International Journal of Advanced Research in Engineering Technology & Science
ISSN: 2394-281
Email: editor@ijarets.org Volume-3, Issue-12 December- 2016 www.ijarets.org

ANALYSIS & ISSUES IN CRYPTOGRAPHY

Praveen Kr Rai
IIMT College of Engineering,
Greater Noida

Vipin Rai
IIMT College of Engineering,
Greater Noida

ABSTRACT: At professional level most of the companies are using some encryption technique to encrypt data before sending it across over the network. For instance in the financial domain projects most of the data that one gets is encrypted and requires decryption first before it can be processed into useful information. This paper looks into the basics of cryptography first. Then it will look into how to use GPG i.e. GnuPG, which is free software available both for Linux & Windows platforms, to encrypt-decrypt your data.

INTRODUCTION

Why we need to learn cryptography to secure our data? There are several other commonly used mechanisms that are commonly employed:-

Controlling access to the computer system or media, for instance through 'logon' authentication.

Restricting physical access, for instance keeping media such as CDs, floppies etc locked away.

All these approaches can be valuable and effective, but equally all can have serious shortcomings. Conventional access control mechanisms can often be bypassed (for instance via hacking). In addition, what if data has to be transmitted, or if the data media (e.g.: floppy disk) has to be moved outside the secure environment? What if a number of people are sharing the computer environment?

If the confidentiality or accuracy of your information is of any value at all, it should be protected to an appropriate level. If the unauthorized disclosure or alteration of the information could result in any negative impact, it should be secured. Cryptography (encryption and decryption) is a technique designed to protect your information in ALL such situations.

This paper is intended for all those who wish to secure their data either personal or professional using cryptography. At professional level most of the companies are using some encryption technique to encrypt data before sending it across over the network. For instance in the financial domain projects most of the data that one gets is encrypted and requires decryption first before it can be processed into useful information.

This paper looks into the basics of cryptography first. Then it will look into how to use GPG i.e. GnuPG, which is free software available both for Linux & Windows platforms, to encrypt-decrypt your data.

II. CRYPTOGRAPHY BASICS

a. Cryptography Definition

Cryptography is the science of writing in secret code. In data and telecommunications, cryptography is necessary when communicating over any non-trusted medium, which includes just about any network, particularly the Internet.

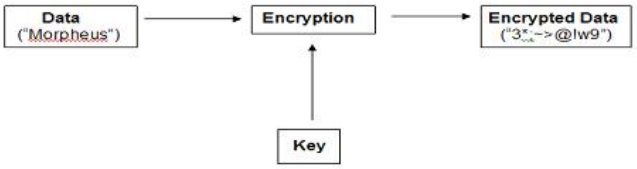
Within the context of any application-to-application communication, there are some specific security requirements, including:

- *Authentication:* The process of proving one's identity.
- *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
- *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
- *Non-repudiation:* A mechanism to prove that the sender really sent this message.

b. Types of Cryptographic Algorithms

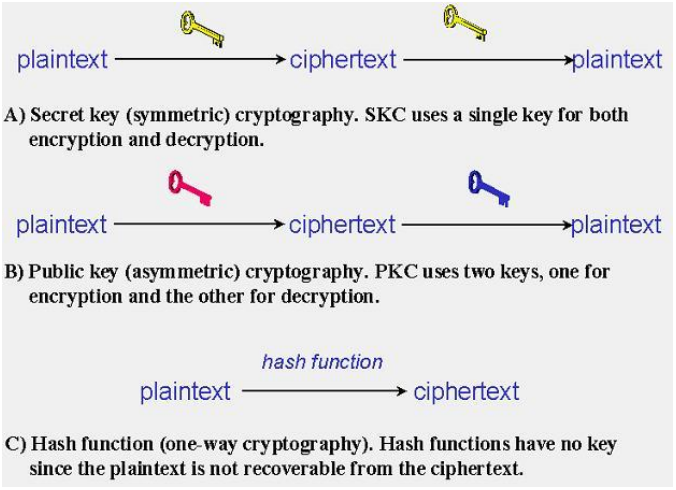
In most of the cases we first do **encryption** which is the process of converting ordinary information (*plaintext*) into unintelligible gibberish (i.e. *cipher text*).**Decryption** is the reverse, in other words, moving

from the unintelligible cipher text back to plaintext. A cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a **key**. In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher. Without a key, the algorithm would have no result.



There are three main types of cryptographic algorithm. They are as follows:-

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.



1. Secret Key Cryptography (SKC)

With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure above, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

The modern study of symmetric-key ciphers relates mainly to the study of block ciphers and stream ciphers and to their applications.

Block Ciphers:-

A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block.

Stream Ciphers:-

Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing.

In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher.

The Secret key cryptography algorithms that are most commonly in use today are DES and AES.

Data Encryption Standard (DES):

The most common SKC scheme DES was designed by IBM in the 1970s. DES is a block-cipher employing a 56-bit key that operates on 64-bit blocks. DES has a complex set of rules and transformations that were designed specifically to yield fast hardware implementations and slow software implementations, although this latter point is becoming less significant today since the speed of computer processors is several orders of magnitude faster today.

Advanced Encryption Standard (AES):

AES uses an SKC scheme called Rijndael, a block cipher designed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The algorithm can use a variable block length and key length; the latest specification allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits.

2. Public Key Cryptography (PKC)

Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others. A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each cipher text exchanged as well.

In a groundbreaking 1976 paper, Whitfield Diffie and Martin Hellman proposed the notion of public-key (also, more generally, called asymmetric key) cryptography in which two different but mathematically related keys are used a public key and a private key. A public key system is so constructed that calculation of one key (the 'private key') is computationally infeasible from the other (the 'public key'), even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair. In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. The public key is typically used for encryption, while the private or secret key is used for decryption.

Public-key cryptography algorithm that is most commonly used is RSA.

RSA

RSA is a public key algorithm invented by Rivest, Shamir and Adleman. The key used for encryption is different from (but related to) the key used for decryption.

The algorithm is based on modular exponentiation. Numbers e, d and N are chosen with the property that if A is a number less than N, then (Ae mod N)d mod N = A.

This means that you can encrypt A with e and decrypt using d. Conversely you can encrypt using d and decrypt using e (though doing it this way round is usually referred to as signing and verification).

a) The pair of numbers (e,N) is known as the public key and can be published.

b) The pair of numbers (d,N) is known as the private key and must be kept secret.

The number e is known as the public exponent, the number d is known as the private exponent, and N is known as the modulus. When talking of key lengths in connection with RSA, what is meant is the modulus length.

An algorithm that uses different keys for encryption and decryption is said to be asymmetric.

Anybody knowing the public key can use it to create encrypted messages, but only the owner of the secret key can decrypt them.

Conversely the owner of the secret key can encrypt messages that can be decrypted by anybody with the public key. Anybody successfully decrypting such messages can be sure that only the owner of the secret key could have encrypted them. This fact is the basis of the digital signature technique.

Without going into detail about how e, d and N are related, d can be deduced from e and N if the factors of N can be determined. Therefore the security of RSA depends on the difficulty of factorizing N. Because factorization is believed to be a hard problem, the longer N is, the more secure the cryptosystem. Given the power of modern computers, a length of 768 bits is considered reasonably safe, but for serious commercial use 1024 bits is recommended.

The problem with choosing long keys is that RSA is very slow compared with a symmetric block cipher such as DES, and the longer the key the slower it is. The best solution is to use RSA for digital signatures and for protecting DES keys. Bulk data encryption should be done using DES.

3. Hash Functions

Hash functions, also called message digests, fingerprints and one-way encryption, are algorithms that, in some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file. Examples of hash algorithms are MD5 & SHA (Secure Hash Algorithm). The Digital Signature Algorithm (DSA) used for digital signatures uses a cryptographic hash function.

III. CONCLUSION

Benefits: The benefits of cryptography are well recognized. Encryption can protect communications and stored information from unauthorized access and disclosure. Other cryptographic techniques, including methods of authentication and digital signatures, can protect against spoofing and message forgeries.

Limitations: Less recognized are cryptography's limitations. Encryption is often oversold as the solution to all security problems or to threats that it does not address. For example, some people buy encryption software assuming that "Encryption could stop computer crackers". Unfortunately, encryption offers no such aegis. Moreover, the protection provided by encryption can be illusory. If the system where the encryption is performed can be penetrated, then the intruder may be able to access plaintext directly from stored files or the contents of memory or modify network protocols, application software, or encryption programs in order to get access to keys or plaintext data or to subvert the encryption process.

Drawbacks: The drawbacks of cryptography are frequently overlooked as well. The widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception (wiretaps) and documents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight. Cryptography poses a threat to organizations and individuals too. With encryption, an employee of a company can sell proprietary electronic information to a competitor without the need to photocopy and handle physical documents.

Hence we can say that we need to combine cryptography with conventional methods of securing data then only it can be used wisely.

REFERENCES

1. C. R. Blackman, 'Convergence between telecommunications and other media: How should regulation adapt?', Telecommunications Policy, vol. 22, no. 3, April 1998.
2. P. Budde, Information Technology Management Report 1997, Paul Budde Communication Pty Ltd, Bucketty, 1997.
3. M. L. James, 'Wait - there's more: the Internet on your very own home television!', Research Note no. 24, Department of the Parliamentary Library, Parliament of Australia, Canberra, February 1997.
4. M. L. James, 'Towards the Cashless Society?', Research Note no. 48, Department of the Parliamentary Library, Parliament of Australia, Canberra, 25 June 1996.
5. DIST, Stats.: e-commerce in Australia, Information Industries and Online Taskforce with www.consult, Canberra, April 1998. rmation for Authors, revised January 2006.
6. Book: - Data Communication and Networking by Behrouz A. Forouzan.
7. Internet: - Wikipedia and GPG Homepage.