IS U2 Block Ciphers and the Data Encryption Standard

Tuesday, November 9, 2021 14:40

1. What is the difference between a block cipher and a stream cipher

following are the important differences between Block Cipher and Stream Cipher.

a. Both Block Cipher and Stream Cipher belong to the symmetric key cipher.
b. These both methods are used to convert plain text into cipher text

Sr. No.	Key	Block Cipher	Stream Cipher
1	Definition	Block Cipher is the type of encryption where the conversion of plain text performed by taking its **block at a time**.	On other hand Stream Cipher is the type of encryption where the conversion of plain text performed by taking **one byte** of the plain text **at a time**.
2	Conversion of Bits	As Block Cipher takes block at a time so **comparatively more bits** get converted as compared to in Stream Cipher specifically **64 bits or more could get converted at a time**.	On other hand in case of Stream Cipher **at most 8 bits** could get converted at a time.
3	Principle	Block Cipher uses **both confusion and diffusion** principle for the conversion required for encryption.	On other hand Stream Cipher uses **only confusion** principle for the conversion.
4	Algorithm	For encryption of plain text Block Cipher uses **Electronic Code Book (ECB)** and **Cipher Block Chaining (CBC)** algorithm.	On other hand Stream Cipher uses **CFB (Cipher Feedback)** and **OFB (Output Feedback)** algorithm.
5	Encryption	The complexity of block cipher is **simple**.	While stream cipher is **more complex**
6	Decryption	As combination of more bits get encrypted in case of Block Cipher so the reverse encryption or **decryption is comparatively complex** as compared to that of Stream Cipher.	On other hand Stream Cipher uses **XOR for the encryption** which can be easily reversed to the plain text.
7	Implementation	The main implementation of Block Cipher is **Feistel Cipher**.	On other hand the main implementation of Stream Cipher is **Vernam Cipher**.
8	Speed	**slow** as compared to a stream cipher	**fast** in comparison to block cipher.

From <https://www.tutorialspoint.com/difference-between-block-cipher-and-stream-cipher>

2. What are the parameters and design features for realization of a Feistel network.

a. The exact realization of a Feistel network depends on the choice of the following parameters and design features:
    i. Block size- Increasing size improves security, but slows cipher
        1) larger: greater security (diffusion)
        2) smaller: faster encryption, decryption

3) typical: 64 bit, 128 bit AES

ii. Key size- Increasing size improves security, makes exhaustive key searching harder, but may slow cipher

1) larger: greater security (brute-force resist)
2) smaller: faster encryption, decryption
3) typical: 128 bit

iii. Number of rounds- Increasing number improves security, but slows cipher

1) multiple rounds increase security
2) typical: 16

iv. Subkey generation Algorithm- Greater complexity can make analysis harder, but slows cipher

1) complexity makes cryptanalysis difficult

v. Round function F- Greater complexity can make analysis harder, but slows cipher

1) complexity makes cryptanalysis difficult

b. Two other considerations in the **design of a Feistel cipher**

i. Speed of execution

1) required for embedded systems

ii. Ease of analysis

1) algorithm easy to understand is easy to identify vulnerabilities
2) DES isn't easy to analyze

iii. Fast software en/decryption & ease of analysis - are more recent concerns for practical use and testing

3. Explain Feistel decryption algorithm.

- Ciphertext is used as input
- Use subkeys K_i in reverse order
- Same algorithm is used
- Notation

LE_i	left half in encryption algorithm
RE_i	right half in encryption algorithm
LD_i	left half in decryption algorithm
RD_i	right half in decryption algorithm

- Output of i^{th} encryption round input to $(16-i)^{th}$ decryption round swapped
- LEi||REi ≡ RD16-i||LD16-i

4. Explain encryption and decryption in Data Encryption Standard (DES).

a. Encryption in DES

i. 64-bit plaintext block

ii. 56-bit key

iii. Exact structure as Feistel except

1) initial permutation of plaintext
2) final permutation of last round's output

iv. 64 bit plaintext pass thru initial permutation

1) rearrange bit to produce permuted input

v. Followed by 16 rounds of same function

1) involve permutation & substitution functions
2) output of last round swapped (LH, RH) to produce preoutput

        vi. Preoutput pass thru a permutation (IP-1)
            1) inverse of IP to produce 64 bit ciphertext

    b. Decryption in DES
        i. As with any Feistel cipher, decryption uses the same algorithm as encryption
        ii. subkeys are reversed

5. Explain key generation in Data Encryption Standard (DES).
    a. 64-bit key used as input (8 × 8 table)
    b. 8th bit in each row is ignored →56 bits
    c. key is permuted using table PC-1
    d. resulting 56 bits separated into two 28-bit parts C0, D0
    e. Each round
        i. circular left shift C_{i-1} , D_{i-1} of 1 or 2 bits (table)
        ii. shifted values go to next round
        iii. also used as input to table PC-2
        iv. PC-2 produce 48-bit output Ki used in F(R_{i-1} , Ki)

6. What is the purpose of the S-boxes in Data Encryption Standard (DES)?
    a. 8 s-boxes, each has 6 bits input, 4 bits out
    b. outer 2 bits (1,6) used to select row
    c. inner 4 bits (2-5) used to select column
    d. decimal value of cell converted to 4 bits out
        i. note that decimal values are [0-15]
    e. 8 4-bit groups produce 32 bit output

7. Explain operation of S-Boxes in Data Encryption Standard (DES).

8. Explain Single Round of DES Algorithm with neat diagram.

9. Explain general structure of Advanced Encryption Standard (AES).

10. Explain detailed structure of Advanced Encryption Standard (AES).

11. Explain Advanced Encryption Standard (AES) transformation functions.

12. Explain Advanced Encryption Standard (AES) key expansion.