09 (10) September, 2024

Data Encryption Standard
DES: encryption, key generation
AES Structure
AES Transformation

(mostly taken from William Stallings, *Cryptography and Network Security: Principles and Practices*)

Data Encryption Standard

Data is encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps with the same key are used to reverse the encryption.

In 1999: the 3DES was introduced by the NIST. In essence, repeat the DEA (the algorithm of DES is known as DEA, the Data Encryption Algorithm) 3 times, using 2 or 3 different keys.

DES has the exact structure of a Feistel cipher, except for the initial and final permutations.

Key (56-bit): Initially, the key is passed through a permutation function. Then, for each of the sixteen rounds, a subkey (K_i) is produced by the combination of a left circular shift and a permutation. The permutation function is the same for each round, but a different subkey is produced because of the repeated shifts of the key bits.

We can group the DES algorithm into three phases:

1) 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the ***permuted input***.
2) Phase of 16 rounds, of the same function, which involved both permutation and substitution functions. The output of the last round (16th) consists of 64-bits that are a function of the input plaintext and the key.
3) Left and right halves of the output are swapped to produce the *pre-output*. Then, the *pre-output* is passed through a permutation (IP^{-1}) that is the inverse of the initial permutation function, to produce the 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.

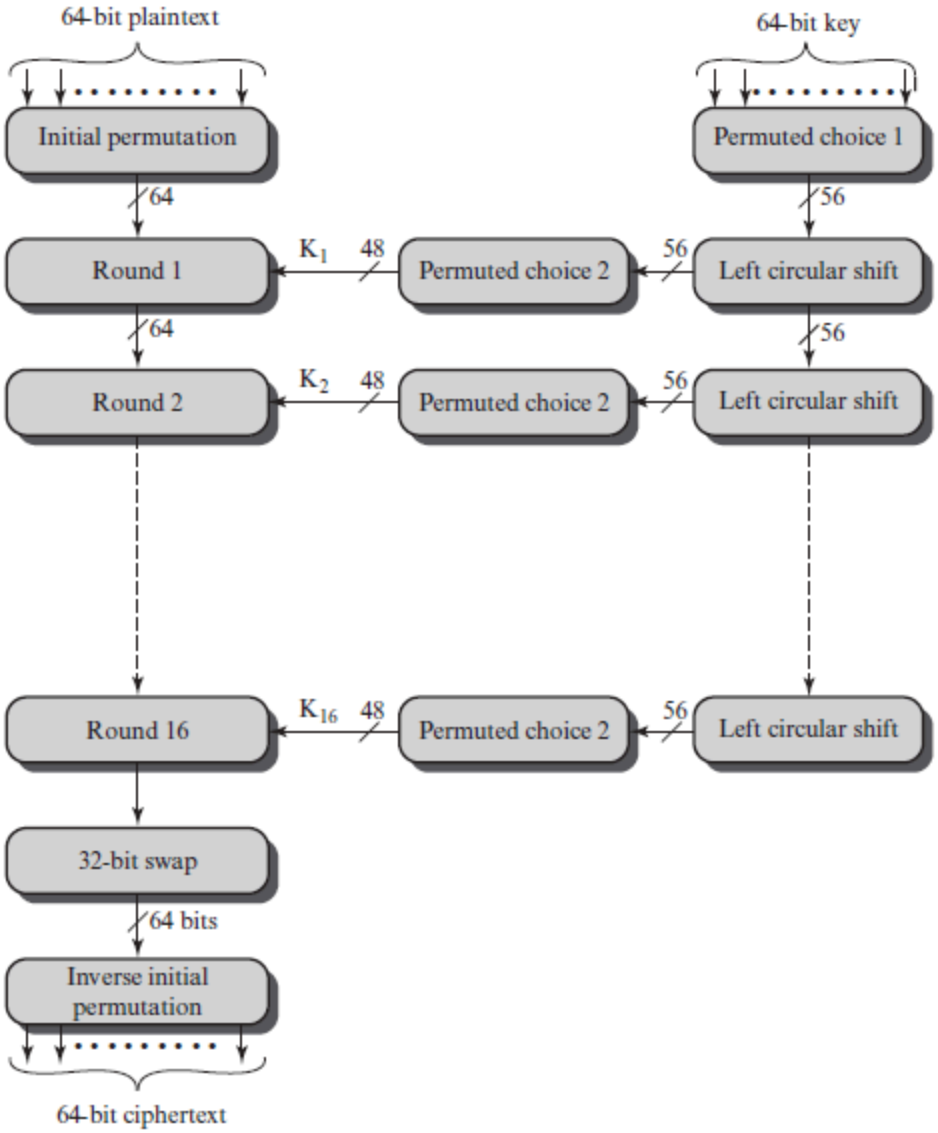


Figure 4.5 General Depiction of DES Encryption Algorithm

Table 4.2 of the text (Stallings, 7ed, Cryptography and Network Security, shows an example of DES. It tries to show the values of the L_i and R_i and the keys K_1 to K_{16} across the IP, all the 16 rounds, and then finally the IP^{-1}.

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. So, a one bit change in the key/plaintext should result in many bits being changed in the ciphertext.

While designing a block cipher, there are three critical aspects: the number of rounds, design of the function F, and key scheduling.

Table 4.5 shows the average time required for Exhaustive Key Search for various cipher mechanisms. This should simply serve to help us to understand the strengths of the various encryption schemes.

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

AES (Advanced Encryption Standard)

AES is a block cipher with block length of 128 bits. AES allows for 3 different key lengths: 128, 192 and 256 bits. We assume a key length of 128 bits, otherwise the key schedule differs.

Encryption consists of 10 rounds of processing for 128 bit keys, 12 rounds for 192 bit keys, and 14 rounds for 256 bit keys.

Except for the last round in each case, all other rounds are identical. Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. Note: the order in which these 4 steps are executed is different for encryption and decryption.

To appreciate the use of “row” and “column” in the previous point, you need to think of the input 128 bit block as consisting of a 4*4 array of bytes, arranged as follows:

$byte_0$ $byte_4$ $byte_8$ $byte_{12}$
$byte_1$ byte5 $byte_9$ $byte_{13}$
$byte_2$ $byte_6$ $byte_{10}$ $byte_{14}$
$byte_3$ $byte_7$ $byte_{11}$ $byte_{15}$

Note that the first 4 bytes of a 128-but input block occupy the first column of a 4*4 array of bytes. The next four bytes occupy the 2nd column, and so on.

The 4*4 array of bytes shown above is referred to as the state array in AES.

AES also has the notion of a ***word***. A word consists of 4 bytes, i.e., 32 bits. Therefore, each column of the state array is a word, as is each row.

Each round of processing works on the input ***state array*** and produces an output ***state array***. The output ***state array*** produced by the last round is rearranged into a 128-bit output block.

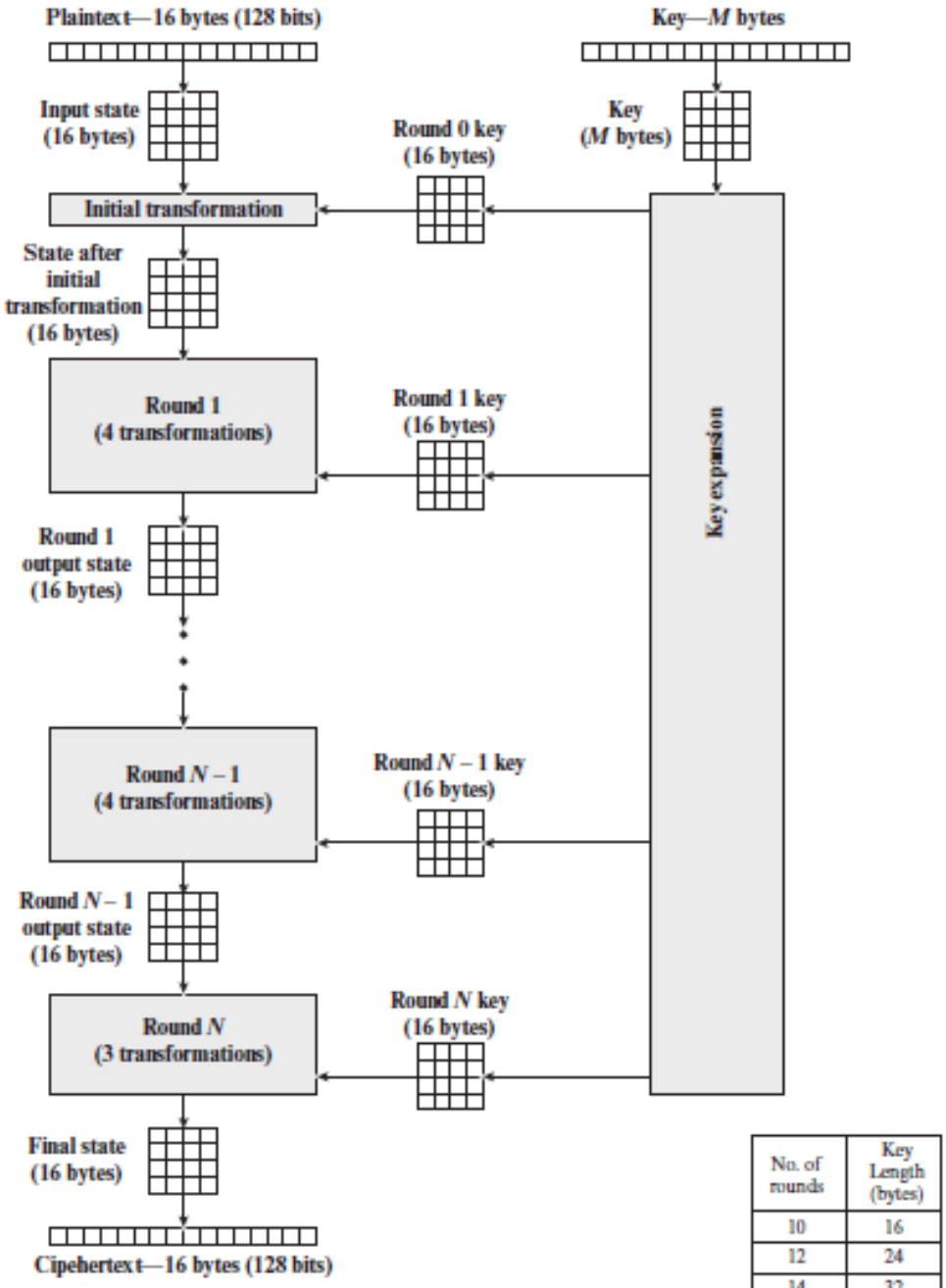
Unlike DES, the decryption algorithm differs substantially from the encryption algorithm. Although very similar steps are used in encryption and decryption, their implementations are not identical and the order in which the steps are involved is different.

AES (standard notified by NIST, 2001) is a slight variation of the Rijndael cipher invented by two Belgian cryptographers Joan Daemen and Vincent Rijmen.

While DES was based on the Feistel network, AES uses a substitution-permutation network in a more general sense. Each round of processing in AES involves byte-level substitutions followed by word-level permutations.

In general, DES also involves substitutions and permutations, except that the permutations are based on the Feistel notion of dividing the input block into 2 halves, processing each half separately, and then swapping the two halves.

DES is a bit-oriented cipher, AES is a byte-oriented cipher, this makes AES more convenient and fast for software implementation.



No. of rounds	Key Length (bytes)
10	16
12	24
14	32

Figure 6.1 AES Encryption Process