Cryptography

Amit Paul

January 2025

1 Discussion

1.1 AES and Symmetrical Encryption

1.1.1 Introduction to AES

Security has always been a major aspect in every tech-driven company, or even for the average person with remote access to the internet. However, current ciphers will not be able to keep up with the rate of advancing technology.Especially now that Quantum Computers are rising, the development of Quantum Proof Ciphers is essential. This is where AES (Advanced Encryption Standard), formerly known as Rijndael, comes into play.

AES works as a block cipher with a plain text size of 128 bits and a key size of 128/192/256 bits. The plain text, which we shall refer to as the "state", is separated into a block of 4 by 4 bytes. We can then apply a series of functions in order to the state, resulting in a cipher text.

AES works on 2 fundamental rules:

- Diffusion
- Confusion

Confusion is all about complicating the relationship between the key and the cipher text. 1 bit of the cipher text should depend on more than 1 bit of the key.
Diffusion is all about changing the statistical structure of the cipher text, for every bit changed in the key, approximately half of the bits should change for the cipher.

We are now going to explore the AES algorithm and how it is used to encrypt the state, primarily focusing on AES-128.

1.1.2 Key expansion

Firstly, the original key is expanded into multiple round keys depending on the size of the original key. The size of the original key also determines how many rounds of transformations there will be.

AES-128	AES-192	AES-256
11 round keys	13 round keys	15 round keys
10 rounds	12 rounds	14 rounds

As seen from the figure, AES-128 consists of 11 round keys and a total of 10 rounds. Firstly, we are now going to concatenate the bytes in each of the columns resulting in 4 words.

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

$\downarrow$

W_0	W_1	W_2	W_3

Hence, getting the first round key. For the subsequent round keys, you are going to input the last word into a g function. This g function will then perform some operations to this input, returning a completely different word.