Tweet

Hello Peeps,

Sorry for such a late post. But now in this post, I will deep dive into the internals and the structure of the AES Algorithm.

Since we have discussed with the basic definition of AES, we will get into details this time. As we know, AES is the most important symmetric key algorithm widely used in the world. We will try to understand the structure and internals of AES.
As we have learnt before, AES is a symmetric key algorithm. It only has single key for both encryption and decryption. It is a block cipher with three major things(these are common in other algorithms also):

1. Input
2. Output
3. Key

The input required should be 128 bits in length and there are three different key lengths that it supports, depending upon the requirement as shown below:

Key Length	Number of Rounds
128	10
192	12
256	14

As we can see from the above table, number of rounds is key dependent. Each of the round consists of processing steps to create a cipher text. These rounds also have reverse rounds to transform the cipher text back to the plain text (hence the inverse that we talked about before. □)

Also each of the round consists of 4 layers:

1. Byte Substitution
2. Shift Rows
3. Mix Columns
4. Key Addition

Now the question arises why do we need to have rounds and then layers within them?? :O

Basically, we need to make sure that the cipher text generated is random enough and secure as well. So, we follow two major properties of a secure cipher, which are:

1. Confusion
2. Diffusion

Confusion means that there is a complex relationship between the key and the cipher text. Each and every bit of cipher text should be dependent on different parts of the key.

Diffusion means change in one single character of the plain text results into the change of several different characters in the cipher text, therefore resulting into two different outputs having no relationship between them.

So, if a cipher does not have the above two properties, they might be vulnerable to frequency analysis attack, which is again a different topic. :/

So we can conclude that number of rounds depends on the key length in AES, so higher the length of the key, higher will be the round, and hence the performance might slow down but will be stronger.

That’s all for this post, in my upcoming post, we will learn about the four layers mentioned above and how they actually follow confusion and diffusion, hence resulting into a secure cipher. Till then, Happy Decoding

PS: For understanding Extension Fields in details, we will learn them in a separate blog post dedicated only to this particular topic.

cryptfreak

I am currently improving my skills in Application and mobile-based security. My area of research includes **Blockchain**, specially **Ethereum based Smart Contracts**. But **Cryptography** and **Mathematics** have always been my first love. I am highly passionate about information security and I deeply involve myself into the logic behind. **I prefer Decoding things than Breaking them**