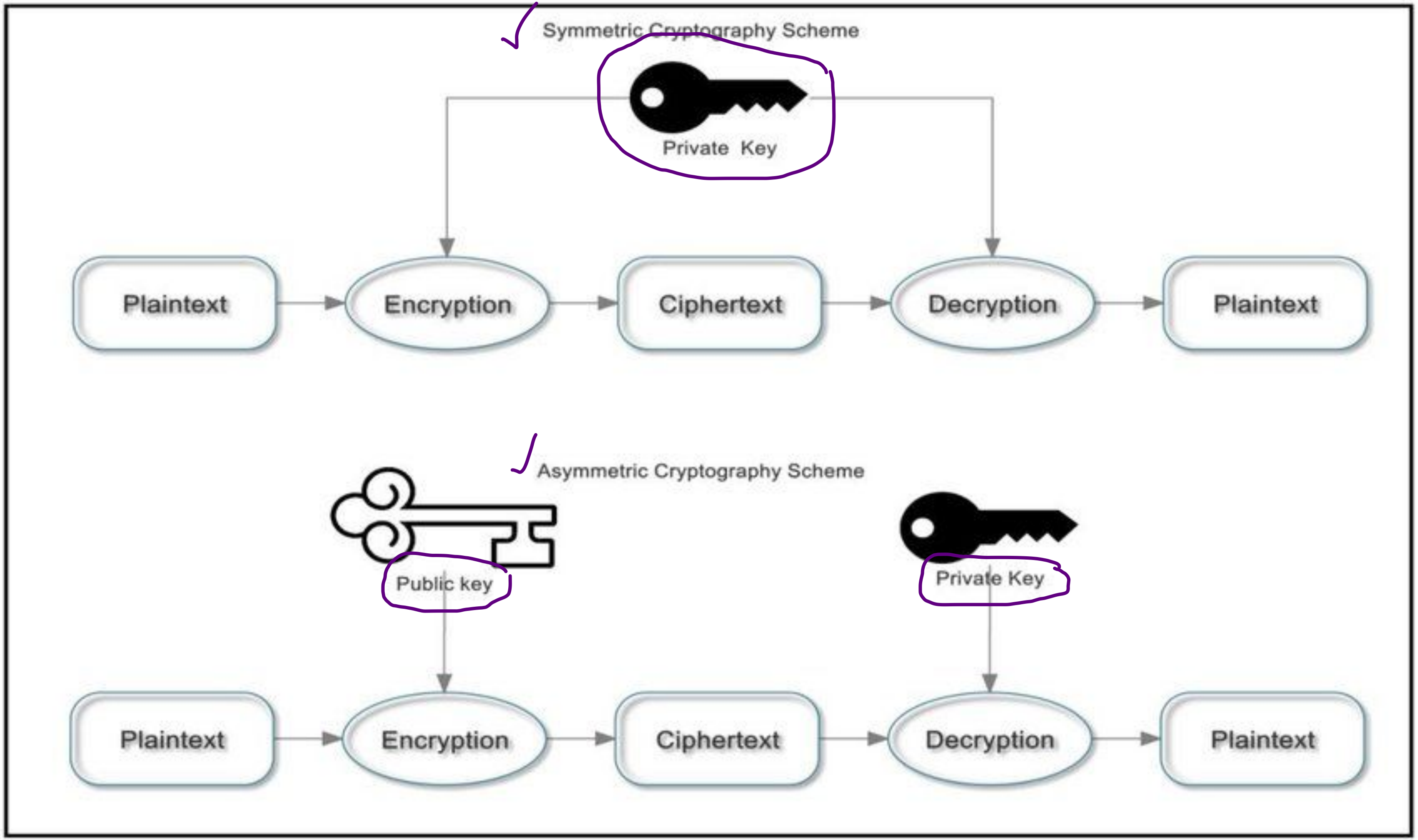
Types of Encryption



✓ Symmetric Cryptography Scheme

Private Key

Plaintext → Encryption → Ciphertext → Decryption → Plaintext

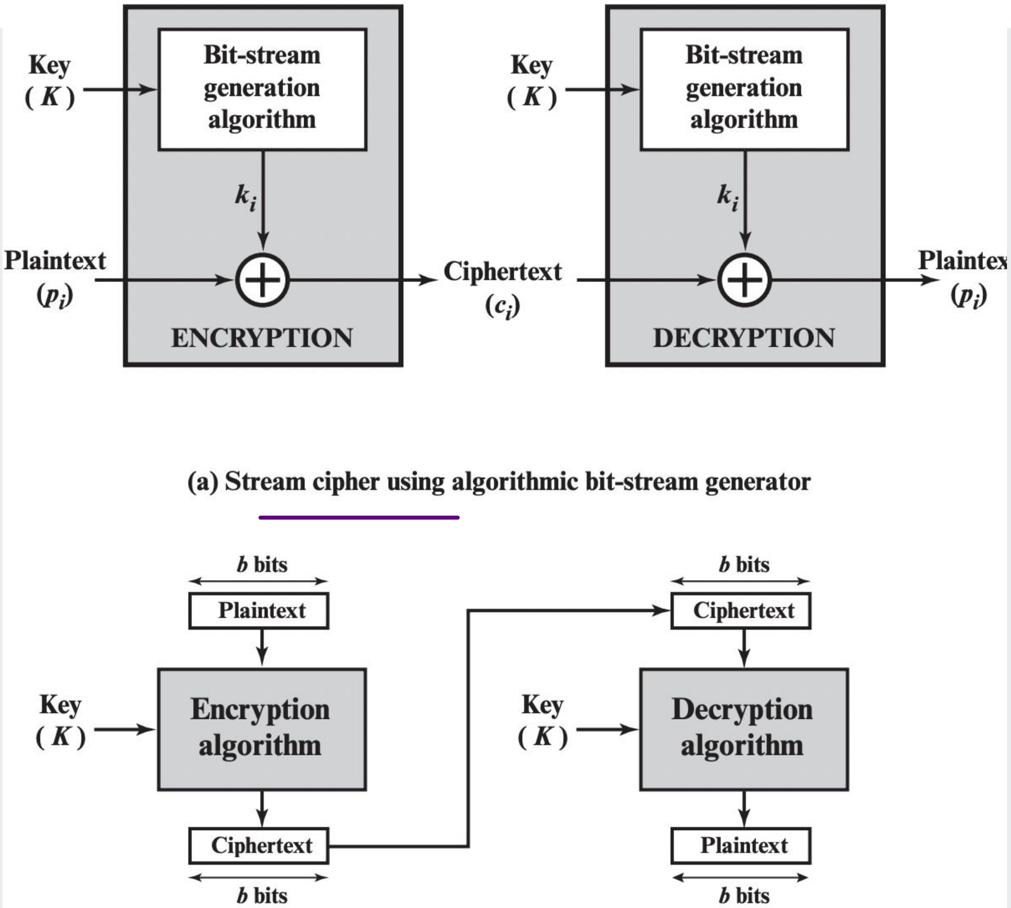
✓ Asymmetric Cryptography Scheme

Public key

Private Key

Plaintext → Encryption → Ciphertext → Decryption → Plaintext

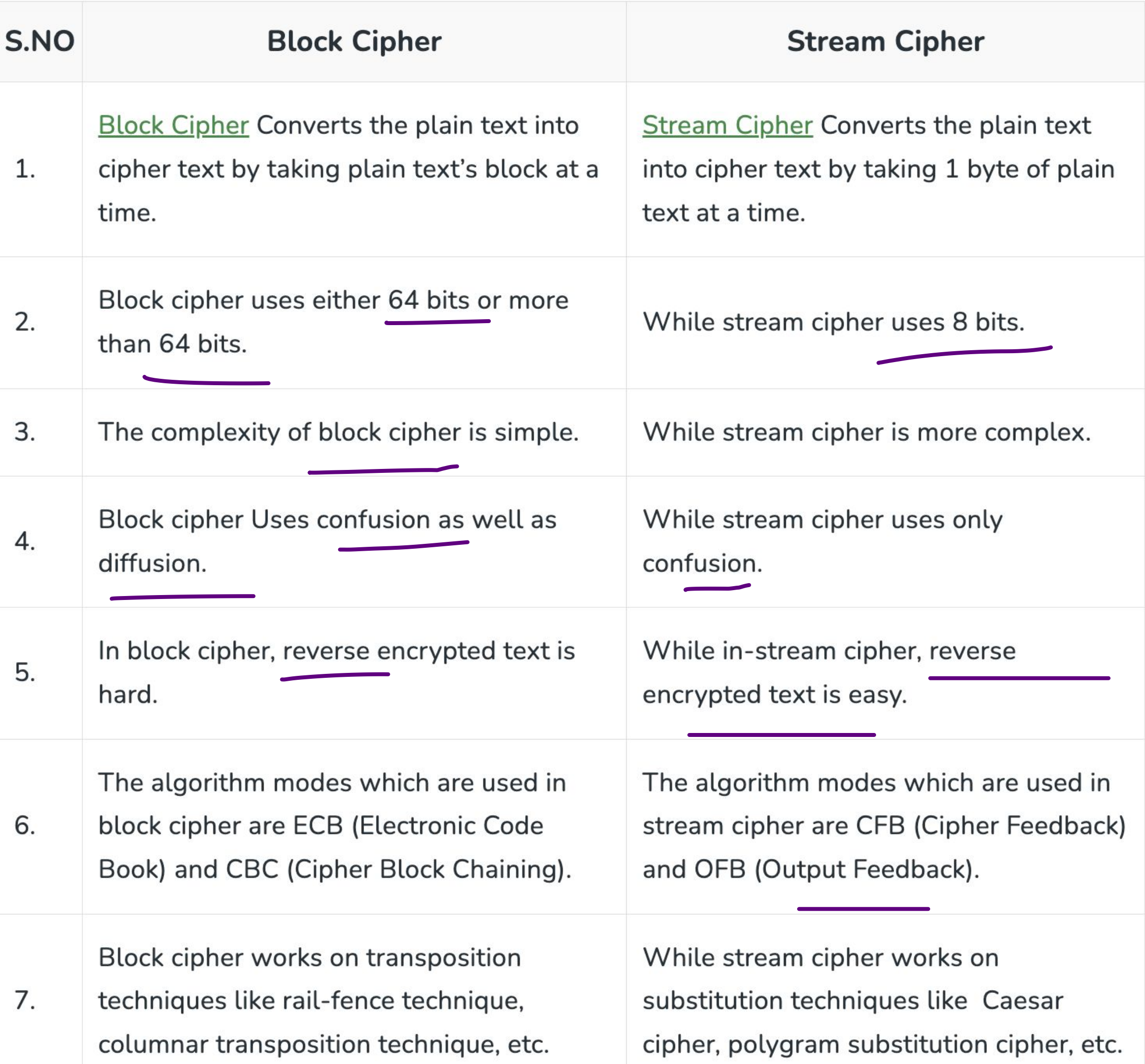
B



(a) Stream cipher using algorithmic bit-stream generator

✓

(b) Block cipher



S.NO	Block Cipher	Stream Cipher
1.	Block Cipher Converts the plain text into cipher text by taking plain text's block at a time.	Stream Cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.
2.	Block cipher uses either 64 bits or more than 64 bits.	While stream cipher uses 8 bits.
3.	The complexity of block cipher is simple.	While stream cipher is more complex.
4.	Block cipher Uses confusion as well as diffusion.	While stream cipher uses only confusion.
5.	In block cipher, reverse encrypted text is hard.	While in-stream cipher, reverse encrypted text is easy.
6.	The algorithm modes which are used in block cipher are ECB (Electronic Code Book) and CBC (Cipher Block Chaining).	The algorithm modes which are used in stream cipher are CFB (Cipher Feedback) and OFB (Output Feedback).
7.	Block cipher works on transposition techniques like rail-fence technique, columnar transposition technique, etc.	While stream cipher works on substitution techniques like Caesar cipher, polygram substitution cipher, etc.

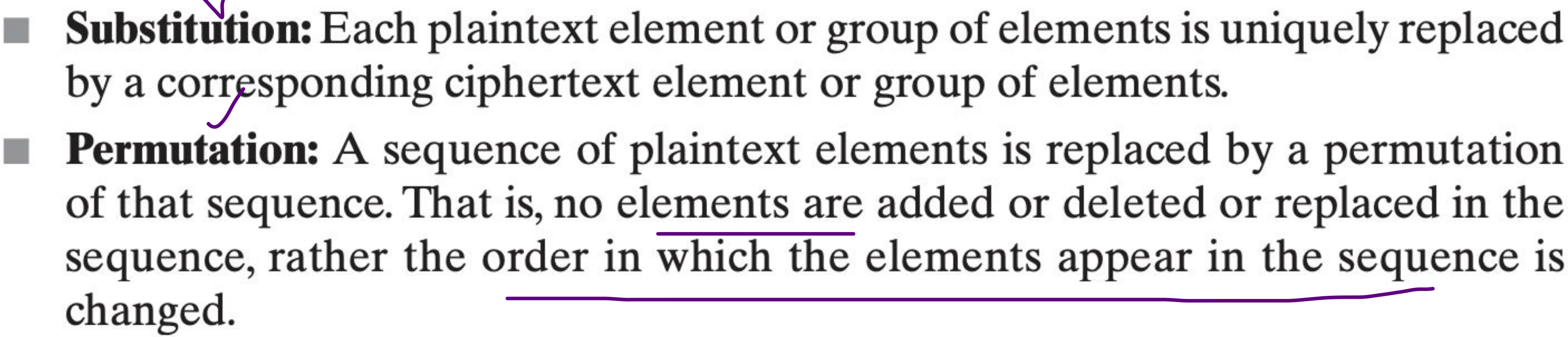
LIKE

COMMENT

SHARE

SUBSCRIBE

Feistal Cipher Basics



- **Substitution:** Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.
- **Permutation:** A sequence of plaintext elements is replaced by a permutation of that sequence. That is, no elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed.

Plain Text	MONKEY
Substitution (Replacing)	NPOLFZ
Permutation(Rearranging)	ONKEYM

Diffusion Vs Confusion (To prevent cryptanalysis)

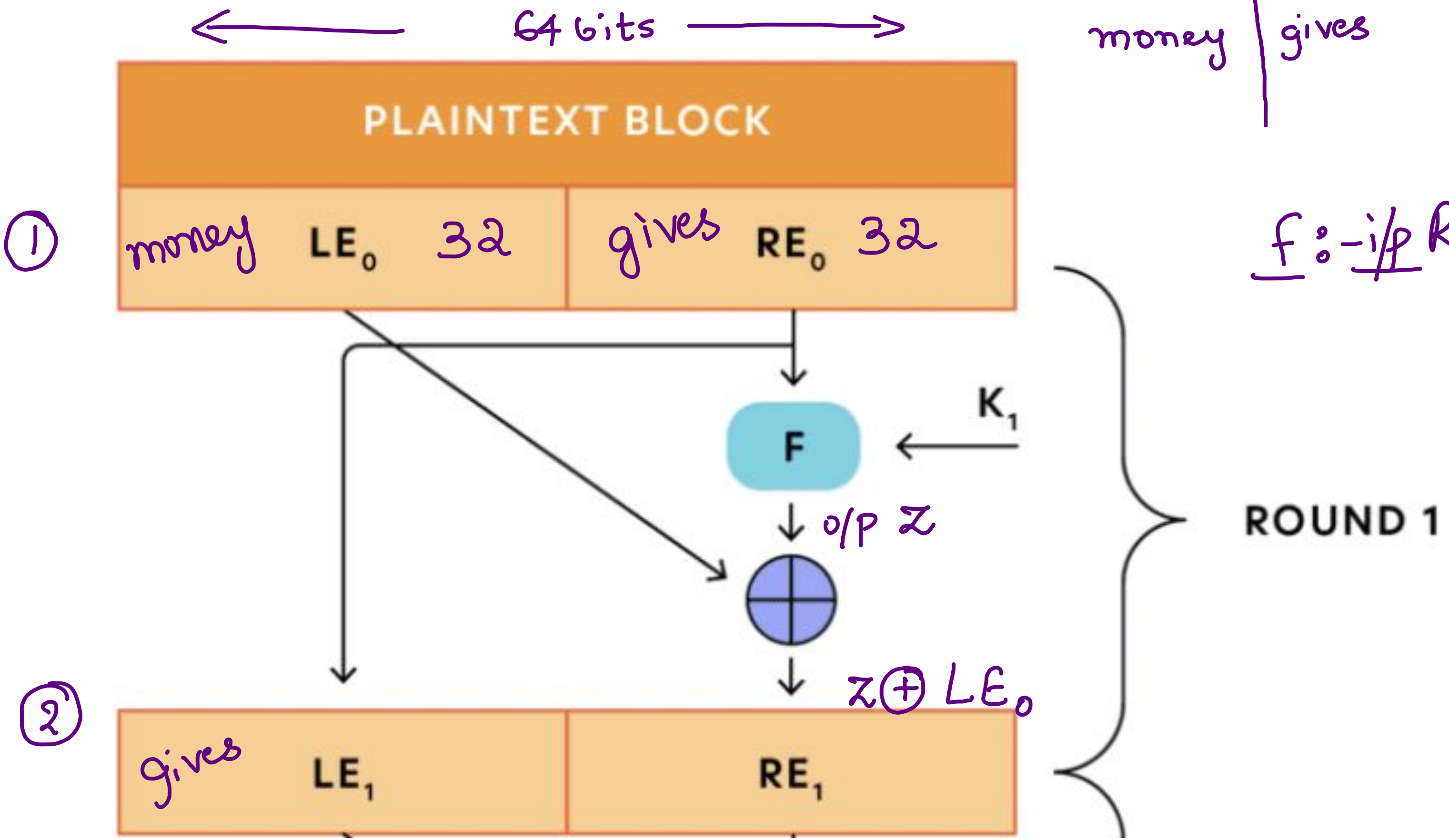
mon

↳ abcdef

- In **diffusion**, the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext.
- This is achieved by having each plaintext digit affect the value of many ciphertext digits; generally, this is equivalent to having each ciphertext digit be affected by many plaintext digits.

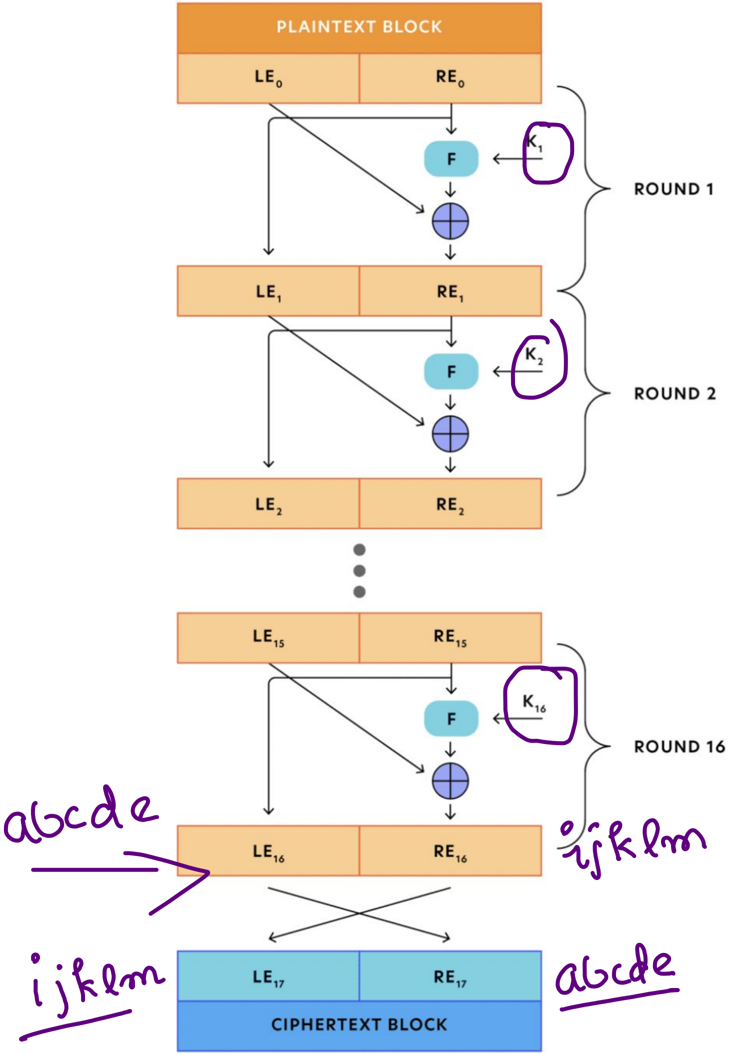
- **Confusion** seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key

Single Round of Fiestel Encryption



money | gives

f :- i/p Right block
+
key

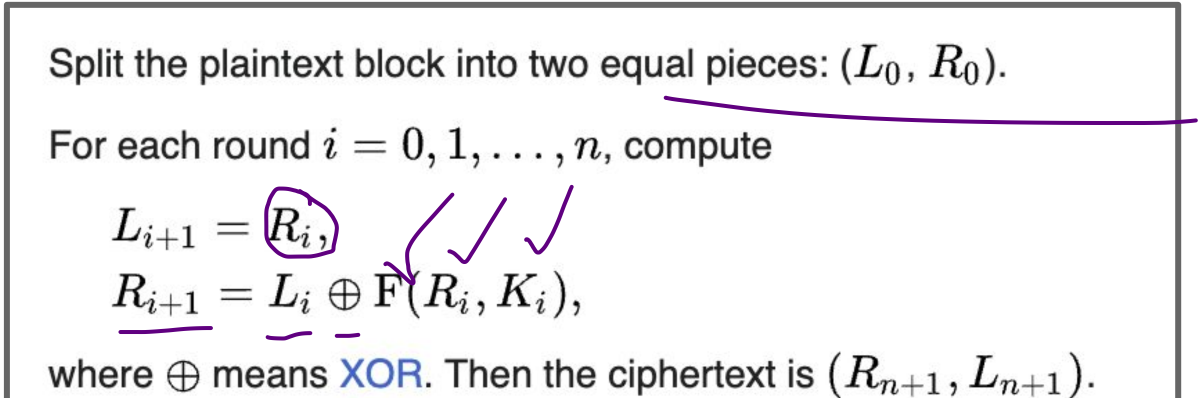


K → key

K → K_1, K_2, K_3, . . ., K_{16} unique

Key Points

1. Inputs - plaintext block of length 2w bits and a key K.
2. The plaintext block is divided into two halves,LE_0 and RE_0.
3. The two halves of the data pass through n rounds of processing and then combine to produce the ciphertext block.
4. Each round i has as inputs LE_{i-1} and RE_{i-1} derived from the previous round, as well as a subkey K_i derived from the overall K.
5. Each round has a different key.
6. All rounds have the same structure.



Split the plaintext block into two equal pieces: (L_0, R_0).

For each round $i = 0, 1, \dots, n$, compute

$$L_{i+1} = \boxed{R_i},$$
$$\underline{R_{i+1}} = \underline{L_i} \oplus \mathrm{F}(R_i, K_i),$$

where $\oplus$ means XOR. Then the ciphertext is (R_{n+1}, L_{n+1}).

Main Parameters

1. **Block size -** Larger size means better security
2. **Key size:** Larger key size means greater security but may decrease encryption/ decryption speed.
3. **Number of rounds:** The essence of the Feistel cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. A typical size is 16 rounds.
4. **Subkey generation algorithm:** Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.
5. **Round function F:** Again, greater complexity generally means greater resistance to cryptanalysis.

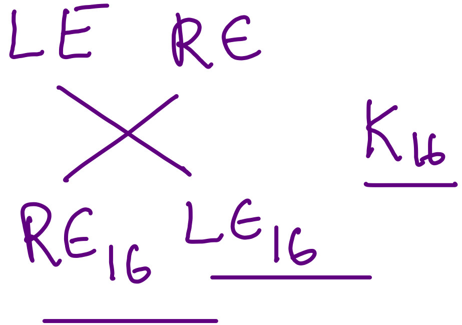
LIKE

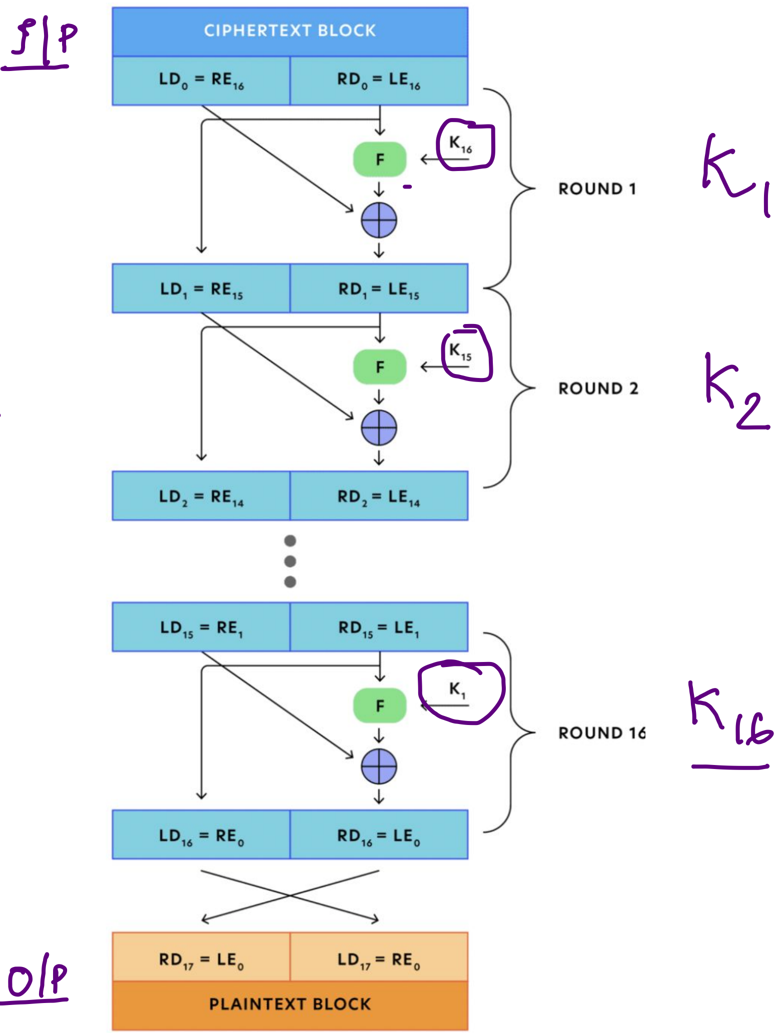
COMMENT

SHARE

SUBSCRIBE

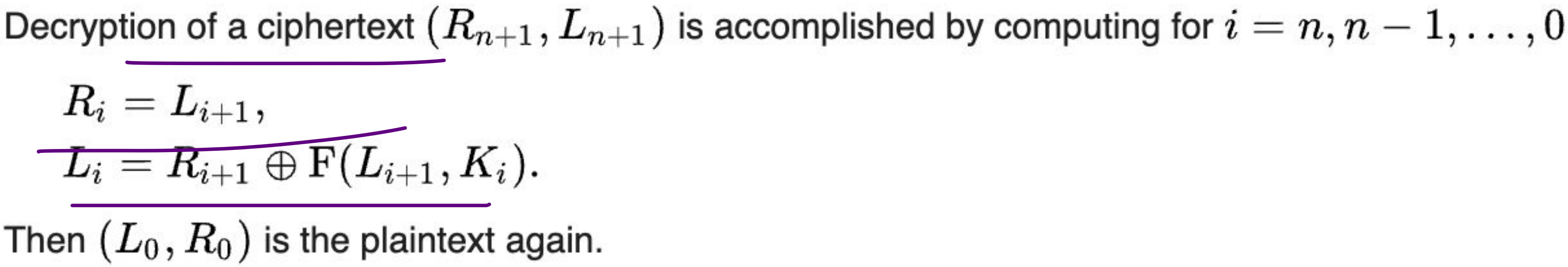
Feistel Cipher Decryption





$$L_{i+1} = R_i$$

$$R_{i+1} = L_i \oplus F(R_{i+1}, K_i)$$



Decryption of a ciphertext (R_{n+1}, L_{n+1}) is accomplished by computing for $i = n, n-1, \ldots, 0$

$$R_i = L_{i+1},$$
$$L_i = R_{i+1} \oplus \mathrm{F}(L_{i+1}, K_i).$$

Then (L_0, R_0) is the plaintext again.

LIKE

COMMENT

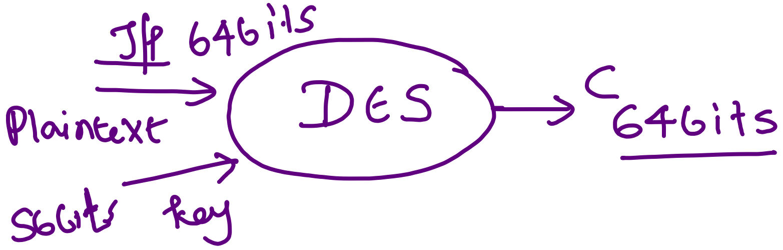
SHARE

SUBSCRIBE

X X

Data Encryption Standard (DES)

Key Points



1. Symmetric Encryption Algorithm ✓
2. DES is a block cipher and encrypts data in blocks of size of **64 bits** each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext.
3. The same algorithm and key are used for encryption and decryption, with minor differences.
4. The key length is **56 bits**.

DES Encryption

abc

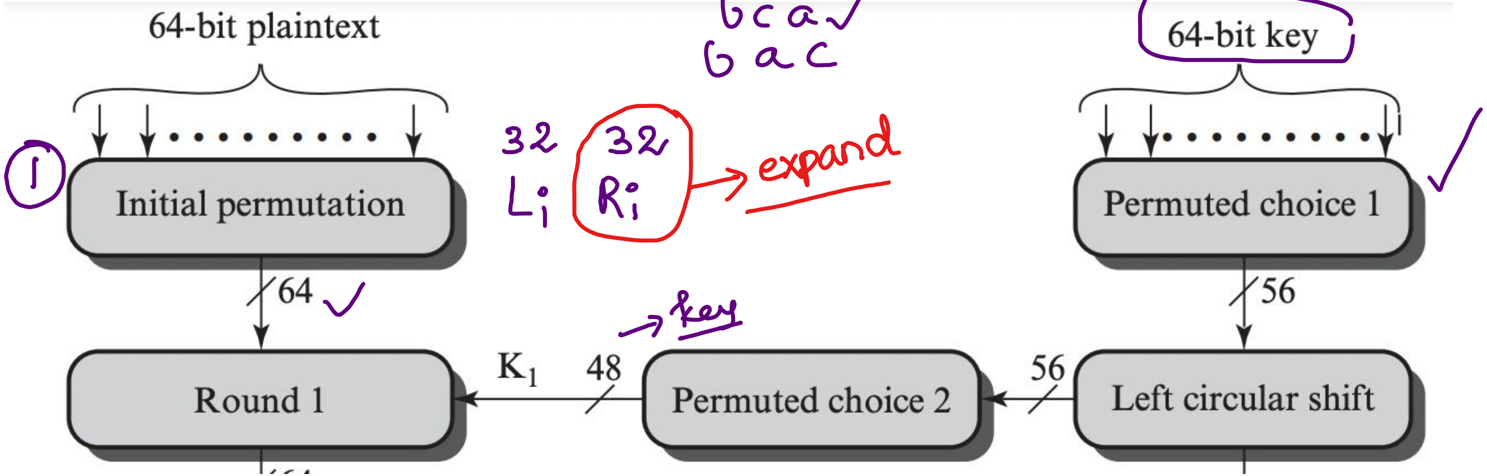
acb

bca ✓

bac

$L_{i+1} = R_i$

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



64-bit plaintext

Initial permutation

64

Round 1

K_1

48

Permuted choice 2

56

Left circular shift

56

Permuted choice 1

64-bit key

8 x 8 byte

Feistel Function

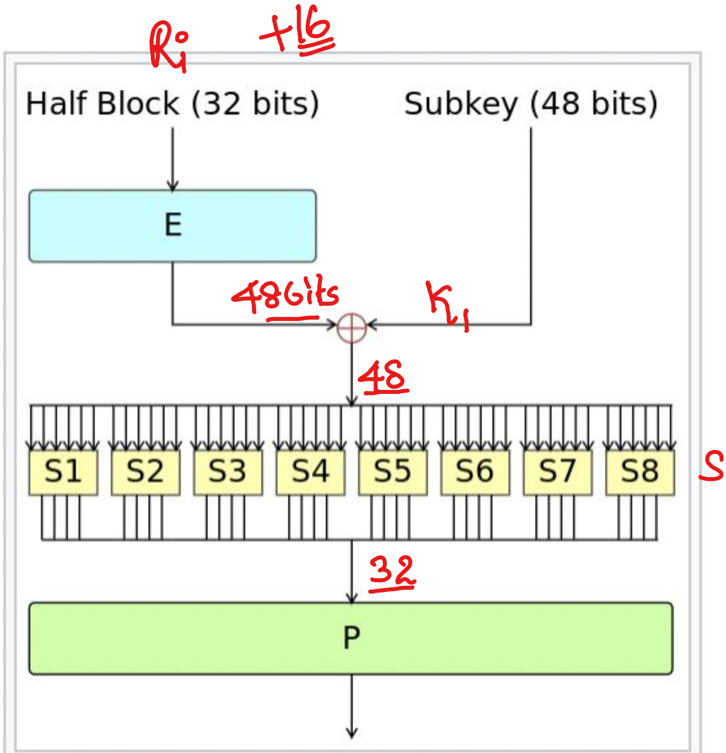


Figure 2—The Feistel function (F-function) of DES

Substitution table

1 0 1 1 ✓   0 0 0 0   1 1 1 1 ✓

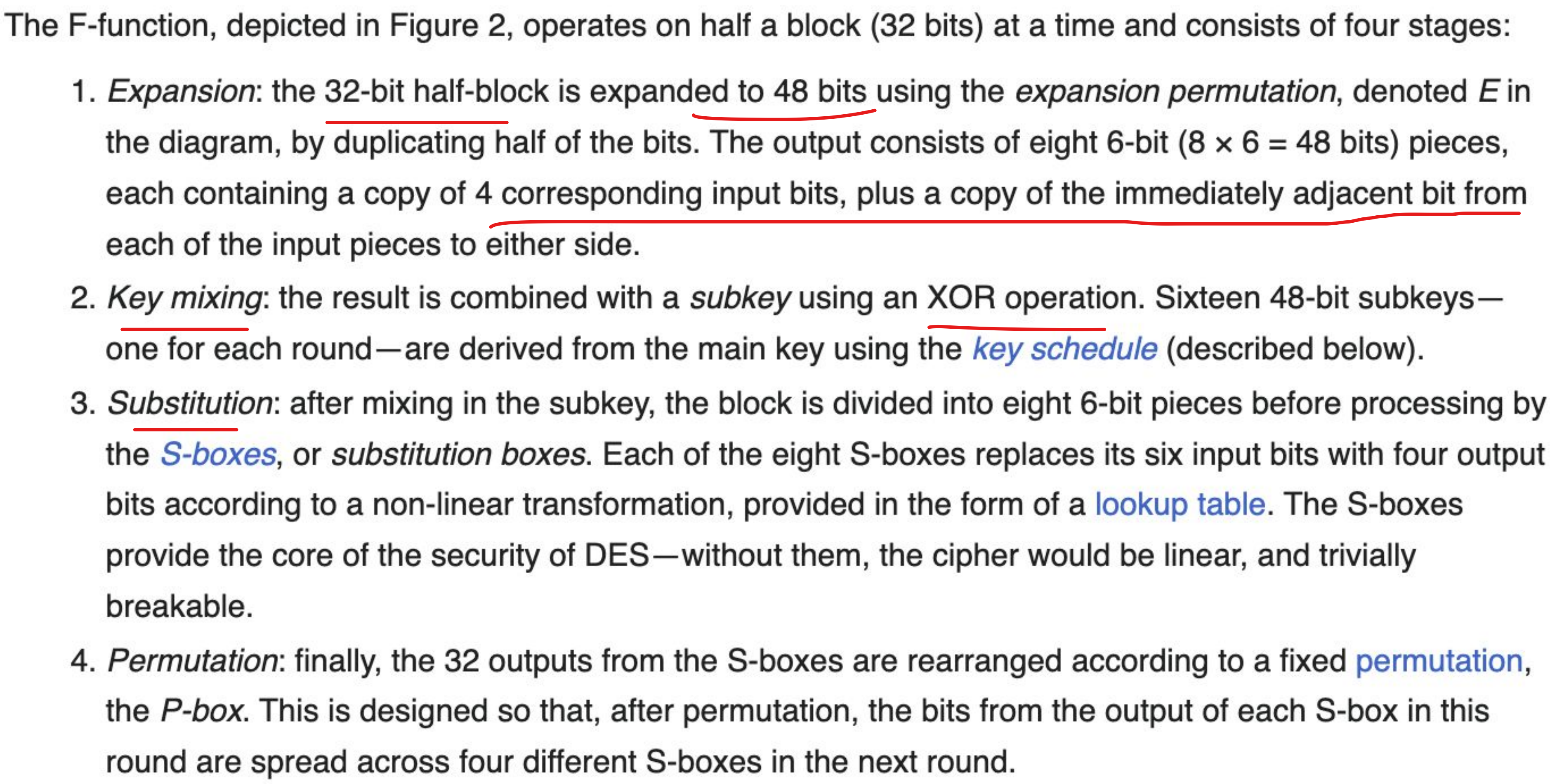
1 1 1 1   1 0 1 1 ✓   0 0 0 0   6bits

0 0 0 0   1 1 1 1   1 0 1 1

1 0 1 1   0 0 0 0   1 1 1 1

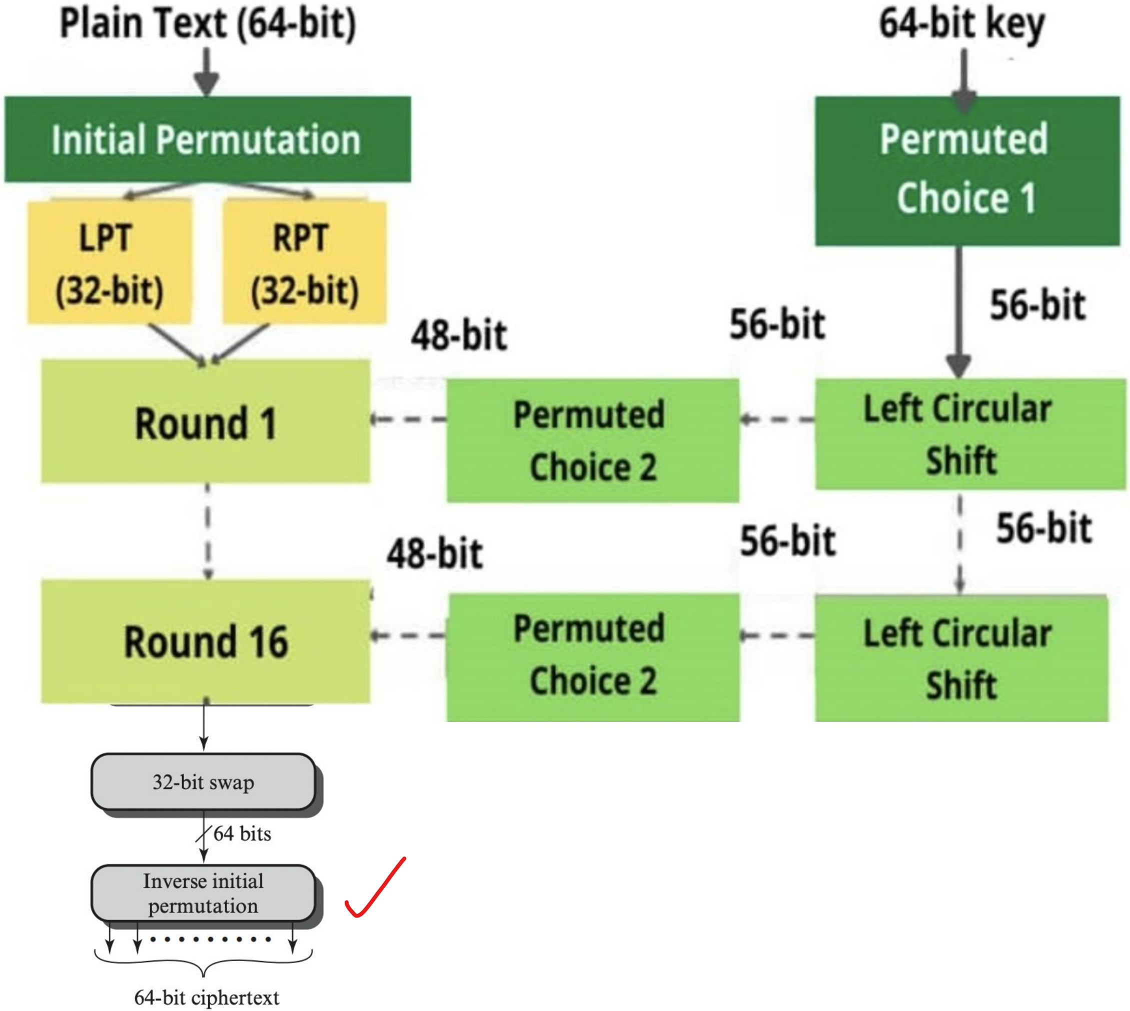
4 → 6 bits

$\frac{32}{4} \Rightarrow 8 \times 2 = 16$bits



The F-function, depicted in Figure 2, operates on half a block (32 bits) at a time and consists of four stages:

1. *Expansion*: the 32-bit half-block is expanded to 48 bits using the *expansion permutation*, denoted *E* in the diagram, by duplicating half of the bits. The output consists of eight 6-bit (8 × 6 = 48 bits) pieces, each containing a copy of 4 corresponding input bits, plus a copy of the immediately adjacent bit from each of the input pieces to either side.
2. *Key mixing*: the result is combined with a *subkey* using an XOR operation. Sixteen 48-bit subkeys—one for each round—are derived from the main key using the *key schedule* (described below).
3. *Substitution*: after mixing in the subkey, the block is divided into eight 6-bit pieces before processing by the *S-boxes*, or *substitution boxes*. Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation, provided in the form of a lookup table. The S-boxes provide the core of the security of DES—without them, the cipher would be linear, and trivially breakable.
4. *Permutation*: finally, the 32 outputs from the S-boxes are rearranged according to a fixed permutation, the *P-box*. This is designed so that, after permutation, the bits from the output of each S-box in this round are spread across four different S-boxes in the next round.



Plain Text (64-bit)

Initial Permutation

LPT (32-bit)

RPT (32-bit)

Round 1

48-bit

Permuted Choice 2

56-bit

64-bit key

Permuted Choice 1

56-bit

Left Circular Shift

56-bit

48-bit

56-bit

Round 16

Permuted Choice 2

Left Circular Shift

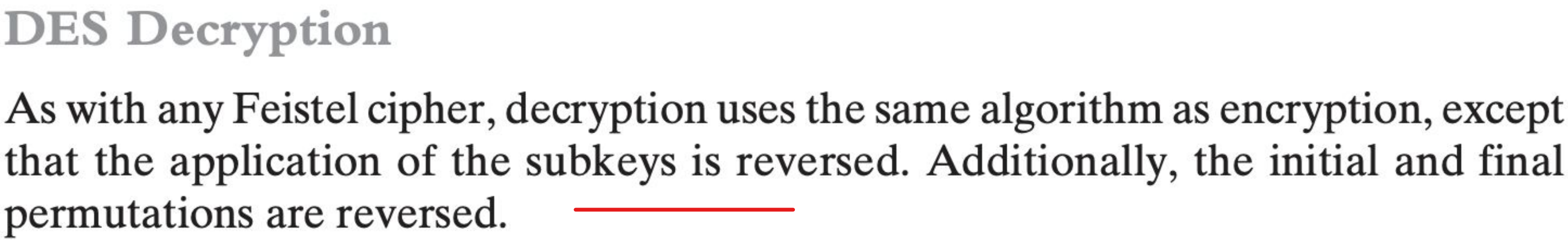
32-bit swap

64 bits

Inverse initial permutation

✓

64-bit ciphertext



DES Decryption

As with any Feistel cipher, decryption uses the same algorithm as encryption, except that the application of the subkeys is reversed. Additionally, the initial and final permutations are reversed.

Avalanche Effect

- A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the ciphertext.
- In particular, a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext.

LIKE

COMMENT

SHARE

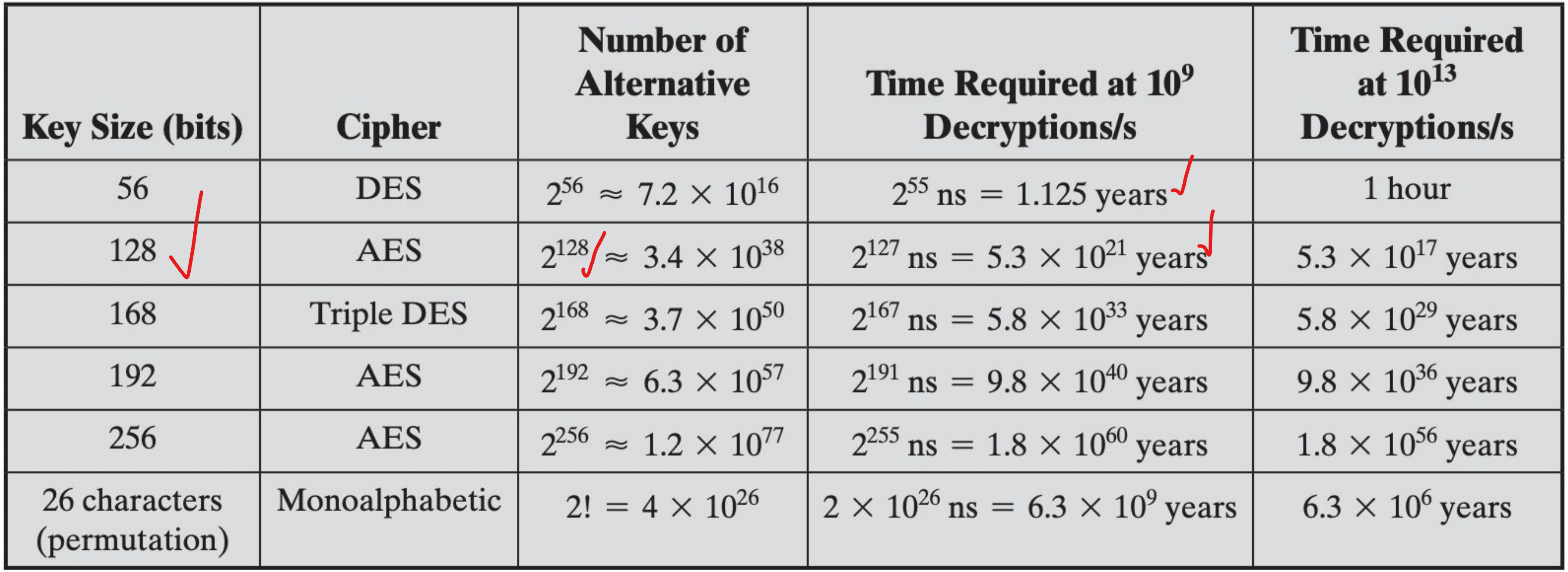
SUBSCRIBE

1

Strength Of DES - Use of 56 bit keys

2^{56} ✓

Table 4.5 Average Time Required for Exhaustive Key Search



Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 Decryptions/s	Time Required at 10^{13} Decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years ✓	1 hour
128 ✓	AES	2^{128} ✓ $\approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years ✓	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years
26 characters (permutation)	Monoalphabetic	$2! = 4 \times 10^{26}$	2×10^{26} ns = 6.3×10^{9} years	6.3×10^{6} years

2. Use of Substitution Boxes

- The focus of concern has been on the eight substitution tables, or S-boxes, that are used in each iteration.
- Because the design criteria for these boxes, and indeed for the entire algorithm, were not made public, there is a suspicion that the boxes were constructed in such a way that cryptanalysis is possible for an opponent who knows the weaknesses in the S-boxes.
- Despite all this no one has so far succeeded in discovering the supposed fatal weaknesses in the S-boxes.

3. Resilient against Timing Attack

$S \xrightarrow[X]{} R$

A timing attack is one in which information about the key or the plaintext is obtained by observing how long it takes a given implementation to perform decryptions on various ciphertexts.

A timing attack exploits the fact that an encryption or decryption algorithm often takes slightly different amounts of time on different inputs.

LIKE

COMMENT

SHARE

SUBSCRIBE

Block Cipher Design Principles

1 **Number of Rounds (More rounds more secure)**

- The cryptographic strength of a Feistel cipher derives from three aspects of the design: the number of rounds, the function F, and the key schedule algorithm. Let us look first at the choice of the number of rounds.
- The greater the number of rounds, the more difficult it is to perform cryptanalysis, even for a relatively weak F.
- In general, the criterion should be that the number of rounds is chosen so that known cryptanalytic efforts require greater effort than a simple brute-force key search attack. This criterion was certainly used in the design of DES.

Block Cipher Design Principles

2 Design of Feistel Function F

- It must be difficult to **“unscramble”** the substitution performed by F. One obvious criterion is that F be nonlinear.
- have good **avalanche** properties (Strict Avalanche Criterion)
- **Bit independence criterion (BIC),** which states that output bits j and k should change independently when any single input bit i is inverted for all i, j, and k. The SAC and BIC criteria appear to strengthen the effectiveness of the confusion function.

Block Cipher Design Principles

K / K_1

⋮

K_{15}

3) Key Schedule Algorithm

- With any Feistel block cipher, the key is used to generate one subkey for each round. In general, we would like to select subkeys to maximize the difficulty of deducing individual subkeys and the difficulty of working
- at minimum, the key schedule should guarantee key/ciphertext Strict Avalanche Criterion and Bit Independence Criterion.

LIKE

COMMENT

SHARE

SUBSCRIBE