A TECHNICAL ANALYSIS OF BLOCK CIPHER OPERATION MODES

Jordan Patterson
2024

Introduction to Block Ciphers

Block ciphers are widely used in cryptography to secure and authenticate data both in storage and in transit. It is a symmetric encryption algorithm that operates on a fixed size block of data using a secret key. The same key is used for encryption and decryption. With a block cipher, plaintext is transformed into a block of ciphertext and then back again when being decrypted.

Block Ciphers use the principles of confusion and diffusion to make itself as complex and unpredictable as possible.

Overview: Block Cipher Operation Modes

There are 5 main Block Cipher operation modes, each with their own unique advantages and disadvantages. ECB, CBC, CFB, OFB, and CTR.

Electronic Code Block (ECB):

In ECB, each block of plaintext is encrypted independently with the same key. It is simple and efficient. It is not very secure because identical blocks of plaintext will produce identical blocks of ciphertext. For example, if I were to encrypt the phrase "My name is Jordan" 10 times, the ciphertext output would be the same every time. This will allow patterns to be found in the ciphertext and allow it to be decoded.

Cipher Block Chaining (CBC):

CBC provides better encryption the ECB. XOR (Exclusive or) is applied to each block of plaintext before being encrypted, which ensures that the encryption is more secure because identical blocks of plaintext wont always produce the same ciphertext like with ECB.

Cipher Feedback Mode (CFB):

In CFB, the previous ciphertext block is encrypted and then XOR is applied to the output using the current plaintext block to produce the ciphertext.

Output Feedback Mode (OFB):

In OFB, a keystream is generated using the block cipher. XOR is applied to the keystream to output the ciphertext. OFB is similar to CFB but is better designed to prevent error propagation.

Counter Mode (CTR):

In CTR, similar to OFB, a keystream is generated using the block cipher. XOR is applied to the keystream to output the ciphertext. The keystream in CTR is generated by encrypting a counter value that is incremented for each block.

Cipher Block mode comparison

ECB: Ecrypts each block of data independently with the same key. It is fast and simple but lacks security.

CBC: Encrypts each block of data by applying XOR to it using the previous ciphertext block. More secure and random than ECB. Can propagate errors and requires some padding.

CFB: Transforms a block cipher into a stream cipher by encrypting the previous ciphertext block and applying XOR using the current plaintext block. Can encrypt partial blocks and does not require padding. Is prone to propagate errors.

OFB: Turns a block cipher into a stream cipher by encrypting the previous output block and applying XOR using the current plaintext block. Does not rely on the ciphertext and is good at preventing errors. Is vulnerable to replay attacks.

CTR: Turns a block cipher into a stream cipher by encrypting a counter value and applying XOR to it using the current plaintext block. Does not rely on the ciphertext or require padding. Is vulnerable to replay attacks and it requires a unique counter value.

Analysis of the weaknesses of using ECB

As explained above, ECB is both simple and fast. It is the simplicity that is its downfall, however. The same block of plaintext will always produce the exact same block of ciphertext. This will allow threat actors to identify letters and words based on patterns that ECB will create. This leaves you with a basic mode of encryption that may be ok for testing, learning, or for insensitive data but it should not be used in production environments due to its sever vulnerabilities.

Technical Analysis of GCM:

GCM , also known as Galois/Counter Mode, combines CTR with a hash function based on the Galois Field Arithmatic. The combination these two things are what gives this mode its name. GCM can not only protect data but it can also protect its metadata. It does not require padding on the ciphertext. It is very efficient and does not require huge hardware/software overhead to function. Like with all operation modes, there are also downsides associate with GCM. GCM requires a unique initialisation vector for each encryption leaving it vulnerable to nonce reuse attacks. Its use of Galois Field Arithmatic also makes it somewhat difficult to implement correctly and is sometimes incompatible with certain platforms. GCM also has a limited maximum message size which makes it unsuitable for large data sets.

Summary:

In summary, we've analyzed what a block cipher is and some of the various block cipher modes that exist. While researching the various block cipher modes, it has become clear that they all have their own unique advantages and disadvantages. While some modes are clearly better and more secure than others, its not always so easy to decide which is best especially when it comes to the more complex modes such as CFB, OFB, CTR, or GCM.

References:

What is a block cipher? (techtarget.com)

Block cipher - Wikipedia

Cipher Definition – What is a Block Cipher and How Does it Work to Protect Your Data? (freecodecamp.org)

Deterministic algorithm - Wikipedia

Block Cipher modes of Operation - GeeksforGeeks

Block cipher mode of operation - Wikipedia

Exclusive or - Wikipedia

Galois/Counter Mode - Wikipedia

encryption - Why would I ever use AES-256-CBC if AES-256-GCM is more secure? - Information Security Stack Exchange