1- Stream cipher : encrypts a digital data stream one bit or one byte at a time.

2-If the cryptographic keystream is random, then this cipher is unbreakable.

3- Block Cipher: a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

4-Feistel proposed : an approximation to the ideal block cipher by utilizing the concept of a product cipher.

5-Substitutions: Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements

6-Permutation: A sequence of plaintext elements is replaced by a permutation of that sequence.

7-Diffusion: The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext.

8-Confusion: Seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible.

9-Data are encrypted in 64-bit blocks using a 56-bit key.

10-DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.

11-The combination of bits 1 and 6 of the input defines one of 4 rows.

12-the combination of bits 2 through 5 defines one of the 16 columns.

13-The 2 nd column of the table shows the intermediate 64-bit values at the end of each round for the two plaintexts.

14-It drops the parity bits (bits 8, 16, 24, 32, …, 64) from the 64-bit key and permutes the rest of the bits according to the flowing Table.

Shifting.

| Rounds | Shift |
|---|---|
| 1.2.9.16 | One bit |
| Others | Two bits |

انتهينا من شابتر ٤

1-Random Numbers: A number of network security algorithms and protocols based on cryptography make use of random binary numbers.

2-These applications give rise to two distinct and not necessarily compatible requirements for a sequence of random numbers:

\ Randomness and Unpredictability/

3-Uniform distribution: The distribution of bits in the sequence should be uniform; that is, the frequency of occurrence of ones and zeros should be approximately equal.

4-Independence: No one subsequence in the sequence can be inferred from the others.

5-the resulting sequences will pass many tests of randomness and are referred to as:

pseudorandom numbers.

6-the source is often referred to as an : entropy source.

7-• **Pseudorandom number generator:** An algorithm that is used to produce an open-ended sequence of bits is referred to as a PRNG.

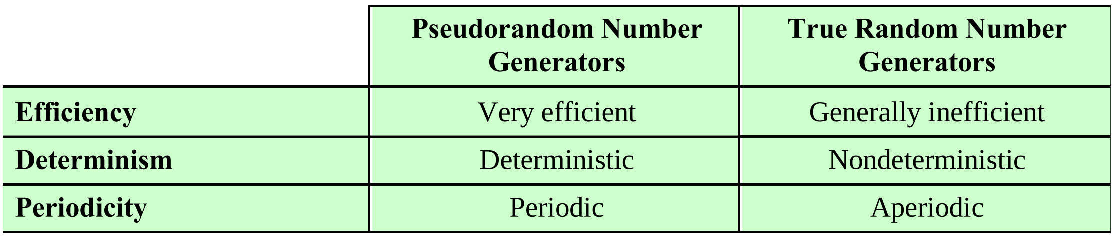
**8-• Pseudorandom function (PRF):** is used to produced a pseudorandom string of bits of some fixed length.

9- Typically the seed is generated by: TRNG

10-RC4: is used in the WiFi Protected Access (WPA) protocol that are part of the IEEE 802.11 wireless LAN standard.

11-LavaRnd is an open source project for creating truly random numbers using inexpensive cameras, open source code, and inexpensive hardware.

12-



| | **Pseudorandom Number Generators** | **True Random Number Generators** |
|---|---|---|
| **Efficiency** | Very efficient | Generally inefficient |
| **Determinism** | Deterministic | Nondeterministic |
| **Periodicity** | Periodic | Aperiodic |

ناهينا من شابتر8

1-Key distribution

• How to have secure communications in general without having to trust a Key Distribution Center (KDC) with your key.

2-Digital signatures

• How to verify that a message comes intact from the claimed sender.

3-Public-key encryption is a general-purpose technique that has made symmetric encryption obsolete.

4-Plaintext.: The readable message or data that is fed into the algorithm as input.

.5-Encryption algorithm

Performs various transformations on the plaintext.

6-Public key.:Used for encryption or decryption.

7-Ciphertext :.The scrambled message produced as output.

8-Decryption algorithm.:

Accepts the ciphertext and the matching key and produces the original plaintext.

9-• Encryption/decryption: The sender encrypts a message with the recipient’s public key .

10- • Digital signature: The sender “signs” a message with its private key .

11- • Key exchange: Two sides cooperate to exchange a session key .

**12■ Brute force**: This involves trying all possible private keys.

**13■ Mathematical attacks:** There are several approaches, all equivalent in effort to factoring the product of two primes.

**14■ Timing attacks:** These depend on the running time of the decryption algorithm.

**15■ Hardware fault-based attack:** This involves inducing hardware faults in the processor that is generating digital signatures.

**16■ Chosen ciphertext attacks:** This type of attack exploits properties of the RSA algorithm.

17- Constant exponentiation time: Ensure that all exponentiations take the same amount of time before returning a result .

18- Random delay: Better performance could be achieved by adding a random delay to the exponentiation algorithm to confuse the timing attack.

19- Blinding: Multiply the ciphertext by a random number before performing exponentiation.