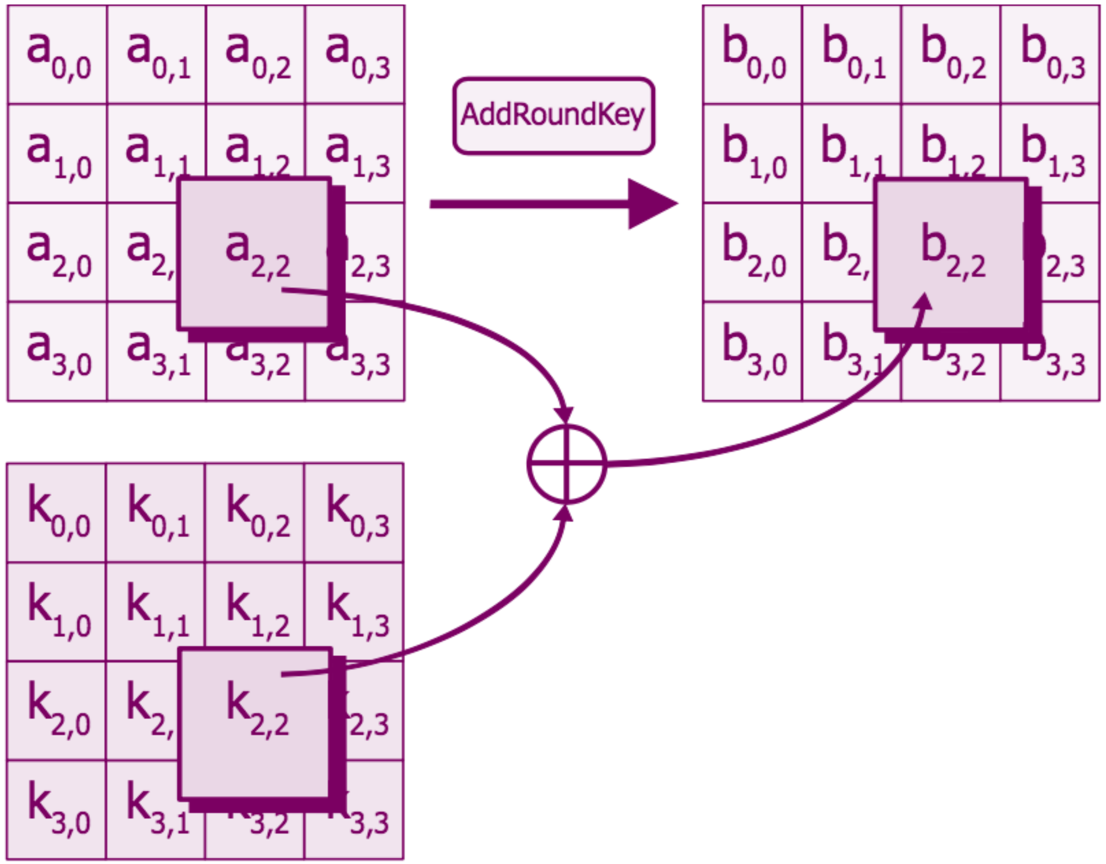
Substitute Byte Transformation

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	3	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

- Example: Byte value 53 will be substituted by ED

Add Round key step

In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main [key](key) using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise [XOR](XOR).



ShiftRow Transformation

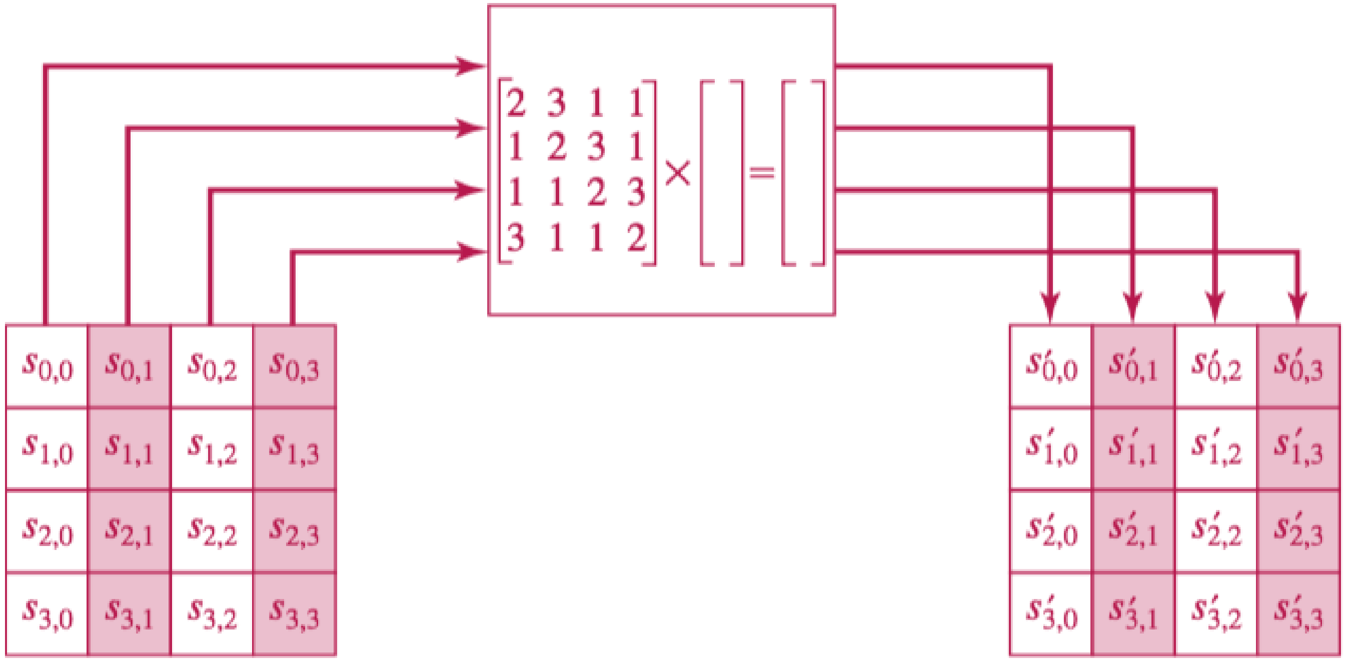
- Circular Left Shift of a number of bytes equal to the row number

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

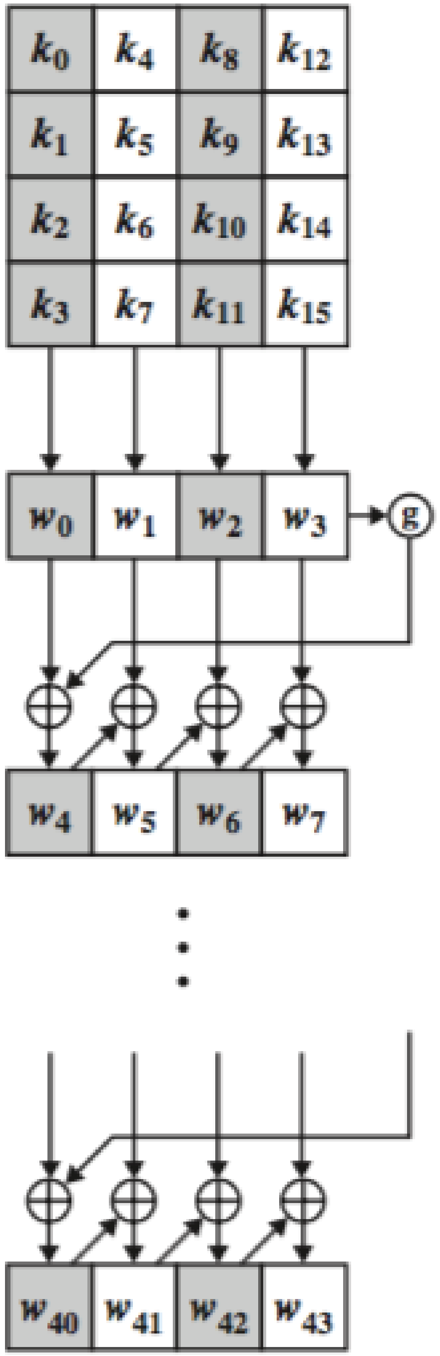
MixColumn Transformation

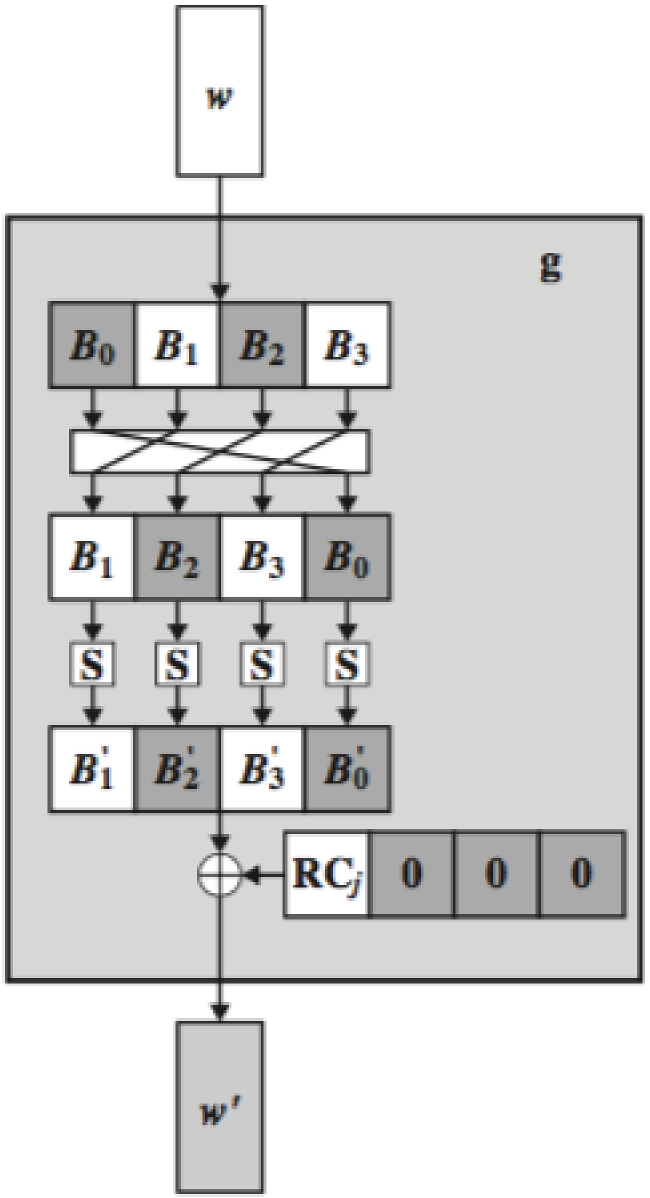
- The MixColumns transformation operates on each column individually.
- Each byte of a column is mapped into a new value that is a function of all four bytes in the column; the transformation is performed in GF (Galois Field)
- *This with shiftRows* transformation provides *diffusion*



AES Key Expansion

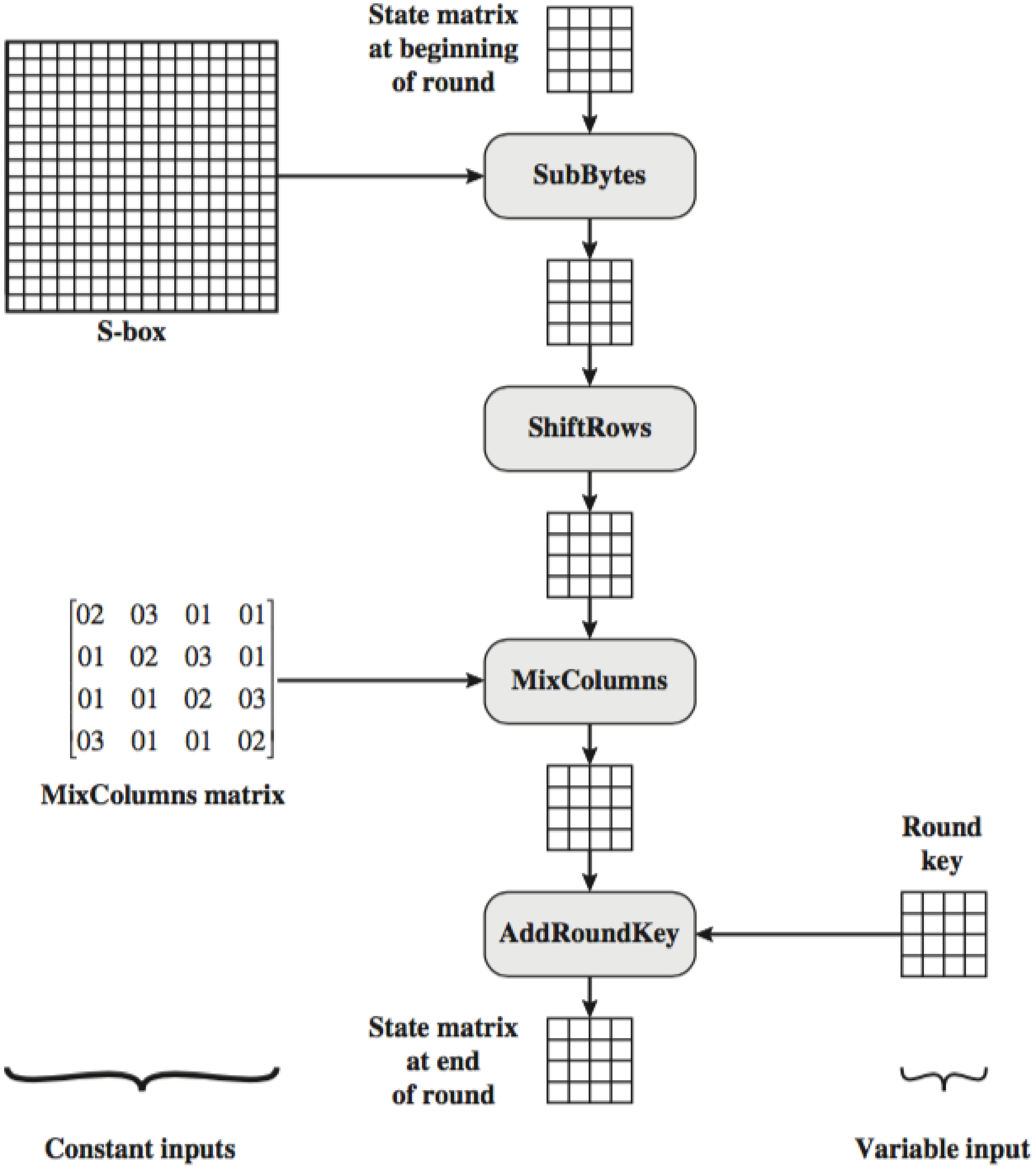
- Takes a four-word (16-byte) key input
- Produces a linear array of 44 words (176 bytes). This is sufficient to provide a four-word round key for the initial AddRoundKey stage and each of the 10 rounds of the cipher.





(b) Function g

Inputs for a single AES Round



DES vs. AES

- Substitution-Permutation, iterated cipher, Fiestel structure
- 64-bit block size, 56-bit key size
- 8 different S-boxes
- Design optimized for hardware implementations
- Closed (secret) design process

- Substitution-Permutation, iterated cipher
- 128-bit block size, 128-bit (192, 256) key sizes
- 1 S-box
- Design optimized for byte-orientated implementations
- Open design and evaluation process

AES Avalanche effect: Change in plaintext

Round		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

AES Avalanche effect: Change in key

Round		Number of Bits that Differ
	0123456789abcdeffedcba9876543210 0123456789abcdeffedcba9876543210	0
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	657470750fc7ff3fc0e8e8ca4dd02a9c c5a9ad090ec7ff3fc1e8e8ca4cd02a9c	22
2	5c7bb49a6b72349b05a2317ff46d1294 90905fa9563356d15f3760f3b8259985	58
3	7115262448dc747e5cdac7227da9bd9c 18aeb7aa794b3b66629448d575c7cebf	67
4	f867aee8b437a5210c24c1974cffeabc f81015f993c978a876ae017cb49e7eec	63
5	721eb200ba06206dcbd4bce704fa654e 5955c91b4e769f3cb4a94768e98d5267	81
6	0ad9d85689f9f77bc1c5f71185e5fb14 dc60a24d137662181e45b8d3726b2920	70
7	db18a8ffa16d30d5f88b08d777ba4eaa fe8343b8f88bef66cab7e977d005a03c	74
8	f91b4fbfe934c9bf8f2f85812b084989 da7dad581d1725c5b72fa0f9d9d1366a	67
9	cca104a13e678500ff59025f3bafaa34 0ccb4c66bbfd912f4b511d72996345e0	59
10	ff0b844a0853bf7c6934ab4364148fb9 fc8923ee501a7d207ab670686839996b	53

AES Implementation aspect

For 8-Bit Processor

- AES can be implemented very efficiently on an 8-bit processor.
  AddRoundKey is a bytewise XOR operation.
  ShiftRows is a simple byte-shifting operation.
  SubBytes operates at the byte level and only requires a table of 256 bytes.
- The transformation MixColumns requires matrix multiplication in the field GF(2^8), which means that all operations are carried out on bytes.

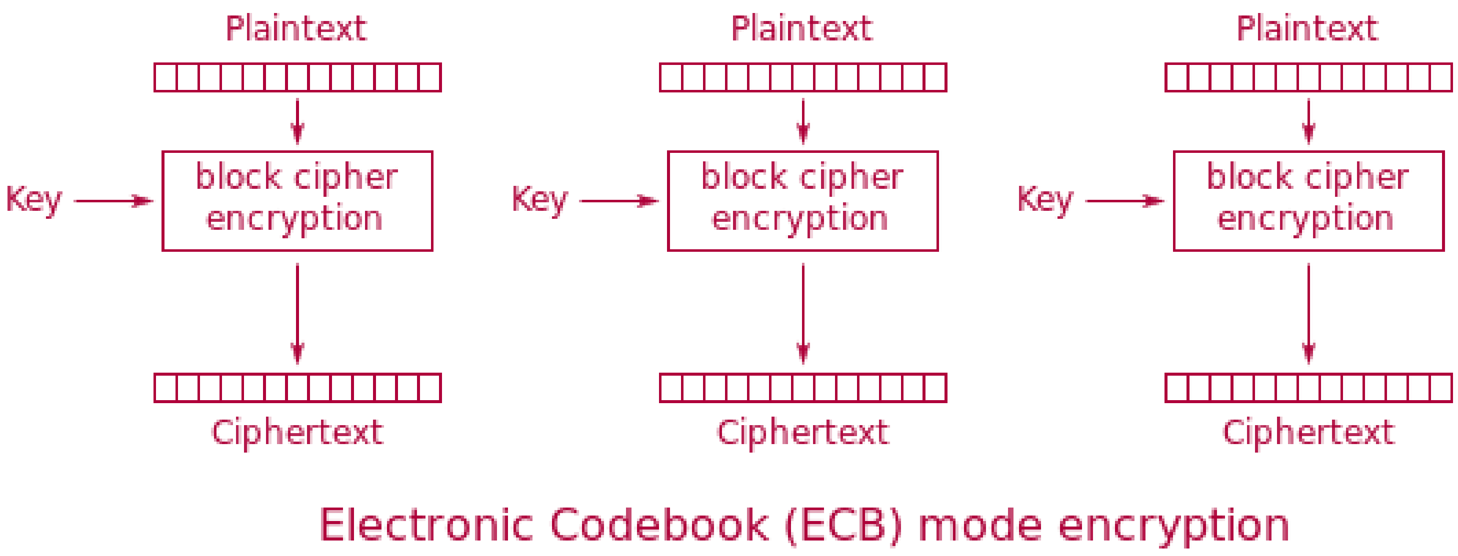
Encrypting a large message

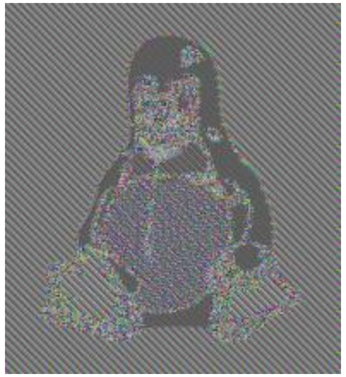
- Partition into n-bit blocks
- Choose mode of operation
  - Electronic Codebook (ECB),
  - Cipher-Block Chaining (CBC),
  - Cipher Feedback (CFB),
  - Output Feedback (OFB),
  - Counter (CTR)
- Padding schemes

Evaluation Criteria

- Identical messages
  - Under which conditions ciphertext of two identical messages are the same
- Chaining dependencies
  - How adjacent plaintext blocks affect encryption of a plaintext block
- Error propagation
  - Resistance to channel noise
- Efficiency
  - Parallelization: random access

Electronic Codebook (ECB)

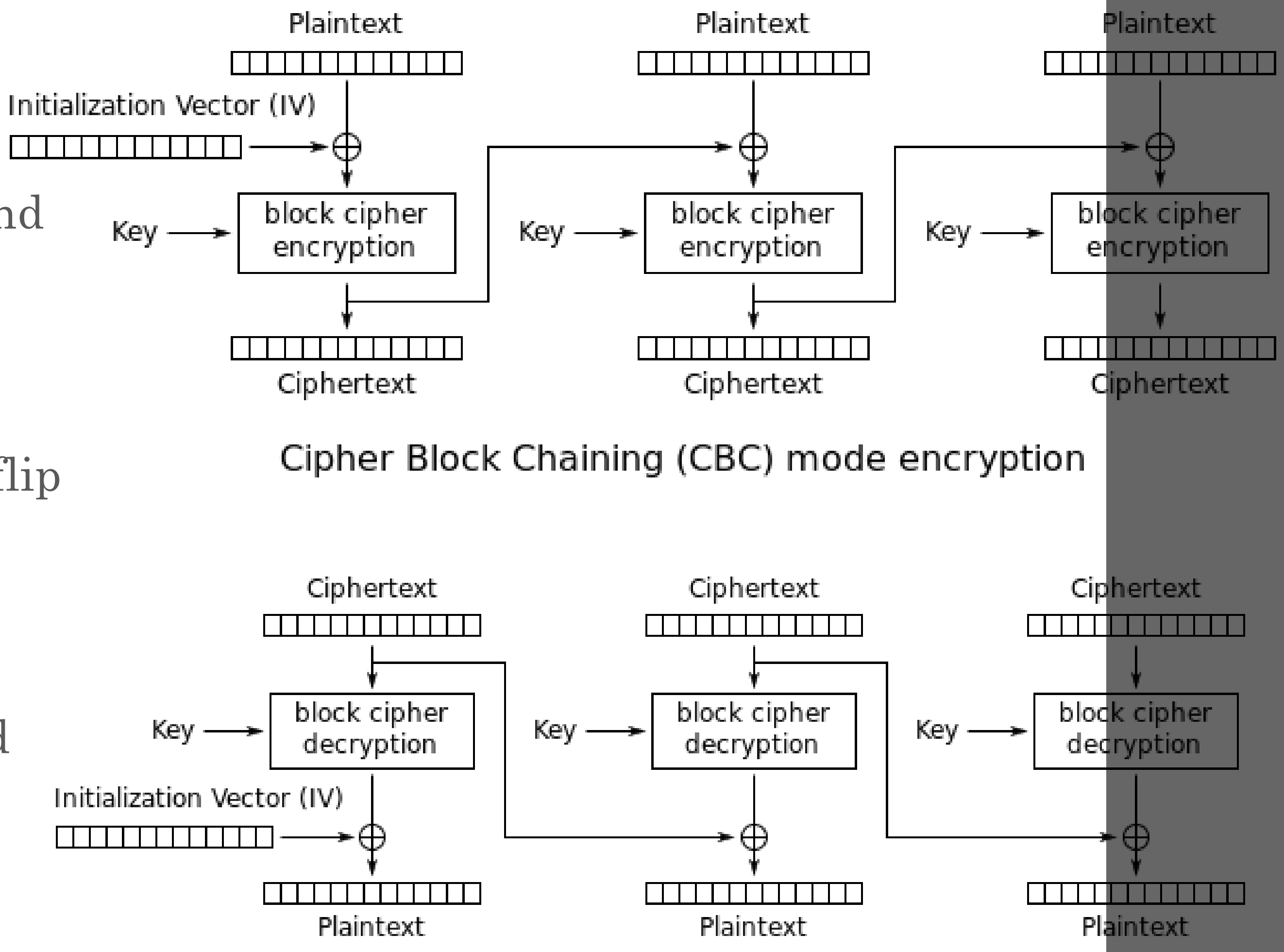




- The simplest of the encryption mode: the message is divided into blocks, and each block is encrypted separately.
- The disadvantage of this method is that identical plaintext blocks are encrypted into identical ciphertext blocks ➔ does not hide data patterns well ➔ doesn't provide serious message confidentiality ➔ is not recommended for use in cryptographic protocols.

Cipher Block Chaining (CBC)

- Identical messages: Changing IV results in different ciphertext.
- Chaining: Ciphertext block cj depends on xj and all preceding plaintext blocks (dependency contained in cj-1)
- Error propagation: Single bit error on cj may flip the corresponding bit on xj+1, but changes xj significantly.
- IV needs not be secret, but its integrity should be protected.
- Block processing cannot be parallelized



Cipher Block Chaining (CBC) mode encryption

Cipher Block Chaining (CBC) mode decryption

Protecting Message Integrity

- Need to prevent or detect any unauthorized modification to the message.
- One standard approach: send the last block of CBC (CBC residue), along with a plain text.
- The CBC residue provides a protection of message integrity