Harsh Mishra
T21-64
Security Lab
Assignment-3

Assignment-3

Aim- To explore the different network reconnaissance tools to gather information about networks.

Electronic Code Block

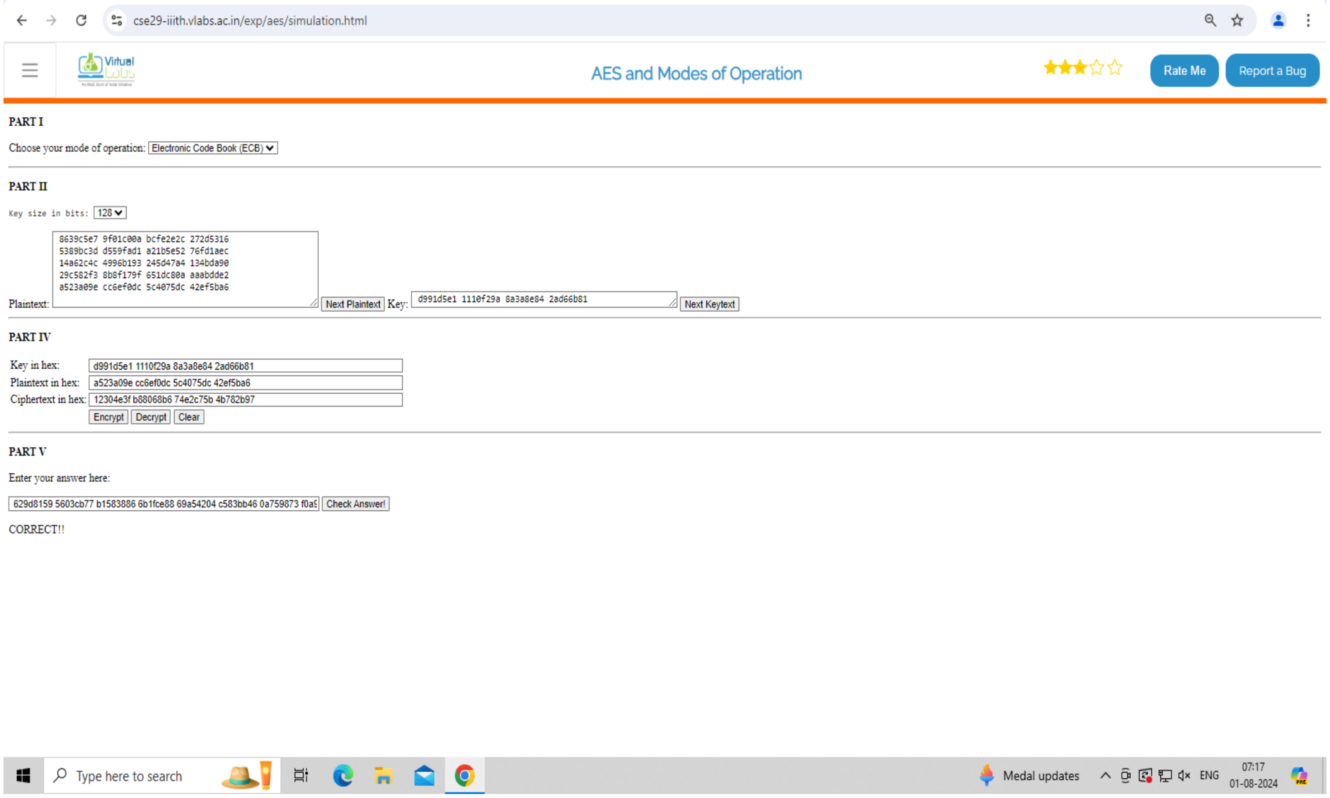
Theory:

Electronic Codebook (ECB) is a simple mode of operation for block ciphers. It encrypts each block of plaintext independently using the same encryption key.

1. Block-based: The plaintext is divided into fixed-size blocks (e.g., 64 or 128 bits), and each block is encrypted separately.
2. Independent Encryption: Each block is treated independently, meaning identical plaintext blocks will produce identical ciphertext blocks.
3. Weakness: Because of this independence, ECB does not hide data patterns well, making it vulnerable to certain types of attacks, especially when encrypting large amounts of data or highly structured data (e.g., images).

Due to these weaknesses, ECB is generally not recommended for encrypting sensitive data.

Implementation:



PART I

Choose your mode of operation: Electronic Code Book (ECB)

PART II

Key size in bits: 128

Plaintext:

```
8639c5e7 9f01c00a bcfe2e2c 272d5316
5389bc3d d559fad1 a21b5e52 76fd1aec
14a62c4c 4996b193 245d47a4 134bda90
29c582f3 8b8f179f 651dc80a aaabdde2
a523a09e cc6ef0dc 5c4075dc 42ef5ba6
```

Key: d991d5e1 1110f29a 8a3a8e84 2ad66b81

PART IV

Key in hex: d991d5e1 1110f29a 8a3a8e84 2ad66b81
Plaintext in hex: a523a09e cc6ef0dc 5c4075dc 42ef5ba6
Ciphertext in hex: 12304e3f b88068b6 74e2c75b 4b782b97

PART V

Enter your answer here:

629d8159 5603cb77 b1583886 6b1fce88 69a54204 c583bb46 0a759873 f0a

CORRECT!!

Harsh Mishra
T21-64
Security Lab
Assignment-3

Cipher Block Chaining

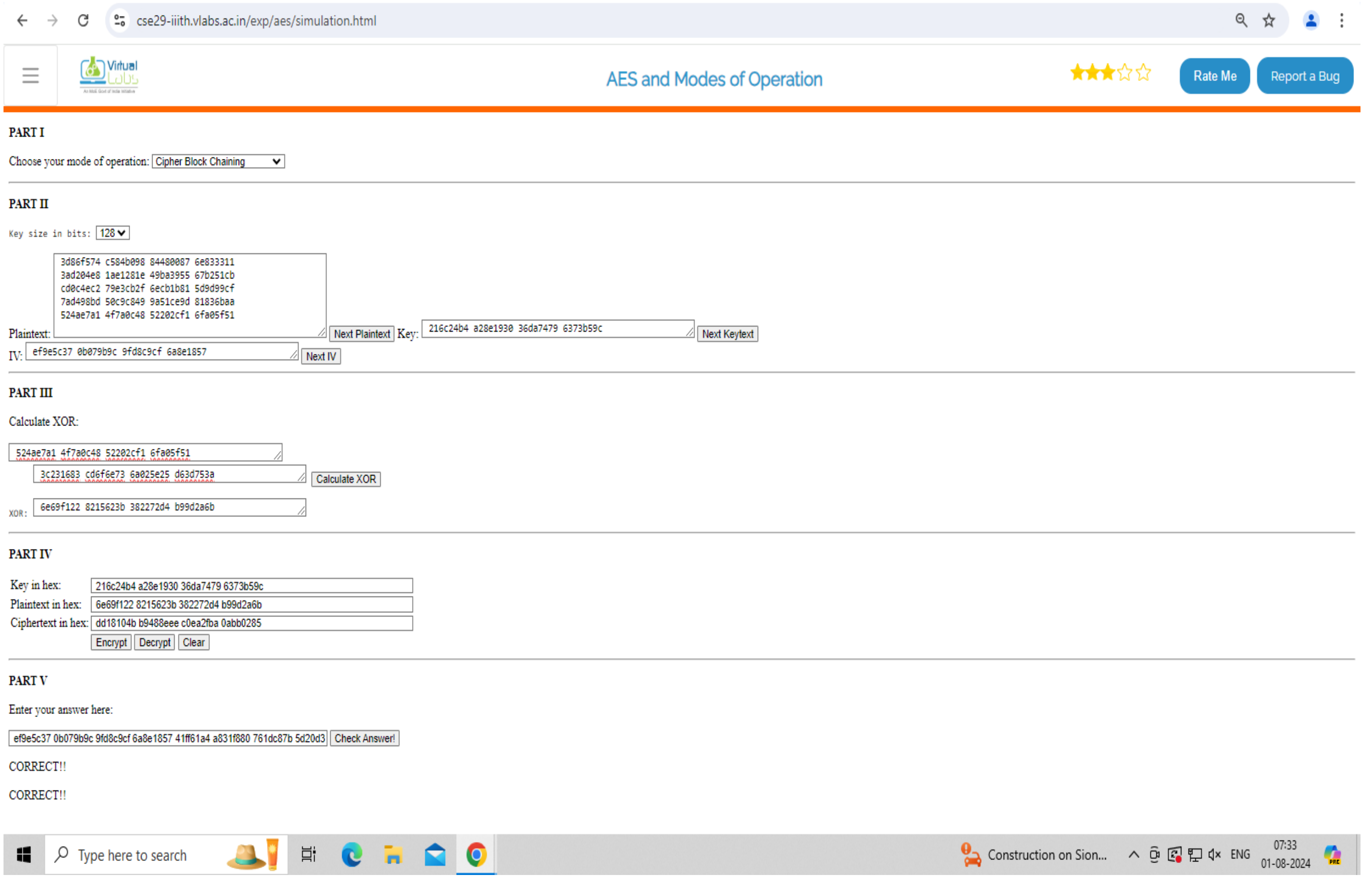
Theory:

Cipher Block Chaining (CBC) is a mode of operation for block ciphers that provides enhanced security by linking the encryption of each block to the previous one.

1. Chaining: Each plaintext block is XORed with the previous cipher-text block before encryption. This means that the encryption of each block depends on the previous block, making patterns less visible in the cipher-text.
2. Initialization Vector (IV): The process starts with an IV, a random block that is XORed with the first plaintext block. This ensures that even if the same plaintext is encrypted multiple times, the resulting cipher-text will be different each time.
3. Security: The chaining mechanism helps in hiding patterns in the plaintext, making CBC much more secure than ECB. However, if an error occurs in one block, it can affect the decryption of subsequent blocks.

CBC is widely used in practice due to its improved security features compared to simpler modes like ECB.

Implementation:


cse29-iiith.vlabs.ac.in/exp/aes/simulation.html
Virtual Labs
AES and Modes of Operation
Rate Me
Report a Bug

PART I

Choose your mode of operation: Cipher Block Chaining

PART II

Key size in bits: 128

Plaintext:

```
3d86f574 c584b098 84480087 6e833311
3ad204e8 1ae1281e 49ba3955 67b251cb
cd0c4ec2 79e3cb2f 6ecb1b81 5d9d99cf
7ad498bd 50c9c849 9a51ce9d 81836baa
524ae7a1 4f7a0c48 52202cf1 6fa05f51
```

Next Plaintext

Key: 216c24b4 a28e1930 36da7479 6373b59c

Next Keytext

IV: ef9e5c37 0b079b9c 9fd8c9cf 6a8e1857

Next IV

PART III

Calculate XOR:

524ae7a1 4f7a0c48 52202cf1 6fa05f51

3c231683 cd6f6e73 6a025e25 d63d753a

Calculate XOR

XOR: 6e69f122 8215623b 382272d4 b99d2a6b

PART IV

Key in hex: 216c24b4 a28e1930 36da7479 6373b59c

Plaintext in hex: 6e69f122 8215623b 382272d4 b99d2a6b

Ciphertext in hex: dd18104b b9488eee c0ea2fba 0abb0285

Encrypt Decrypt Clear

PART V

Enter your answer here:

ef9e5c37 0b079b9c 9fd8c9cf 6a8e1857 41ff61a4 a831f880 761dc87b 5d20d3

Check Answer!

CORRECT!!

CORRECT!!

Harsh Mishra
T21-64
Security Lab
Assignment-3

Counter Mode

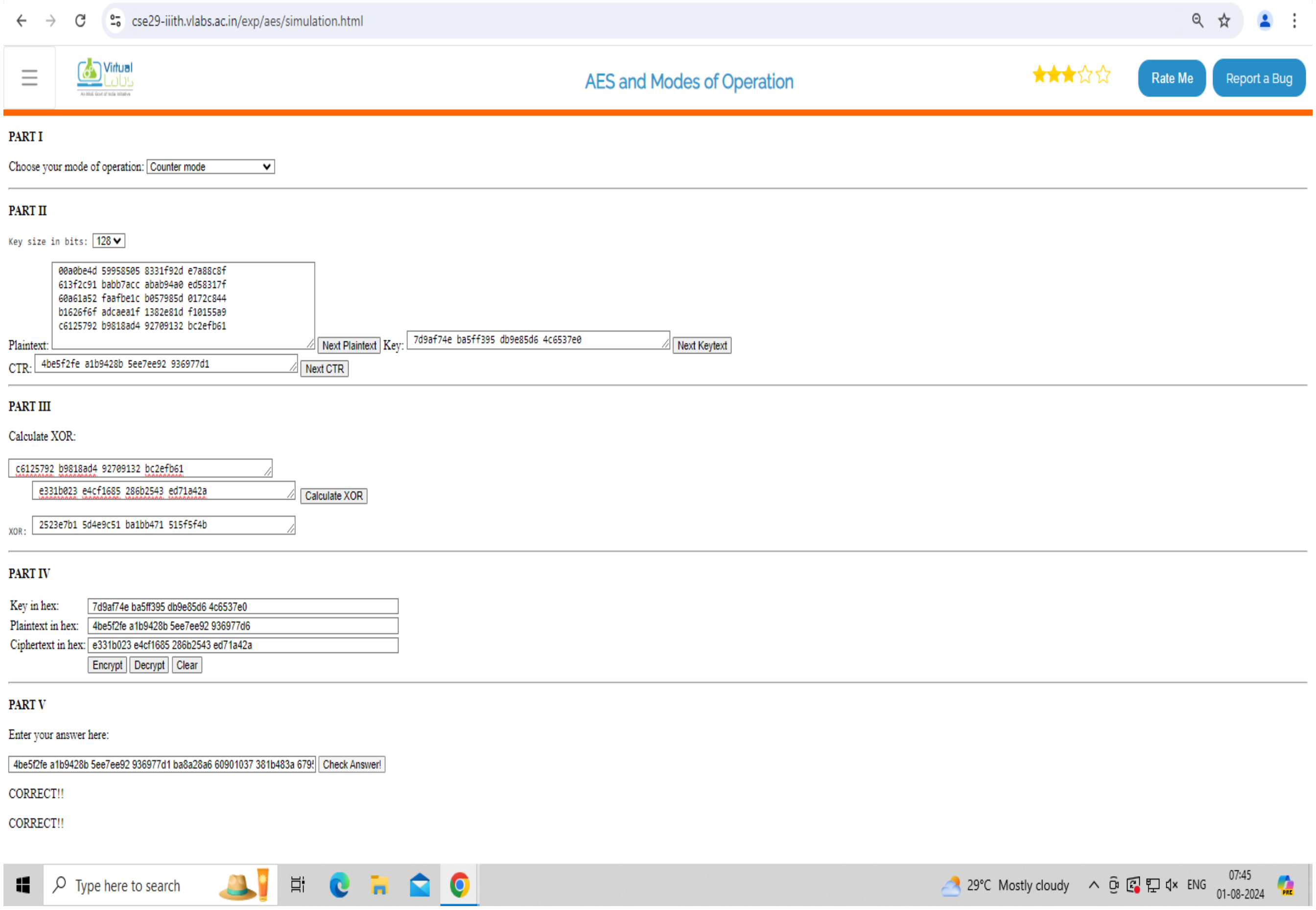
Theory:

Counter (CTR) Mode is a mode of operation for block ciphers that turns a block cipher into a stream cipher by generating a unique key stream for each block.

1. Counter-Based: Instead of directly encrypting the plaintext, CTR mode encrypts a counter value, which is then XORed with the plaintext to produce the cipher-text. The counter is usually a simple incrementing number, ensuring that each block uses a different key stream.
2. Parallelizable: Unlike other modes like CBC, CTR mode allows for parallel encryption and decryption of blocks because the counter values are independent of the plaintext. This makes CTR mode very efficient for high-speed encryption.
3. Initialization Vector (IV): CTR mode uses an IV or a nonce to start the counter sequence, ensuring that the same plaintext encrypted multiple times will produce different cipher-texts.
4. Security: CTR mode is secure and widely used, but care must be taken to never reuse the same IV/counter combination with the same key, as it would lead to vulnerabilities.

CTR mode is popular in modern encryption due to its efficiency and ability to handle parallel processing.

Implementation:



PART I

Choose your mode of operation: Counter mode

PART II

Key size in bits: 128

Plaintext:

```
00a0be4d 59958505 8331f92d e7a88c8f
613f2c91 babb7acc abab94a0 ed58317f
60a61a52 faafbe1c b057985d 0172c844
b1626f6f adcaea1f 1382e81d f10155a9
c6125792 b9818ad4 92709132 bc2efb61
```

Next Plaintext

Key: 7d9af74e ba5ff395 db9e85d6 4c6537e0 Next Keytext

CTR: 4be5f2fe a1b9428b 5ee7ee92 936977d1 Next CTR

PART III

Calculate XOR:

c6125792 b9818ad4 92709132 bc2efb61

e331b023 e4cf1685 286b2543 ed71a42a Calculate XOR

XOR: 2523e7b1 5d4e9c51 ba1bb471 515f5f4b

PART IV

Key in hex: 7d9af74e ba5ff395 db9e85d6 4c6537e0
Plaintext in hex: 4be5f2fe a1b9428b 5ee7ee92 936977d6
Ciphertext in hex: e331b023 e4cf1685 286b2543 ed71a42a

Encrypt Decrypt Clear

PART V

Enter your answer here:

4be5f2fe a1b9428b 5ee7ee92 936977d1 ba8a28a6 60901037 381b483a 679 Check Answer!

CORRECT!!

CORRECT!!

Harsh Mishra
T21-64
Security Lab
Assignment-3

Output Feedback

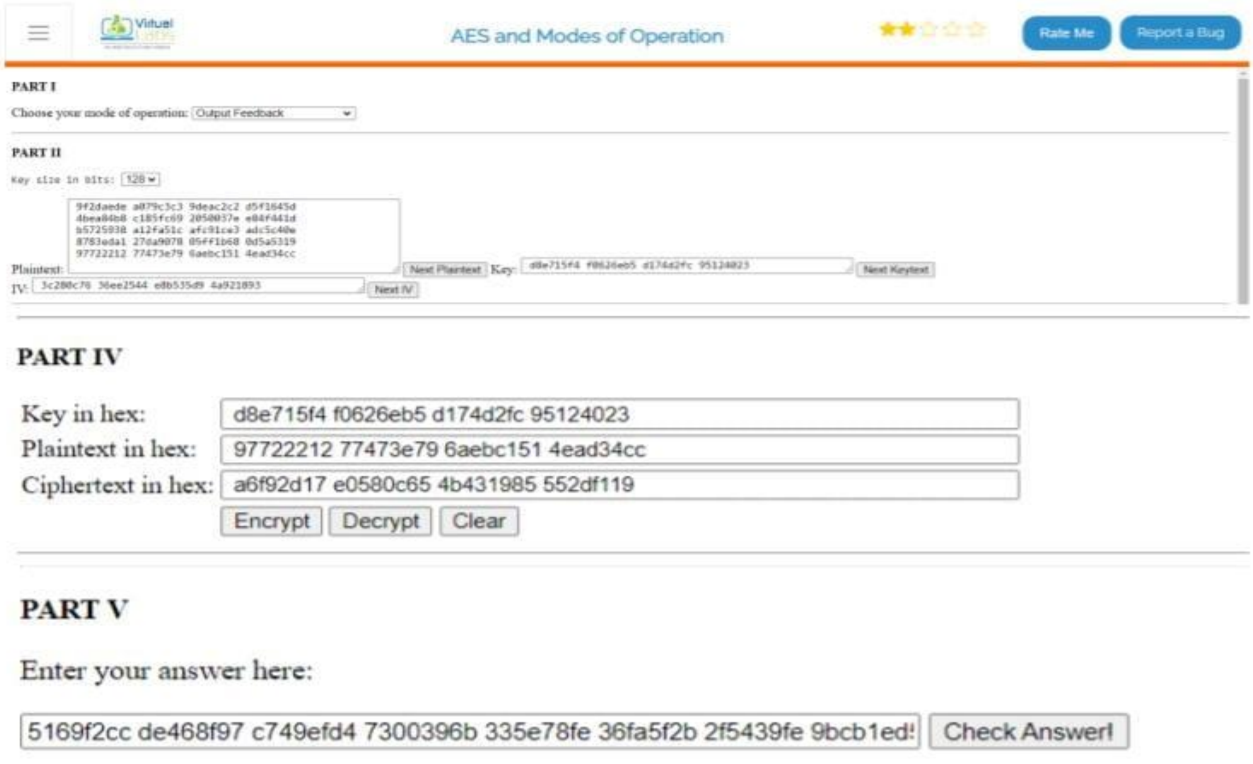
Theory:-

Output Feedback (OFB) Mode is a mode of operation for block ciphers that turns a block cipher into a stream cipher by generating a key stream independently of the plaintext.

1. Stream Generation: OFB mode generates a key stream by encrypting an initialization vector (IV) and then repeatedly encrypting the output of the previous encryption to produce the next part of the key stream.
2. XOR Operation: Each block of plaintext is XORed with the corresponding block of the key stream to produce the ciphertext. This makes it similar to a stream cipher.
3. No Error Propagation: Errors in one block do not affect the decryption of other blocks, making OFB mode resilient to transmission errors.
4. Initialization Vector (IV): The IV is critical in OFB mode and must be unique for each encryption session to ensure security. Reusing an IV with the same key compromises the security of the cipher.

OFB mode is useful for scenarios where error propagation needs to be minimized, such as in noisy communication channels.

Implementation:-



PART I

Choose your mode of operation: Output Feedback

PART II

Key size in bits: 128

Plaintext:
```
9f2daede a079c3c3 9deac2c2 d5f1645d
4bea84b8 c185fc69 2050037e e84f441d
b5725938 a12fa51c afc91ce3 adc5c40e
8783eda1 27da9078 05ff1b68 0d5a5319
97722212 77473e79 6aebc151 4ead34cc
```
Next Plaintext

Key: d8e715f4 f0626eb5 d174d2fc 95124023 Next Keytext

IV: 3c280c76 36ee2544 e8b535d9 4a921893 Next IV

PART IV

Key in hex: d8e715f4 f0626eb5 d174d2fc 95124023

Plaintext in hex: 97722212 77473e79 6aebc151 4ead34cc

Ciphertext in hex: a6f92d17 e0580c65 4b431985 552df119

Encrypt Decrypt Clear

PART V

Enter your answer here:

5169f2cc de468f97 c749efd4 7300396b 335e78fe 36fa5f2b 2f5439fe 9bcb1ed! Check Answer!