**Symmetric Encryption:**

Encryption methodologies that require the same **secret key** to encipher and decipher the message are using what is called **private key encryption** or **symmetric encryption**.

There are a number of popular symmetric encryption cryptosystems. One of the most widely known is the **Data Encryption Standard (DES),** which was developed by IBM and is based on the company’s Lucifer algorithm, which uses a key length of 128 bits.

The successor to 3DES is the Advanced Encryption Standard (AES). AES is a federal information processing standard (FIPS) that specifies a cryptographic algorithm used within the U.S. government to protect information in federal agencies that are not a part of the national defence infrastructure.

**Asymmetric Encryption**

While symmetric encryption systems use a single key to both encrypt and decrypt a message, asymmetric encryption uses two different but related keys, and either key can be used to encrypt or decrypt the message. If, however, key A is used to encrypt the message, only key B can decrypt it, and if key B is used to encrypt a message, only key A can decrypt it.

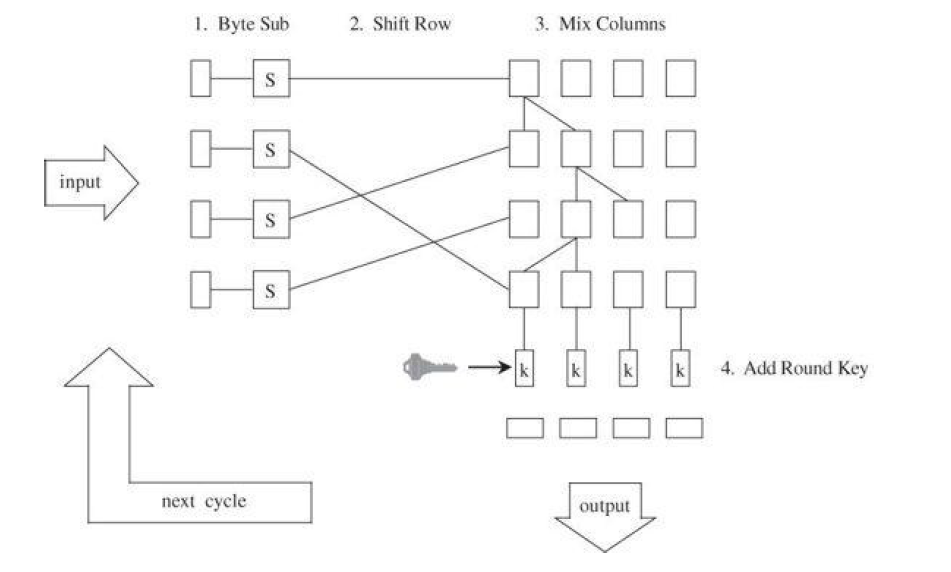
The algorithm consists of 10, 12 or 14 cycles, for a 128-, 192-, or 256-bit key, respectively. Each cycle (called a “round” in the algorithm) consists of four steps.

• **Byte substitution**. This step uses a substitution substituting each byte of a 128- bit block according to a substitution table. This is a straight diffusion operation.

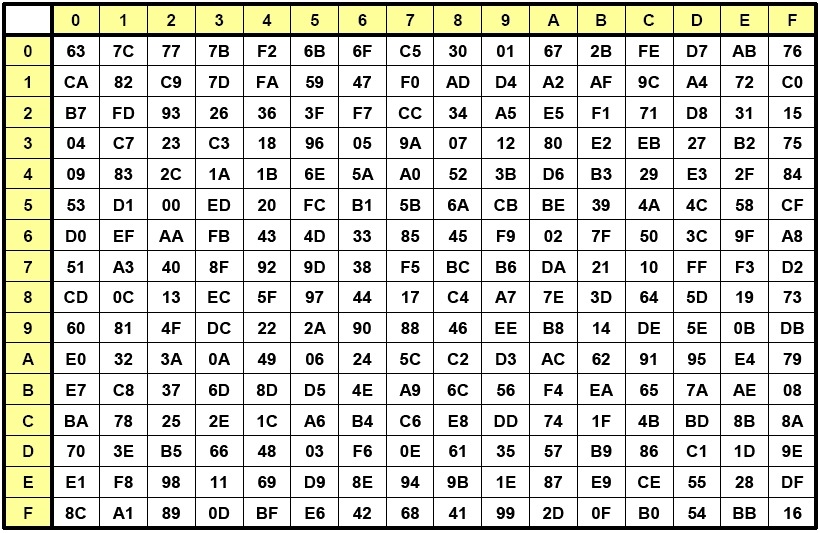
• **Shift row**. Certain bits are shifted to other positions. This is a straight confusion operation.

• **Mix column**. This step involves shifting left and XORing bits with themselves. These operations implement both confusion and diffusion.

• **Add subkey**. Here, a portion of the key unique to this cycle is XORed with the cycle result. This operation delivers confusion and incorporates the key.



**Structure of AES**



00 04 08 19

01 05 09 19

02 06 0A 19

03 07 0B 19

00 04 08 19 2 3 1 1 A B C D

05 09 19 01 1 2 3 1 E F G H

0A 19 02 06 1 1 2 3 I J K L

19 03 07 0B 3 1 1 2 M N O P

ANS=00\*02 ⊕ 04\*01 ⊕ 08\*01 ⊕ 19\*03

16\*8=128=4X4

192=4X6

256=4X8

192/8=24

256/8=32

A B C D

E F G H

I J K L

M N O P

01 02 03 04

05 06 07 08

09 10 11 12

13 14 15 16

K2=W1’(W2⊕ W1’)(W3⊕W1’)(W4⊕W1’))

K3=W2’(W3⊕ w2’)

introduction

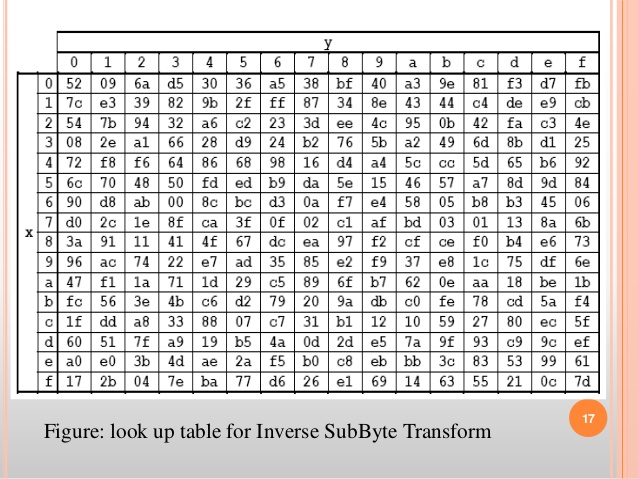
08

0d

14

12

25=19



A=00

B=01

C=02

D=04

ABCDEFGHIJKL

00 01 02 03 04 05 06 07 08 09 10 11 25 25 25 25

00 01 02 03 04 05 06 07 08 09 0A 0B 19 19 19 19