Imagen que contiene Icono

Descripción generada automáticamenteDiagrama, Forma

Descripción generada automáticamente

Instituto Politécnico Nacional

Escuela Superior de Cómputo

Cryptography

**Programming exercises:**

**“Lab 5: More about block ciphers”**

Students:

Esquivel Ventura Yaron David

Hernández Rodríguez Armando Giovanni

Morales Hernández Carlos Jesús

Teacher:

Díaz Santiago Sandra

Group: 3CM15

November 8th, 2021

**Research**

1. Find how to decipher one round for AES. Use the example that you made in the previous session to apply the deciphering process. Use the inverse S-box and the table for inverse mixcolumn.







2) Look for a web page that uses the protocol https (e.g. a bank portal, a web site like amazon, etc). Find out which are the symmetric algorithms (block cipher, mode of operation, etc). Also find out information about the digital certificate of the web site, i.e. what is the cryptographic hash function used and the public-key algorithms used specified in the certificate.

We chose Amazon Web Services, we chose this one, because use the https protocol for services than required security for the actions that they required. All the connections that connected with this service are cypher through TLS, this service admits TLS 1.2, TLS 1.1 and TLS 1.0

Some of the symmetric algorithms that use AWS are used by AES (Advanced Encryption Standard) with 128-192 or 256-bit keys. AES often combined with Galois/CounterMode (GCM) and known as AES-GCM.

Triple DES (3DES) uses three 56-bit keys. The scheme works on a block of data by splitting it in two and iteratively applying arbitrary round functions derived from an initial function. Triple DES uses 48 rounds to encrypt a block of data.

For AWS, the most common type of certificate is based on the ISO X.509 standard. An X.509 certificate affirms the identity of the certificate subject and binds that identity to a public key. The subject can be a user, an application, a computer, or other device. The certificate authority signs a certificate by hashing its contents and then encrypting the hash with the private key corresponding to the public key in the certificate. A client application such as a web browser that needs to affirm the identity of a subject uses the public key to decrypt the certificate signature. It then hashes the certificate contents and compares the hashed value to the decrypted signature to determine whether they match. The certificate authority creates a signature by using a hash function (such as SHA256) over the variable-sized certificate content to produce an irreversible fixed-size data string. The fixed data is called a hash.

**References**

https://docs.aws.amazon.com/crypto/latest/userguide/pki-concepts.html#concept-signing