**Cesar, Xor and AES**

Here I am going to explain the difference and Why the AES encryption is safer than the naïve Encryptions such as Cesar and XOR

Let’s start from the navies encryptions.

**Cesar:**

Cesar is a digit shift which shifts every letter of a word by a key number.

Our plain will result with the letters shifted, making it unreadable to a machine that doesn’t have the key to decrypt the file.

This technique can be simply brute force it. As we know, Cesar uses a number in the alphabetical list, but we know that the letters in the alphabet are 26.

So we do a for loop that shifts key for each letter of the alphabet, until we found our secret message. Making the pattern easily breakable and unsafe.

**Xor:**

Xor encrypting is the same concept as Cesar encrypting, but instead of using letters it uses 256 bits for encryption as the key component. Putting more numbers on the table and making decryption more difficult. Luckily, we do know what the digits in the Ascii table are.

Again, we are going to use a for loop, but this time we are going to pass the ascii table and pass every bit in order to find our secret message.

This still demonstrates why this pattern is considered a Naïve pattern, because with the technology and the knowledge we have now, any programmer would be able to break them.

**AES:**

Also known as Advanced Encryption Standard. This is based on the design principle known as substitution – permutation network. The Difference between the predecessor, is that it does not use the Feistel network, and it has a fixed bloc size of 128 bits, and the keys can range between 128 to 256 bits.

It works by representing both the key and the plain text into matrices, then various operations are taken between the matrices in order to crypt it. They can mix the columns of the matrices, shift positions, swapping objects between the objects or even using a subkey to add layers to the encryption.

The reason of why AES is way difficult to break, is without the key, the hacker has to figure out what changes happen between the key and the plain text.