Cryptography - Network Security

Published on Thursday, December 31, 2015

Hello Folks,

New Year is around the corner. I wish you all a very happy and awesome 2016 ahead. May you crack all the examinations you appear in! Today, we'll be learning about cryptography. Any doubts/ clarifications - raise it in comments.
==>> This article is a part of PK Series (IT)

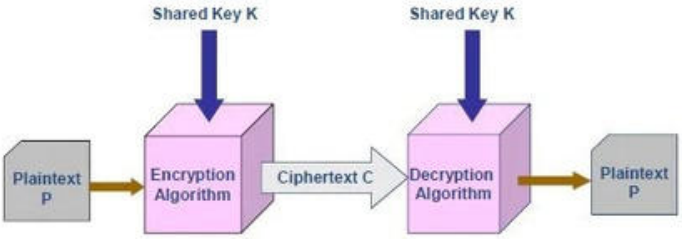
Cryptography

Its a technique to encrypt the plain text data into cipher text using keys which makes it difficult to understand and interpret. Decryption is the reverse of encryption. There are several cryptographic algorithms available as described below:

- Secret Key
- Public Key
- Message Digest

1. Secret Key Encryption

In this process, both sender and receiver have **one secret key**. This secret key is used to encrypt the data at sender's end. After the data is encrypted, it is sent on public domain to the receiver. Now using the same secret key receiver decrypts the data. Algorithms encrypt/decrypt the message block by block, a block referring to group of bits. It is also called symmetric key system. The algorithms using this system are faster and the only problem is that key management is not easy.



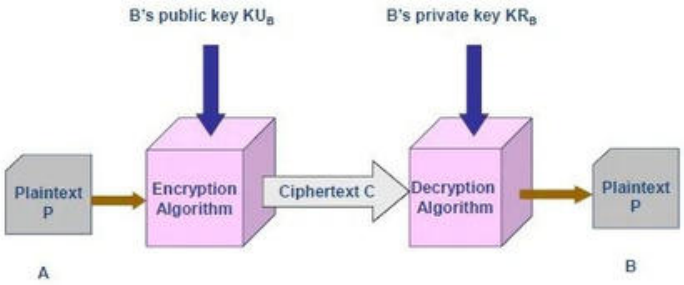
E.g.- Data Encryption Standard (DES), Advanced Encryption Standard (AES), International data encryption algorithm (IDEA).

DES: block size - 64 bits, key size - 56 bits
IDEA: block size - 64 bits, key size - 128 bits
AES: block size - 128,192,256 bits, key size - 128,192,256 bits

2. Public Key Encryption

In this process, every user has its own secret key which is never made public. Along

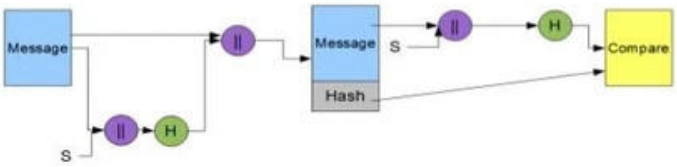
with that, every user has its own public key which is always in public domain and is used by sender to encrypt the data. Upon receiving, receiver decrypts that data by using its own secret key. In other words, every communication node will have a **pair of keys**.



E.g.- **RSA algorithm**: Based on the principles of number theory, it involves 4 steps - key generation, key distribution, encryption, decryption. This algorithm was invented in 1978 by Rivest, Shamir and Adleman. DES is about 100 times faster than RSA.

3. Message Digest

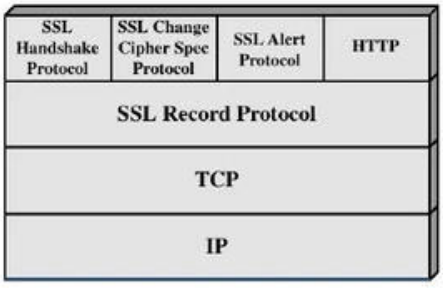
In this method, actual data is not sent, instead a **hash value (128 bits)** is calculated and sent. Receiver computes its own hash value and compare with the one it receives. If both hash values match, message is accepted otherwise rejected. This method was designed by Ronald Rivest in 1991.



E.g. - MD5 hashing - mostly used in authentication where user password is cross checked with the one saved on server.

Web Security - Secure Socket Layer (SSL)

SSL is a cryptographic protocol to secure the network across a connection oriented layer. It was first developed by **NetScape in 1994** and became an internet standard in 1996. It uses a **dedicated TCP/IP** socket (e.g - 443 for https). Along with that it also provides built in **data compression**. Look at the SSL architecture below.



SSL handshake verifies the server and allows client and server to agree on an **encryption set** before any data is send out.

Compression and decompression are functions of this record layer. Encryption of data occurs after compression.

Alert protocol explains the **severity of the message** and a description (e.g. 'fatal' - then terminate immediately).

Function of cipher spec protocol is to notify the other party to use a **new cipher suite**.

Some other sections of this topic will be covered in next article.

Interesting fact of today

The first popular web browser called Mosaic was released in 1993.