CLASSICAL ENCRYPTION TECHNIQUES

BY

DR. ZIA UR REHMAN

ONE-TIME PAD

- Joseph Mauborgne, proposed an improvement to the Vernam cipher that yields the ultimate in security. He suggested using a random key that is as long as the message, so that the key need not be repeated.
- The key is to be used to encrypt and decrypt a single message, and then is discarded. Each new message requires a new key of the same length as the new message. Such a scheme, known as a **one-time pad**.
- It produces random output that bears no statistical relationship to the plaintext.
- The cipertext contains no information whatsoever about the plaintext, there is simply no way to **break the code**

ONE-TIME PAD

- Consider the following ciphertext

```
ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
```

We now show two different decryptions using two different keys:

```
ciphertext:  ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:         pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
plaintext:   mr mustard with the candlestick in the hall

ciphertext:  ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:         pftgpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt
plaintext:   miss scarlet with the knife in the library
```

ONE-TIME PAD – FUNDAMENTAL DEFICULTIES

- There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
- Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

TRANSPOSITION CIPHER

- A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.
- The example of such cipher is Rail Fence cipher, e.g.
- to encipher the message "meet me after the toga party" with a rail fence of depth 2, we write the following:

```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

- The encrypted form
- MEMATRHTGPRYETEFETEOAAT

TRANSPOSITION CIPHER

- A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.

```
Key:           4 3 1 2 5 6 7
Plaintext:     a t t a c k p
               o s t p o n e
               d u n t i l t
               w o a m x y z
Ciphertext:    TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

- The transposition cipher can be made significantly more secure by performing more than one stage of transposition.

TRANSPOSITION CIPHER

- Lets re-transpose the ciphertext:

```
Key:       4 3 1 2 5 6 7
Input:     t t n a a p t
           m t s u o a o
           d w c o i x k
           n l y p e t z
Output:    NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

- To visualize properly, designate the letters in the original plaintext message by the numbers designating their position.

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

TRANSPOSITION CIPHER

- After 1st transposition:

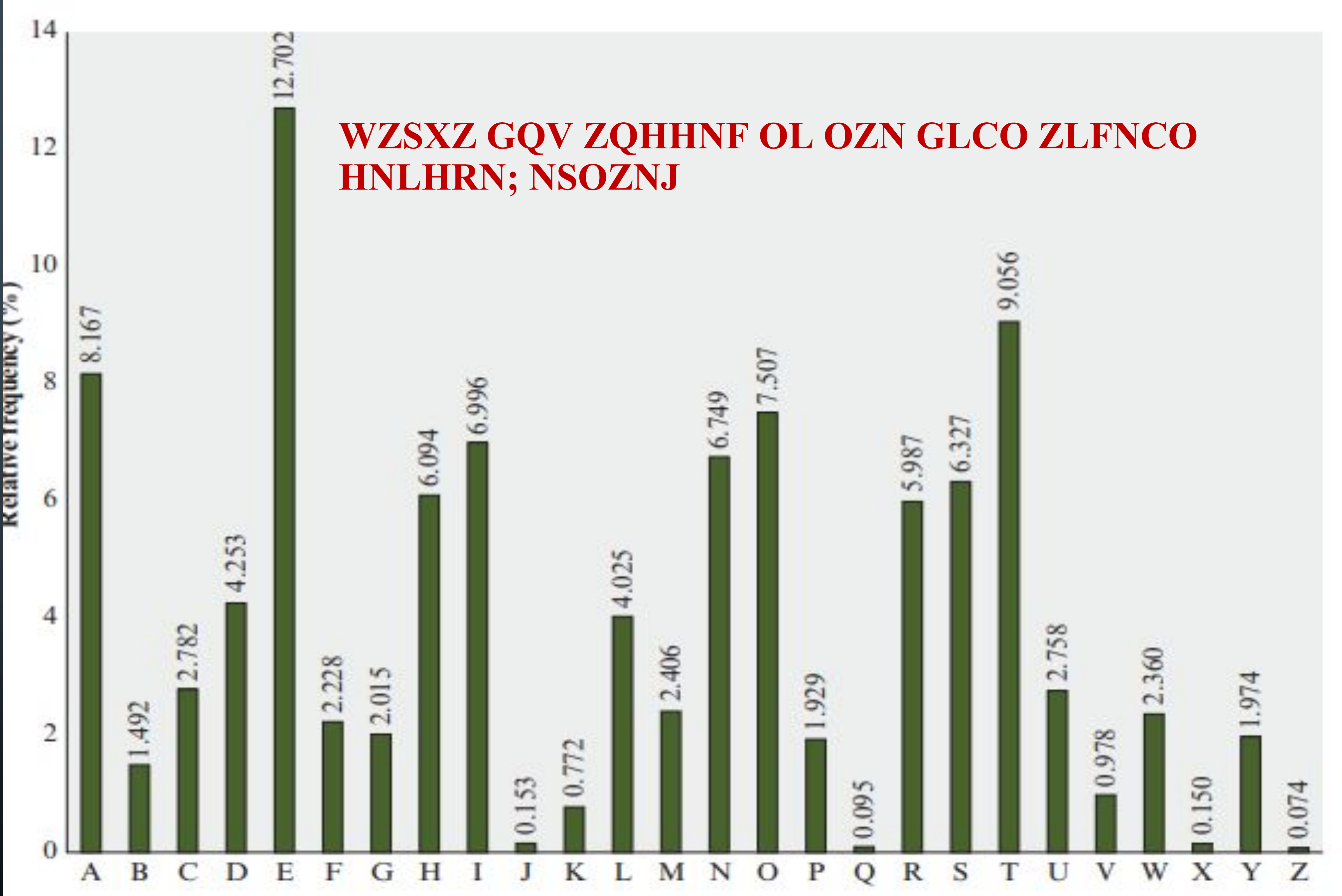
03	10	17	24	04	11	18	25	02	09	16	23	01	08
15	22	05	12	19	26	06	13	20	27	07	14	21	28

- After 2nd transposition:

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

- This is a much less structured permutation and is much more difficult to cryptanalyze.

WZSXZ GQV ZQHHNF OL OZN GLCO ZLFNCO HNLHRN; NSOZNJ



PRODUCT CIPHERS

- Ciphers using substitutions or transpositions are not secure because of language characteristics.
- • hence consider using several ciphers in succession to make harder,
- but:
  - two substitutions make a more complex substitution
  - two transpositions make more complex transposition
  - but a substitution followed by a transposition makes a new much harder cipher
- this is bridge from classical to modern ciphers

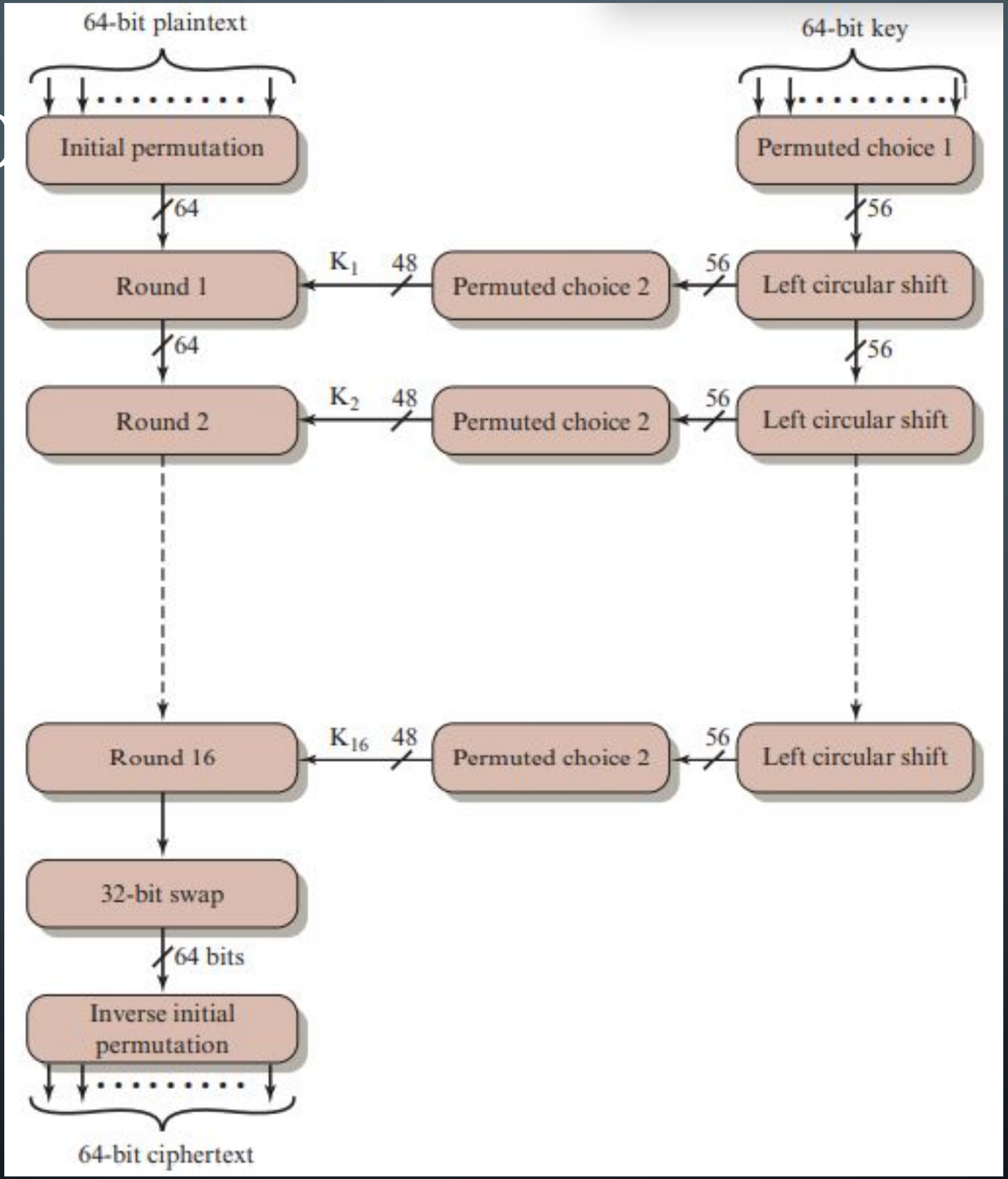
ROTOR CIPHERS

- before modern ciphers, rotor machines were most common complex ciphers in use
- Widely used in WW2
  - German Enigma, Allied Hagelin, Japanese Purple
- Implemented a very complex, varying substitution cipher
- used a series of cylinders, each giving one substitution, which rotated and changed after each letter was encrypted
- with 3 cylinders have 26^3=17576 alphabets

OVERVIEW OF DATA ENCRYPTION STANDARD (DES) ALGO

- DES was issued in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46).
- The algorithm itself is referred to as the Data Encryption Algorithm (DEA).6 For DEA, data are encrypted in 64-bit blocks using a 56-bit key.
- Subsequently Advanced Encryption Algorithm (AES) replaced it in 2001.

DES ALGO



64-bit plaintext
64-bit key
Initial permutation
Permuted choice 1
64
56
Round 1
K_1
48
Permuted choice 2
56
Left circular shift
64
56
Round 2
K_2
48
Permuted choice 2
56
Left circular shift
Round 16
K_{16}
48
Permuted choice 2
56
Left circular shift
32-bit swap
64 bits
Inverse initial permutation
64-bit ciphertext

AES ALGORITHM

- AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications.
- It is most widely used algorithm.
- FINITE FIELD ARITHMETIC
  - In AES, all operations are performed on 8-bit bytes. In particular, the arithmetic operations of addition, multiplication, and division are performed over the finite field.
  - An example of a finite field (one with a finite number of elements) is the set Zp consisting of all the integers {0, 1, …. , p - 1}, where p is a prime number and in which arithmetic is carried out modulo p.

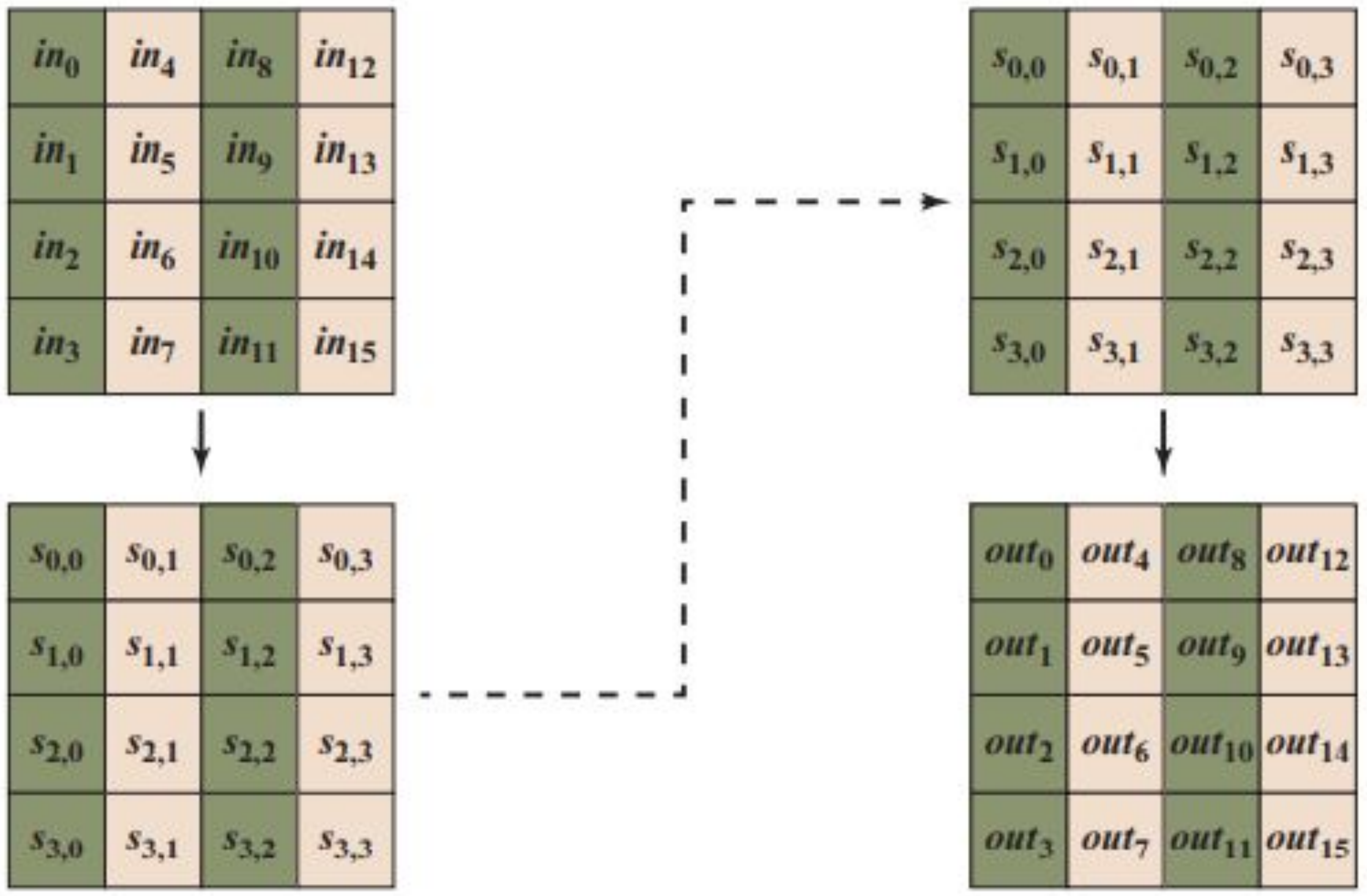
AES ALGORITHM

- The cipher takes a plaintext block size of 128 bits, or 16 bytes
- The key length can be 16, 24, or 32 bytes (128, 192, or 256 bits). The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length.
- The input to the encryption and decryption algorithms is a single 128-bit block.
- this block is depicted as a 4 * 4 square matrix of bytes.
- block is copied into the State array, which is modified at each stage of encryption or decryption. After the final stage, State is copied to an output matrix.

AES ALGORITHM

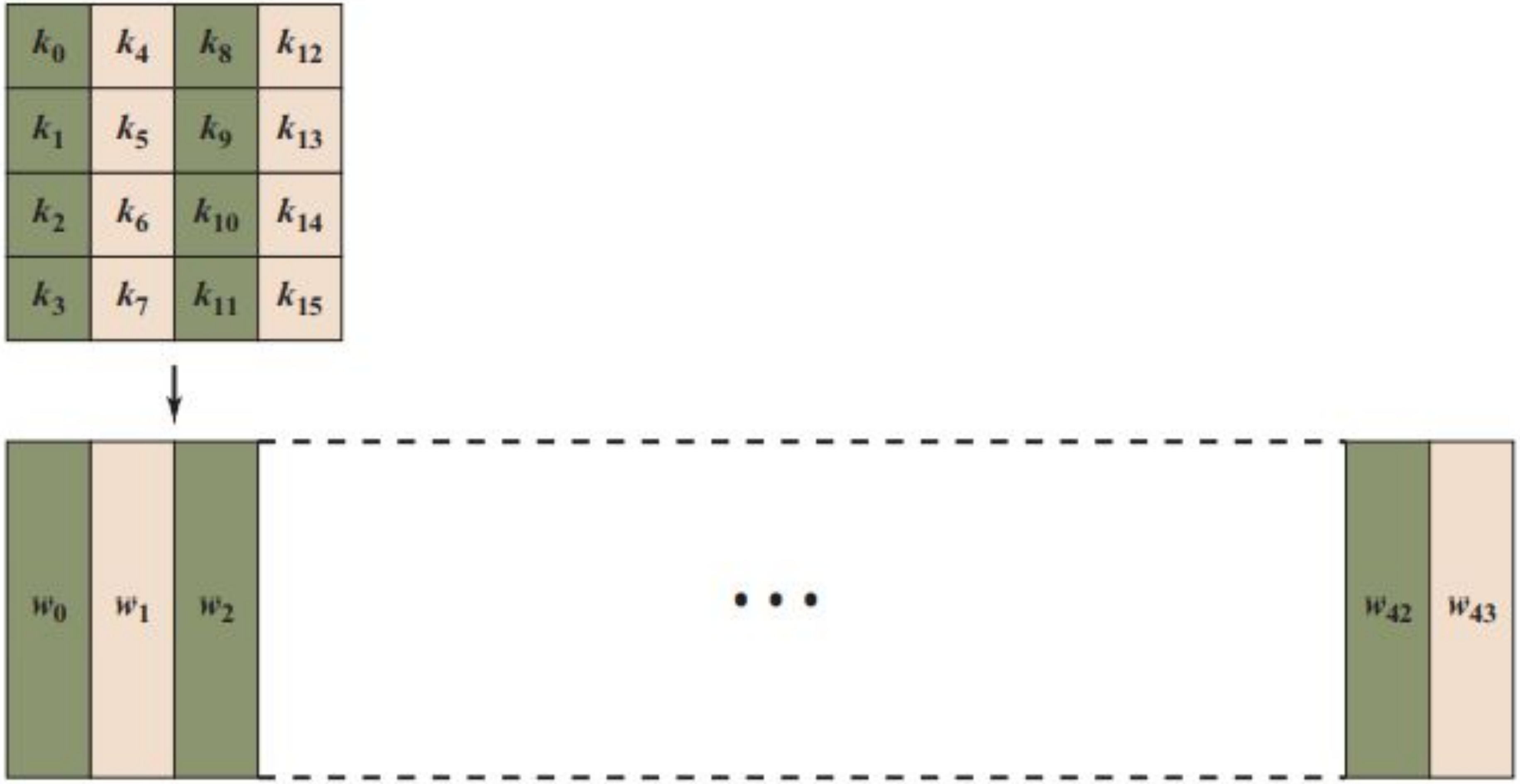
- the key is depicted as a square matrix of bytes. This key is then expanded into an array of key schedule words.
- the first four bytes of the expanded key, which form a word, occupy the first column of the w matrix.
- The cipher consists of N rounds, where the number of rounds depends on the key length: 10 rounds for a 16-byte key, 12 rounds for a 24-byte key, and 14 rounds for a 32-byte key

AES ALGORITHM



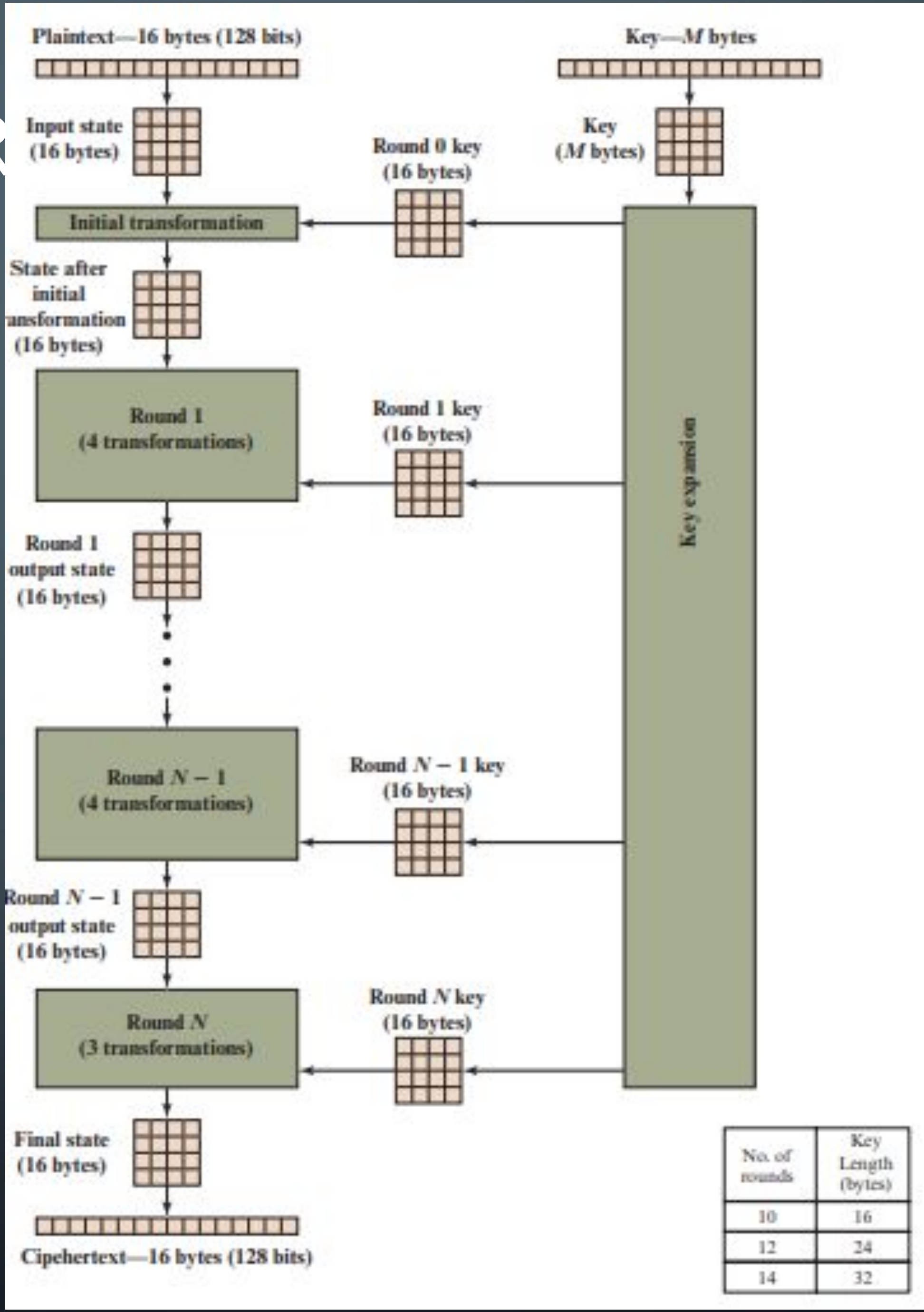
(a) Input, state array, and output

AES ALGORITHM



(b) Key and expanded key

AES STRUCTUR



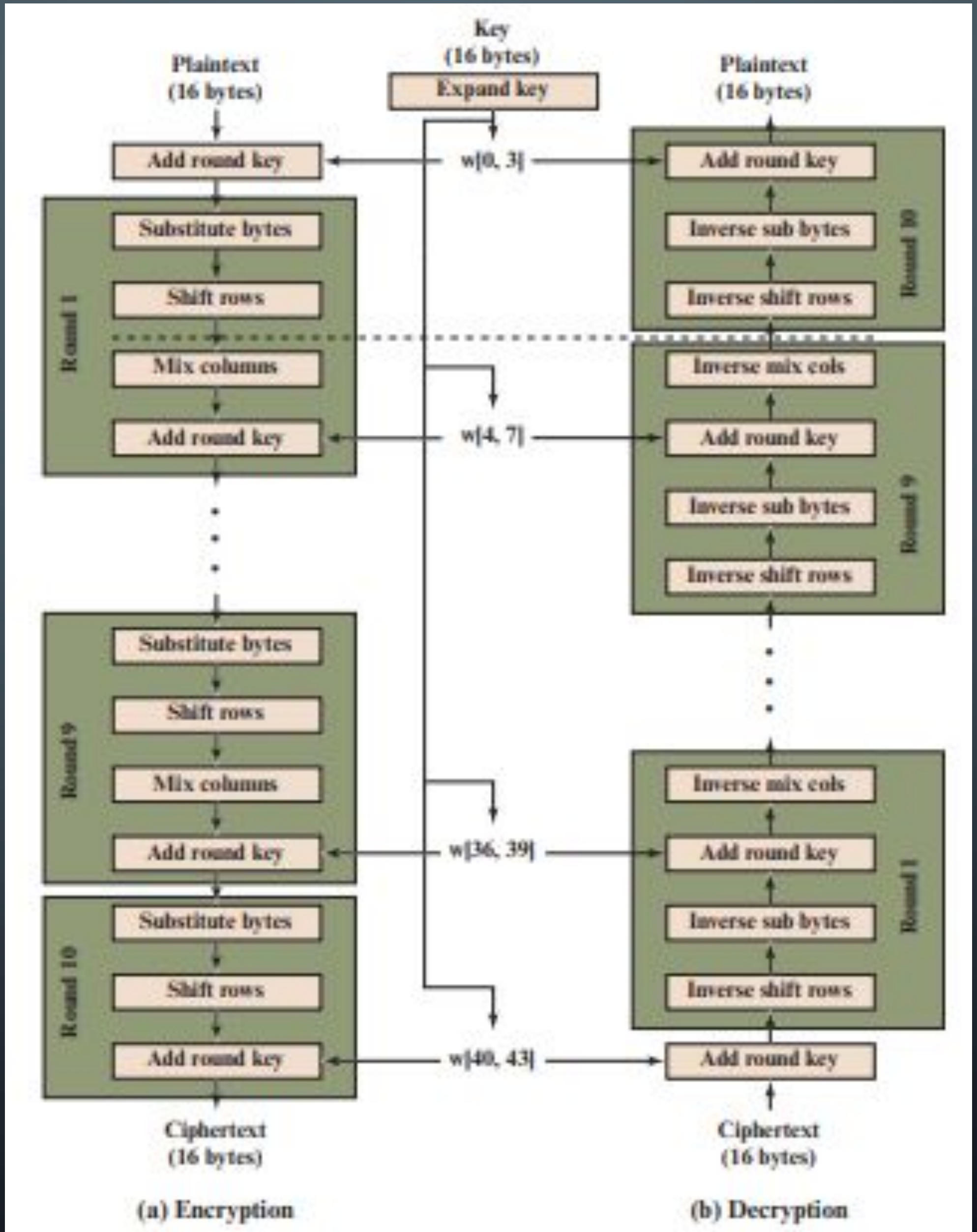
AES PARAMETERS

Key Size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext Block Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of Rounds	10	12	14
Round Key Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded Key Size (words/bytes)	44/176	52/208	60/240

AES TRANSFORMATION FUNCTIONS

- Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block.
- ShiftRows: A simple permutation.
- MixColumns: A substitution that makes use of arithmetic over $GF(2^8)$.
- AddRoundKey: A simple bitwise XOR of the current block with a portion of the expanded key.

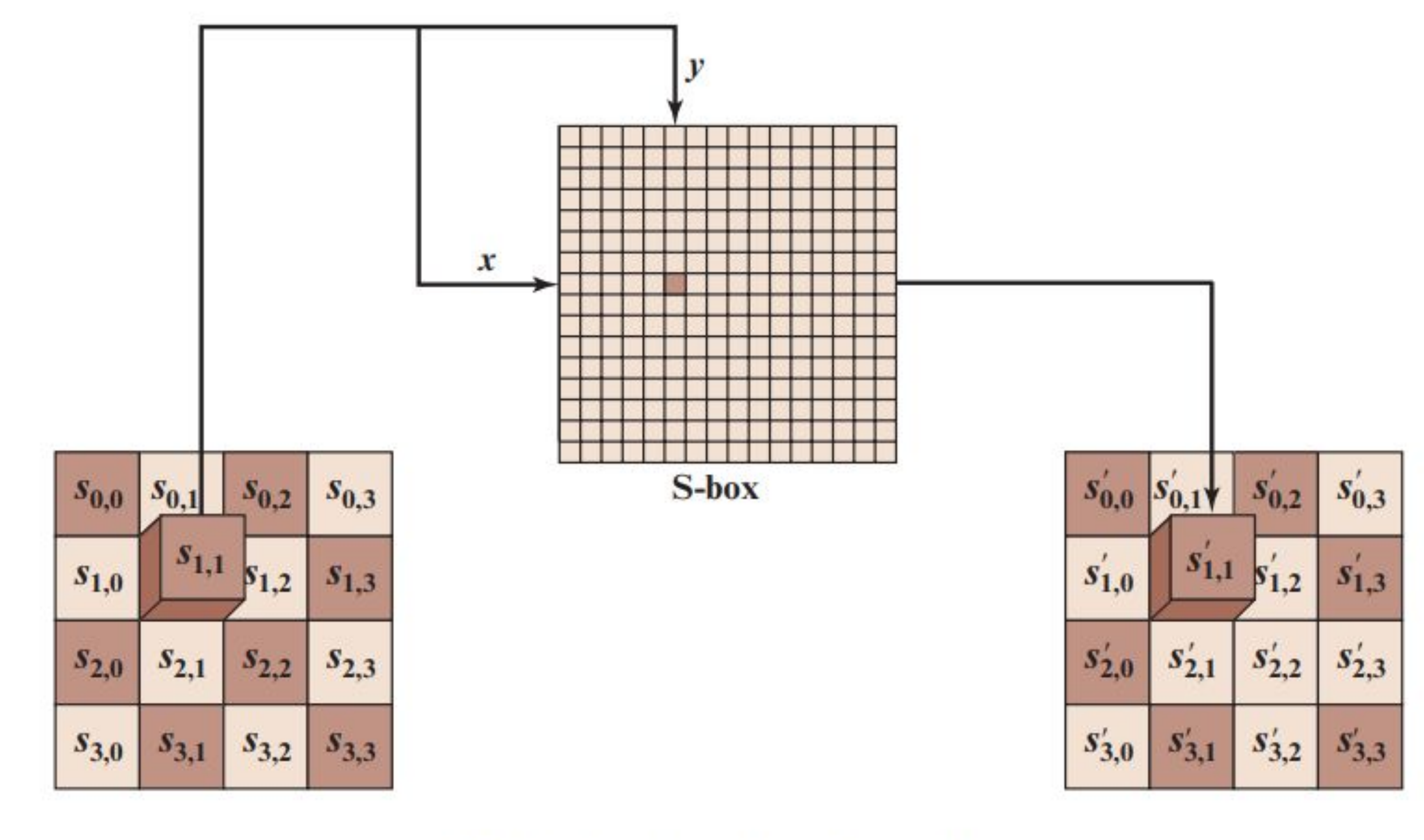
AES ENCRYPTION AND DECRYPTION



SUBSTITUTE BYTES TRANSFORMATION

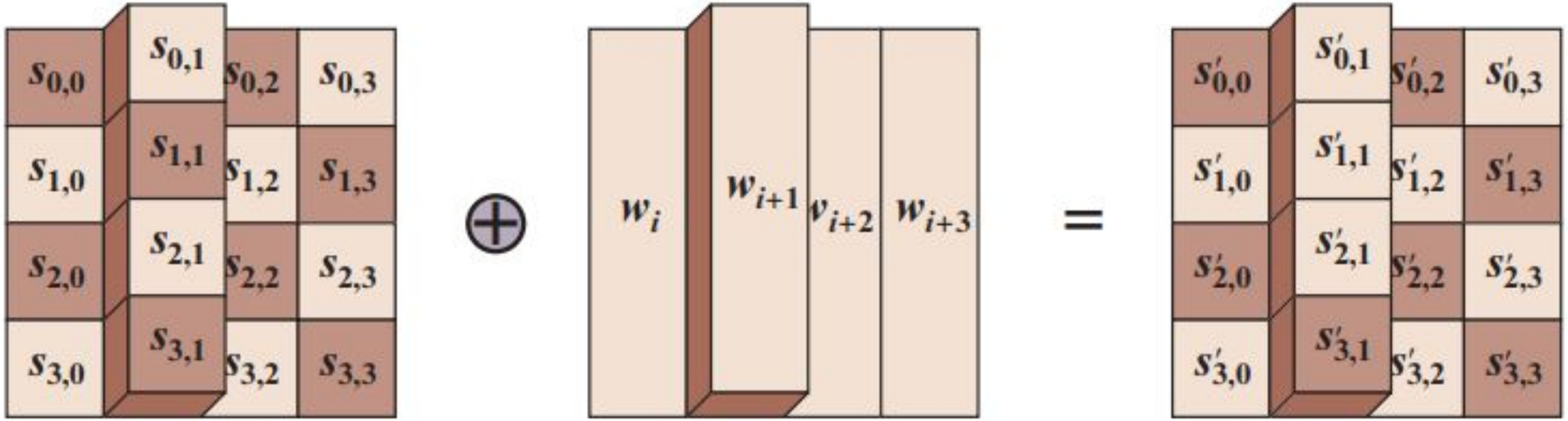
- Forward and Inverse Transformations: The forward substitute byte transformation, called SubBytes, is a simple table lookup.
- AES defines a 16 * 16 matrix of byte values, called an S-box that contains a permutation of all possible 256 8-bit values.
- Each individual byte of State is mapped into a new byte in the following way:
- The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are 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 BYTES TRANSFORMATION



(a) Substitute byte transformation

ADD ROUND TRANSFORMATION



(b) Add round key transformation

AES – MIX COLUMN TRANSFORMATION

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

*

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

=

47			
37			
94			
?			