**Introduction to Cryptography Basic Principles**

by Himanshu Arora on July 18, 2012

Whenever we come across the term cryptography, the first thing and probably the only thing that comes to our mind is private communication through encryption. There is more to cryptography than just encryption. In this article, we will try to learn the basics of cryptography.

**The Basic Principles**

**1. Encryption**

In a simplest form, encryption is to convert the data in some unreadable form. This helps in protecting the privacy while sending the data from sender to receiver. On the receiver side, the data can be decrypted and can be brought back to its original form. The reverse of encryption is called as decryption. The concept of encryption and decryption requires some extra information for encrypting and decrypting the data. This information is known as key. There may be cases when same key can be used for both encryption and decryption while in certain cases, encryption and decryption may require different keys.

**2. Authentication**

This is another important principle of cryptography. In a layman’s term, authentication ensures that the message was originated from the originator claimed in the message. Now, one may think how to make it possible? Suppose, Alice sends a message to Bob and now Bob wants proof that the message has been indeed sent by Alice. This can be made possible if Alice performs some action on message that Bob knows only Alice can do. Well, this forms the basic fundamental of Authentication.

**3. Integrity**

Now, one problem that a communication system can face is the loss of integrity of messages being sent from sender to receiver. This means that Cryptography should ensure that the messages that are received by the receiver are not altered anywhere on the communication path. This can be achieved by using the concept of cryptographic hash.

**4. Non Repudiation**

What happens if Alice sends a message to Bob but denies that she has actually sent the message? Cases like these may happen and cryptography should prevent the originator or sender to act this way. One popular way to achieve this is through the use of digital signatures.

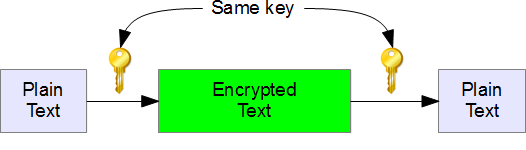
**Types of Cryptography**

There are three types of cryptography techniques:

* Secret key Cryptography
* Public key cryptography
* Hash Functions

**1. Secret Key Cryptography**

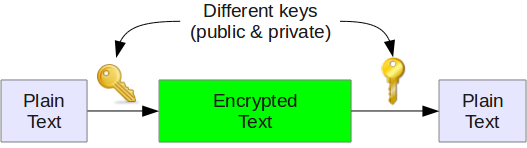
This type of cryptography technique uses just a single key. The sender applies a key to encrypt a message while the receiver applies the same key to decrypt the message. Since only single key is used so we say that this is a symmetric encryption.



The biggest problem with this technique is the distribution of key as this algorithm makes use of single key for encryption or decryption.

**2. Public Key Cryptography**

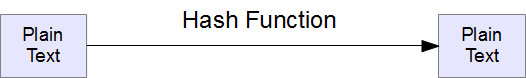
This type of cryptography technique involves two key crypto systems in which a secure communication can take place between receiver and sender over insecure communication channel. Since a pair of keys is applied here so this technique is also known as asymmetric encryption.



In this method, each party has a private key and a public key. The private is secret and is not revealed while the public key is shared with all those whom you want to communicate with. If Alice wants to send a message to bob, then Alice will encrypt it with Bob’s public key and Bob can decrypt the message with its private key.

This is what we use when we setup [public key authentication in openssh](http://www.thegeekstuff.com/2008/11/3-steps-to-perform-ssh-login-without-password-using-ssh-keygen-ssh-copy-id/) to login from one server to another server in the backend without having to enter the password.

**3. Hash Functions**



This technique does not involve any key. Rather it uses a fixed length hash value that is computed on the basis of the plain text message. Hash functions are used to check the integrity of the message to ensure that the message has not be altered, compromised or affected by virus.