#1

https://github.com/alanchuang111/Imformation_security

==========

Experiment 1: Different IVs in Encryption

Plaintext: This is a secret message for AES encryption testing!

Key: a6e15643e201d9ac1fcf53019eeaebb4

IV1: a3b78ba049739a46e13f3adf1711548c

IV2: 2f8618cf03f2fd3e232628dd9a00bcf9

IV3 (same as IV1): a3b78ba049739a46e13f3adf1711548c

--- AES-CBC with Different IVs ---

Ciphertext1:

e4b0ea612da1364383583697c186cf9be4e9866a15ff3a8e8373a29ee36aca3c

Ciphertext2:

deadb66e16e1b6fd2b60ce0e9760c8fc152aaaa530083b3dea69a413da6767c7

Ciphertext3:

e4b0ea612da1364383583697c186cf9be4e9866a15ff3a8e8373a29ee36aca3c

--- AES-OFB with Different IVs ---

Ciphertext1:

d0ff5a6eb8883bbb4c3c698687c13f50b90cbb8219e8f787ee3a8db0b0b8a538

Ciphertext2:

e43c12af06c3325915032b206ff2e5a01e0c369681e148306b7a9d1b8897989b

Ciphertext3:

d0ff5a6eb8883bbb4c3c698687c13f50b90cbb8219e8f787ee3a8db0b0b8a538

==========

Experiment 2: Modified IV in Decryption

Original Plaintext: Block cipher modes are important for security!

--- AES-CBC Mode ---

Correct IV: a10bfd1ba4ef13ea6c76a43b9b60580c

Ciphertext:

1e800a2a06fa3ee07eccc01a790b5e61345d46102b4dd47d7d6b2b822d34c6750a5e69

16601e5703fa0e7d57aaff9f6a

Decryption with CORRECT IV: Block cipher modes are important for security!

Wrong IV: a07802a68c2e63c543f1151b630db5c4

Decryption with WRONG IV: b'C\x1f\x90\xdeC\xe1\x13F_\xef\xd4R\xd8\x00\x82\xaces are important for security!'

--- AES-OFB Mode ---

Decryption with CORRECT IV: Block cipher modes are important for security!

Decryption with WRONG IV:

b'\xf3w\xe8\x0c\xb7U\xf6gf9\xa8V\x04\x12\x08\xbc\n\r\n@\xbf\xed\xaa\xc1\x0cc\xc6\x01\xe6\xf5\xc4f-x+\xbc\x0e\xe5\x04\xcc(\x13\x0c\xa4\xb8\t'

==========

Experiment 3: Modified Ciphertext

Original Plaintext: Message authentication is crucial for data integrity!

--- AES-CBC Mode ---

Original Ciphertext:

486ccff4fe4a658159ca29519613d1af5512b973d722be3344f52369cf114a6c

Decryption with MODIFIED ciphertext:

b'Message authenti8\xcf\xe4iXn\xd3\x18+\x10\xb6\xc5\x9a\x03\x98\xa6l fos data integrity!'

--- AES-OFB Mode ---

Decryption with MODIFIED ciphertext:

b'Message authenticatinn is crucial for data integrity!'

==========

Experiment 4: Wrong Decryption Key

Original Plaintext: The key is essential for decryption!

--- AES-CBC Mode ---

Decryption with CORRECT key: The key is essential for decryption!

Decryption with WRONG key:

b'T\x88\xe0\x81\xe7\xc3q"$r\x1b\xa0\xa6G,\x8d\xb6\xf8(\xf4\x0c\xbf\xac\xeb_\xa5\xcc\
xb6,\x16\xebA\x07\xe2\xcfN_\xa0\x1d]\xc2\xe5/3\xab\xa17\xe3'

--- AES-OFB Mode ---

Decryption with WRONG key:

b'\xfb\x1a\xd4\x90\xcbU\xe6?\x11Z\x01\xd0\xa4\\3\xd2bFZ!\xf5\x08|x\x8e\xa9\xfc\xd3
W&\x97\x04\xbe\x8e\x97^'

==========

SUMMARY OF KEY OBSERVATIONS

==========

1. IV Requirements:
   - Both CBC and OFB require unique IVs for each encryption
   - Same IV with same key produces identical ciphertext (security risk)

2. IV Modification Impact:
   - CBC: Wrong IV only corrupts first block
   - OFB: Wrong IV corrupts entire plaintext

3. Ciphertext Modification:
   - CBC: Error propagates to current and next block
   - OFB: Error only affects corresponding bit (no propagation)

4. Wrong Key:
   - Both modes produce complete garbage with wrong key

5. Padding:

- CBC: Requires padding to block size
- OFB: Stream cipher mode, no padding needed

6. Security Considerations:

- Never reuse IV with the same key
- Use message authentication (MAC) to detect tampering
- OFB is self-synchronizing for bit errors
- CBC provides error propagation (tamper-evident)

#2