Journal of Advanced Research in Cloud Computing, Virtualization and Web Applications
Volume 1, Issue 1 - 2018, Pg. No. 17-19
Peer Reviewed Journal
Research Article

Cryptography: Secure way to Share a Secret

P. R. Mathur[1]

Abstract

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography can also be understand as the way of scrambling data so that it looks like babble to anyone except those who knows the trick of decoding it. Many techniques are used for cryptography purpose such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption).

Keywords: Cryptography, Cryptographic Algorithms, Data Encryption Standards, Triple DES, DSA Algorithm, RSA Algorithm

Introduction

Encryption and Decryption, these are the two important terms that we will come across whenever we consider Cryptography.

To understand the meaning of Encryption and Decryption one must be aware of the terms like Plain text and Cipher text. So, a plain text is one what we normally write or the text that can be understood and is the real information that we want to pass on. Where as, a Cipher text is one which is the output of Encryption, it a text that's not understandable by anyone.

Lets say for our understanding purpose we have a plain text as 'hello' and our key here is AàZ,BàY….i.e, the first alphabet is taken as the last alphabet so now our cipher text will be 'SVOOL' and the process of making this conversion is known as "ENCRYPTION". As we are aware of the key from our understanding point of view we can now get back the original data that's the plain text by applying the rule i.e., AàZ, BàY… so if we do the same substitution then our cipher that's 'SVOOL' will become 'hello' and this process of retrieving back the original or plain text is known as "DECRYPTION".

Now once we encrypt the plain text it is now safe to transmit over a channel because the encrypted text would not be understood by anyone unless they know the key to it.

That's how during the WWR I and WWR II German troupes used to pass on the message for there attacks on enemies now taking about WWR I and WWR II one can just imagine how old this technique is.

What is cryptograph ?

Cryptography has, as its etymology, *kryptos* from the Greek, meaning *hidden*, and *graphein*, meaning *to write*.

- Cryptography is about scrambling data so that it looks like babble to anyone except those who knows the trick of decoding it.
- *Cryptography* is the science of using *mathematics* to encrypt and decrypt data.
- Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

In cryptography, the magic recipe for hiding data is called an *algorithm.*

An algorithm is a precise set of instructions that tells programs how to scramble and unscramble data.

There is no specific convention followed for cryptography, but the CIPHER text is always represented in CAPITAL letters.

Types of Cryptographic Algorithms

There are two types of Cryptographic algorithms present namely

- Symmetric Algorithm
- Asymmetric Algorithm

Symmetric Algorithm

A Symmetric Algorithm can be defined as an algorithm that

E-mail Id: hiabhi2@gmail.com
How to cite this article: Mathur PR., Cryptography: Secure way to Share a Secret. *J Adv Res Cloud Comp Virtu Web Appl* 2018; 1(1): 17-19.

uses the same key for encryption and decryption.

For example

- Caeser Cipher
- Vignere Cipher
- Substitution Cipher
- DES[Data Encryption Standards]
- Triple DES
- AES [Advanced Encryption Standards]

For our understanding purpose what we mean when we say SYMMETRIC ALGORITHM can be easily understood by the CAESER CIPHER.

The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

For example,

Plain: meet me after the toga party

Cipher: PHHW PH DIWHU WKH WRJD SDUWB

Note that the alphabet is wrapped around, so that the letter following Z is A.

Explanation of algorithm

The algorithm can be expressed as follows. For each plaintext letter *p*, substitute the cipher text letter C

C = E(3, *p*) = (*p* + 3) mod 26

A shift may be of any amount, so that the general Caesar algorithm is

C = E(k, *p*) = (*p* + k) mod 26

Where, *k* takes on a value in the range 1 to 25.

The decryption algorithm is simply

p = D(*k*, C) = (C-*k*) mod 26

Asymmetric Algorithm

An Asymmetric Algorithm can be defined as an algorithm that uses two different keys namely public key and private key for encryption and decryption of data i.e., the plain text is encrypted by a public key but the decryption can only be done by the person who has the private key. These keys are completely different but they have some mathematical relation.

By using such type of algorithms we improve our security because anyone can encrypt the data with their public key but the person who has the private key can only get back the original text.

Examples of Asymmetric Algorithms

- RSA
- DSA

In general example is of a bank locker.

The bank provides us with a key to each and every customer who has an locker so here our keys are the public keys and the bank holds a key without it we cannot open our locker there by acting as a private key

Keys for the RSA algorithm

The keys for the RSA algorithm are generated the following way:

- Choose two distinct large random prime numbers *p* and *q*
- Compute $n = pq$,n is used as the modulus for both the public and private keys
- Compute : $\varphi(n) = (p-1)(q-1)$
- Choose an integer *e* such that $1 < e < \varphi(n)$ and e and $\varphi(n)$ share no factors other than 1 (i.e. *e* and $\varphi(n)$ are co prime) ,*e* is released as the public key exponent
- Compute *d* to satisfy the congruence relation $de \equiv 1 \pmod{\varphi(n)}$; i.e. $de = 1 + k\varphi(n)$ for some integer *k*. ,*d* is kept as the private key exponent

Encryption:

$c=m^e \bmod n$

Decryption:

$m=c^d \bmod n$:

ex of RSA

Here is an example of RSA encryption and decryption

1. Choose two prime numbers

p = 61 and *q* = 53

Compute

n = 61 * 53 = 3233

2. Compute

$$\varphi(n) = (p-1)(q-1)$$
$$\varphi(n) = (61-1)(53-1) = 3120$$

3. Choose *e* > 1 co prime to 3120

e = 17

4. Compute d such that $de \equiv 1 \pmod{\varphi(n)}$, by computing the modular multiplicative inverse of *e* modulo $\varphi(n)$:

d = 2753

17 * 2753 = 46801 = 1 + 15 * 3120.

The public key is (*n* = 3233, *e* = 17). For a padded message m the encryption function is:

$$c = m^e \mod n = m^{17} \mod 3233.$$

The private key is (*n* = 3233, *d* = 2753). The decryption function is:

$$m = c^d \mod n = c^{2753} \mod 3233.$$

For example, to encrypt *m* = 123, we calculate

$$c = 123^{17} \mod 3233 = 855.$$

To decrypt *c* = 855, we calculate

$$m = 855^{2753} \mod 3233 = 123$$

An important point of cryptography is the strength of the encrypted data depends upon the algorithm used and the secrecy of the key. The strength is measured in the time and resources one requires to recover the plain text.

Next is Keys, as we already seen a key is a value that works with a cryptographic algorithm to produce a specific cipher text.

Keys are basically really big numbers and we have finally a public key and a private key.

References

1. Menezes AJ, van Oorschot PC, Vanstone SA. Handbook of Applied Cryptography. ISBN 0-8493-8523-7.
2. Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications). by Douglas R. Stinson, Chapman and Hall/CRC. 2005.
3. The Code Book, The Secret History of Codes and Code Breaking, Simon Singh, Anchor, 2000.
4. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. David Kahn. 1996.
5. Applied Cryptography, Second edition, Bruce Schneier, Wiley.
6. Cryptography for Dummies-Chey Cobb.
7. An Introduction to Cryptography-*Rosen* KH.

Date of Submission: 2018-05-12
Date of Acceptance: 2018-05-20