Fundamentals of Cryptography

David Jao

Topics in Quantum-Safe Cryptography

CryptoWorks21

UNIVERSITY OF WATERLOO

June 23, 2016

Part V

Modes of operation

Block ciphers vs. stream ciphers

Recall:

- A stream cipher is a symmetric-key encryption scheme in which each successive character of plaintext determines a single character of ciphertext.
- A block cipher is a symmetric-key encryption scheme in which a fixed-length block of plaintext determines an equal-sized block of ciphertext.

Encrypting bulk data

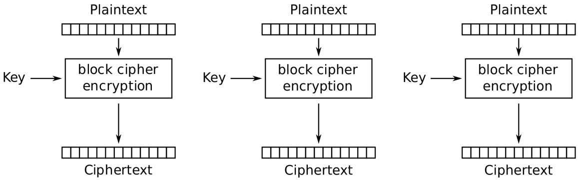
What if one needs to encrypt large quantities of data?

- With a stream cipher, just encrypt each character.
- With a block cipher, there are some complications if:
  - the input is larger than one block, or
  - the input does not fill an integer number of blocks.

To deal with these problems, we use a *mode of operation*, which means a specification for how to encrypt multiple and/or partial data blocks using a block cipher.

Electronic Codebook (ECB) mode

The obvious approach is to encrypt each ℓ bits independently, where ℓ is the block size.



Electronic Codebook (ECB) mode encryption

(All figures from `https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation`)

Problems with ECB mode

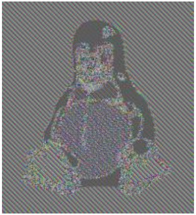
Although stream ciphers are (usually) secure when used in the obvious way, block ciphers in ECB mode are INSECURE!

- A block cipher, unlike a stream cipher, is stateless.
- ECB mode is equivalent to a giant substitution cipher where each ℓ-bit block is a "character"
- Semantic security is immediately violated: One can tell by inspection whether or not two blocks of ciphertext correspond to identical plaintext blocks (violates "no partial information")

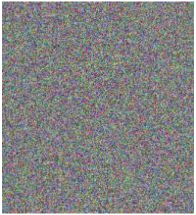
ECB example

Original

ECB mode

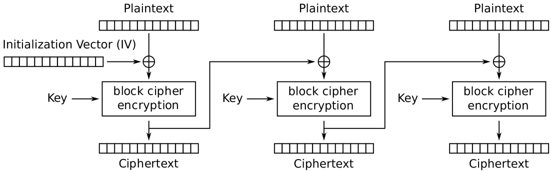


Any other mode

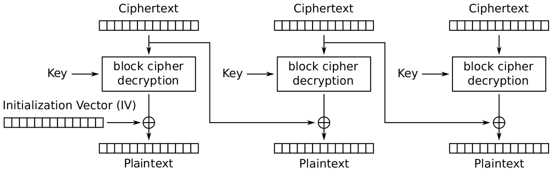


Cipher Block Chaining (CBC) mode

CBC mode: Choose a (non-secret) one-block Initialization Vector (IV) and include it as part of the ciphertext.



Cipher Block Chaining (CBC) mode encryption



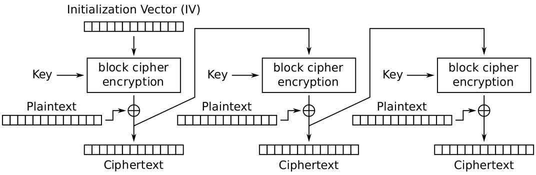
Cipher Block Chaining (CBC) mode decryption

Properties of CBC mode

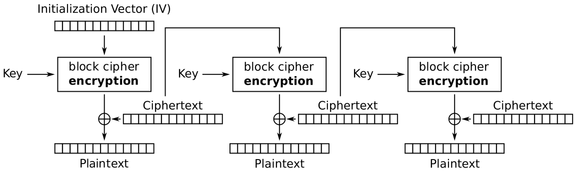
- Encryption is sequential (cannot be parallelized).
- Decryption *can* be parallelized.
- Using an IV twice under the same key invalidates semantic security. (how?)
- A small change in plaintext or IV changes all subsequent encrypted ciphertext blocks.
- A small (length-preserving) change in ciphertext changes only *two* decrypted plaintext blocks. (Active attacks are possible!)
- CBC mode does not handle partial data blocks — padding is required.

POODLE (Padding Oracle On Downgraded Legacy Encryption; published October 14, 2014) is an active attack against TLS/SSL which exploits data block padding in CBC mode.

Cipher Feedback (CFB) mode



Cipher Feedback (CFB) mode encryption

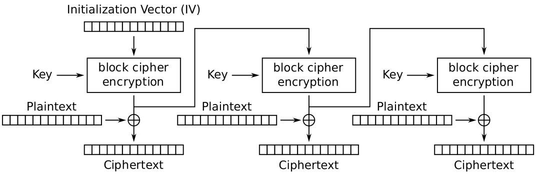


Cipher Feedback (CFB) mode decryption

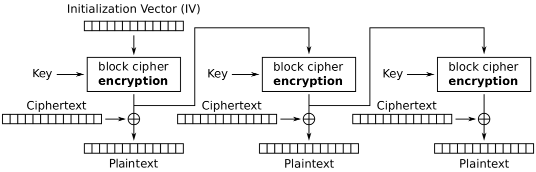
Properties of CFB mode

- The underlying block cipher is only used in **encryption** mode.
- Encryption is sequential (cannot be parallelized).
- Decryption can be parallelized.
- Using an IV twice under the same key invalidates semantic security. (Exercise: better or worse than CBC?)
- A small change in plaintext or IV changes all subsequent encrypted ciphertext blocks.
- A small (length-preserving) change in ciphertext changes two decrypted plaintext blocks. (Active attacks are possible!)
- CFB mode *can* handle partial data blocks without padding — simply transmit a partial ciphertext block.

Output Feedback (OFB) mode



Output Feedback (OFB) mode encryption



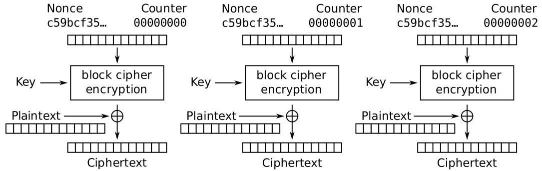
Output Feedback (OFB) mode decryption

Properties of OFB mode

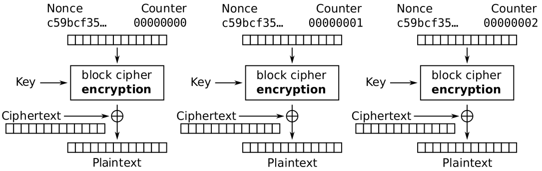
- The underlying block cipher is only used in **encryption** mode.
- Encryption cannot be parallelized, but can be pre-computed.
- Decryption cannot be parallelized.
- Using an IV twice under the same key is disastrous!
- A small change in IV changes all subsequent encrypted ciphertext blocks.
- A small (length-preserving) change in either plaintext or ciphertext produces a small change in the other.
- OFB mode can handle partial data blocks without padding — however, it is insecure in this situation, via a non-obvious attack (Davies and Parkin, 1983).

Counter (CTR) mode

Choose a nonce at random during encryption. Prepend the nonce to the ciphertext.



Counter (CTR) mode encryption

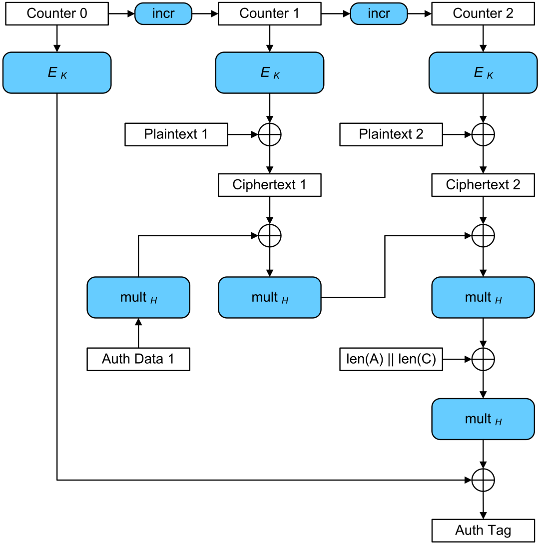


Counter (CTR) mode decryption

Properties of CTR mode

- The underlying block cipher is only used in **encryption** mode.
- Encryption and decryption are highly parallelizable.
- Using a nonce twice under the same key is disastrous!
- A small change in the nonce changes all subsequent encrypted ciphertext blocks.
- A small (length-preserving) change in either plaintext or ciphertext produces a small change in the other.
- CTR mode can handle partial data blocks without padding.

Authenticated encryption (Galois Counter Mode)



Galois Counter Mode (GCM)

- GCM ciphertexts (ignoring the authentication tag) are **identical** to counter (CTR) mode ciphertexts.
  - In particular, the last ciphertext block is truncated if the plaintext length is not an integral number of blocks.
- Authentication tags are computed in

$$GF(2^{128}) = \mathbb{F}_2[x]/(x^{128} + x^7 + x^2 + x + 1).$$

- Hence, GCM requires a 128-bit block size (e.g. AES).
- "Auth Data 1" is a 128-bit block of authenticated unencrypted data, viewed as an element of $GF(2^{128})$.
  - More than one such block is supported, but only one is shown.
- H is defined as $H = E_k(0^{128}) = E_k(\mathbf{0}) \in GF(2^{128})$. Computing H requires knowledge of the key.
- Computing authentication tags can be parallelized using field arithmetic.