RESEARCH ARTICLE OPEN ACCESS

General Summary of Cryptography

AdilJamil Zaru[1], Momeen Khan[2]

Abstract
Cryptographic mechanisms are an important security component of an operating system in securing the system itself and its communication paths. Indeed in many situations cryptography is the only tool that can solve a particular problem. It is the practice and study of techniques for secure communication in the presence of third parties. Modern cryptography is heavily based on mathematical theory, computer science practice and cryptographic algorithms. The algorithms are making in such a way it is difficult to break. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.
Keywords- foundations of cryptography, Plain Text, Cipher Text, Encryption,Security

Date of Submission: 10-02-2018 Date of acceptance: 28-02-2018

I. INTRODUCTION

Can increased security provide comfort to paranoid people? Or can security provide some very basic protections that we are naïve to believe that we can't need? During this time when the internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with it. One essential aspect for secure communications is that of cryptography.

Cryptography has been used for many years. Its main goal is to make sensitive information unreadable to all but the intended recipient. There are so many methods that once were popular for hiding this sensitive data. However researchers and cryptanalysis succeeded to attack the secrecy of a number of these methods. The cryptographic keys must be established between the sender and the receiver either manually or using trusted third party key management.

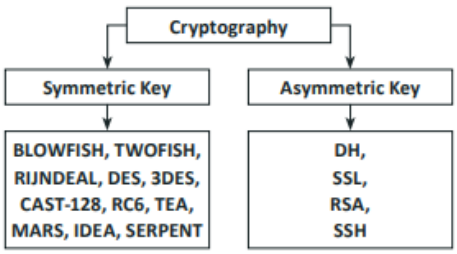

Figure-1 Classification of cryptographic algorithm

The basic classification of cryptographic algorithms is shown in Figure 1. Many authors have compared these algorithms on the basis of time complexity and space complexity. This paper compares these algorithms on the basis of parameters like key length and management, security and limitations pertaining to each algorithm.

II. PURPOSE OF CRYPTOGRAPHY

Cryptography is the science of writing in secret code and is an ancient art. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted 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.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication.

III. TYPES OF CRYPTOGRAPHIC ALGORITHMS

For purposes of this paper, cryptographic algorithms will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. In all cases the initial unencrypted data is

referred as plain text. In general there are three types of cryptographic schemes typically used to accomplish these goals.

- 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

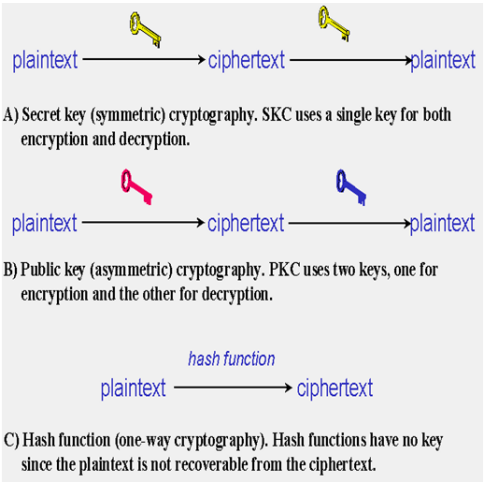

Figure 2: Three types of cryptography: secret-key, public key, and hash function

3.1. Secret Key Cryptography

Secret key cryptography is also called *symmetric cryptography* because the same key is used to both encrypt and decrypt the data. Well-known secret key cryptographic algorithms include the Data Encryption Standard (DES), triple-strength DES (3DES), Rivest Cipher 2 (RC2), and Rivest Cipher 4 (RC4).

With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

One of the major problems with secret key cryptography is the logistical issue of how to get the key from one party to the other without allowing access to an attacker.

Secret key cryptography algorithms that are in use today include:

- **Data Encryption Standard (Des):**

One of the most widely recognized secret-key block ciphers is the Data Encryption Standard (DES) algorithm. DES was developed by IBM cryptographers in the early 1970s and was adopted as a U.S. government standard in 1976. DES is intended for the protection of sensitive but unclassified electronic information. Because it uses the same key for both encryption and decryption, the algorithm is referred to as a symmetric cipher.

DES is a block cipher in which a 64-bit input plaintext block is transformed into a corresponding 64-bit ciphertext output. DES uses a 56-bit key expressed as a 64-bit quantity in which the least relevant bit in each of the 8 bytes is used for parity checking. DES is a Feistel algorithm that iterates over the data 16 times, using a combination of permutation and substitution transformations along with standard arithmetic and logical operations, such as XOR, based on the key value.

For many years, the DES algorithm withstood attacks. Recently, as the result of increased speed of computing systems, DES has succumbed to brute-force attack on several occasions, demonstrating its vulnerability to exhaustive searching of the key space.

Triple-DES

Triple-DES is the DES algorithm applied three times, using either two or three keys.

With two keys, Triple-DES proceeds by using the first key to encrypt a block of data. The second key is then used to decrypt the result of the previous encryption. Finally, the first key is once more used to encrypt the result from the second step. Formally, let us indicate the encrypting and decrypting functions based on a given key k with Ek and Dk, respectively. If k1 and k2 are the two Triple-DES keys and if m is the message to be encrypted, the encrypted

$$E_k(D_k(E_k(m))) = E_k(m)$$

message m′ is obtained as

To decrypt m′ and obtain the original plaintext m,

$$D_k(E_k(D_k(m'))) = D_k(m')$$

it is necessary to compute

The three-key Triple-DES, stronger than the two-key

Triple-DES, uses a separate key for each of the three steps described. With the notation that we have introduced, if k1, k2, and k3 are three distinct keys, a plaintext message m is encrypted into its corresponding ciphertext message m′ by

keys, a plaintext message m is encrypted into its corresponding ciphertext message m′ by

$$c_1 = E_k(v \oplus m_1)$$

To decrypt m′ and obtain the original

plaintext m, it is then necessary to compute

$c_i = E_k(c_{i-1} \oplus m_i)$ In Triple-DES, the second key is used for decryption rather than for encryption to allow Triple-DES to be compatible with DES. A system using Triple-DES can still initiate a communication with a system using DES by using only one key k. Formally, by choosing k1 = k2 =k3 = k, the ciphertext m′ corresponding to a plaintext message mis obtained from

Ek(Dk(Ek(m))) = Ek(m)

By contrast, m is obtained from m′ by computing

Dk(Ek(Dk(m'))) = Dk(m')

This shows that Triple-DES with only one key reduces itself to DES.

3.2. Public Key Cryptography

Public-key cryptography, or asymmetric cryptography, is an encryption scheme that uses two mathematically related, but not identical, keys - a public key and a private key. Unlike symmetric key algorithms that rely on one key to both encrypt and decrypt, each key performs a unique function. The public key is used to encrypt and the private key is used to decrypt.

It is computationally infeasible to compute the private key based on the public key. Because of this, public keys can be freely shared, allowing users an easy and convenient method for encrypting content and verifying digital signatures, and private keys can be kept secret, ensuring only the owners of the private keys can decrypt content and create digital signatures.

Since public keys need to be shared but are too big to be easily remembered, they are stored on digital certificates for secure transport and sharing. Since private keys are not shared, they are simply stored in the software or operating system you use, or on hardware (e.g., USB token, hardware security module) containing drivers that allow it to be used with your software or operating system.

Digital certificates are issued by entities known as Certificate Authorities (CAs).

The main business applications for public-key cryptography are:

Digital signatures - content is digitally signed with an individual's private key and is verified by the individual's public key

Encryption - content is encrypted using an individual's public key and can only be decrypted with the individual's private key.

3.3. Hash Function

Hash functions, also called message digests 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.

The ideal hash function has three main properties:

- It is extremely easy to calculate a hash for any given data.
- It is extremely computationally difficult to calculate an alphanumeric text that has a given hash.
- It is extremely unlikely that two slightly different messages will have the same hash.

Functions with these properties are used as hash functions for a variety of purposes, not only in cryptography. Practical application includes message integrity checks, digital signatures, authentication, and various information security applications.

A hash function takes a string of any length as input and produces a fixed length string which acts as a kind of "signature" for the data provided. In this way, a person knowing the "hash value" is unable to know the original message, but only the person who knows the original message can prove the "hash value" is created from that message.

A cryptographic hash function should behave as much as possible like a random function while still being deterministic and efficiently computable. A cryptographic hash function is considered "insecure" from a cryptographic point of view, if either of the following is computationally feasible:

Finding a (previously unseen) message that matches a given hash values.

Finding "collisions", in which two different messages have the same hash value.

An attacker who can find any of the above computations can use them to substitute an authorized message with an unauthorized one.

Ideally, it should be impossible to find two different messages whose digests ("hash values") are similar. Also, one would not want an attacker to be able to learn anything useful about a message from its digest ("hash values"). Of course the attacker learns at least one piece of information, the digest itself, by which the attacker can recognize if the same message occurred again.

In various standards and applications, the two most commonly used hash functions are MD5 and SHA-1.

IV. TRUST MODEL

There are a number of trust models employed by various cryptographic schemes. This section will explore three of them:

- The web of trust employed by Pretty Good Privacy (PGP) users, who hold their own set of trusted public keys.
- Kerberos, a secret key distribution scheme using atrusted third party.
- Certificates, which allow a set of trusted thirdparties to authenticate each other and, byimplication, each other's users.

Each of these trust models differs in complexity, generalapplicability, scope, and scalability.

V. CONCLUSION

This paper provides how anCryptography is used to achieve few goals likeConfidentiality, Data integrity, Authentication etc. of thesent data. Now, in order to achieve these goals variouscryptographic algorithms are developed by various people.For a very minimal amount of data those algorithmswouldn't be cost effective since those are not designed forsmall amount of data. A single algorithm is used for bothencryption and decryption i.e. it is fallen under secret keycryptographic algorithm. But as public key cryptography ismore secured then secret key algorithm. It is hard to saythat any one is better than the others; it depends upon yourapplication. One of the biggest and fastest growingapplications of cryptography today, though, is electroniccommerce (e-commerce), a term that itself begs for aformal definition. PGP's web of trust is easy to maintainand very much based on the reality of users as people.Kerberos overcomes many of the problems of PGP's web oftrust, in that it is scalable and its scope can be very large.

REFERENCES

[1]. Daemen, J. and Rijmen, V. (1999). AES Proposal: Rijndael. AES Algorithm Submission, September 3, http://www.nist.gov/CryptoToolKit

[2]. Joseph, D. P., Krishna, M. and Arun, K. (2015).Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms.International Journal of Advanced Research in Computer Science, vol. 6, no. 3.

[3]. Mandal, A. K., Parakash, C. and Tiwari, A. (2012). Performance evaluation of cryptographic algorithms: DES and AES. Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on. IEEE, 2012

[4]. Nadeem, A. and YounusJaved, M. (2005).A performance comparison of data encryption algorithms.Information and communication technologies, 2005.ICICT 2005.First international conference on. IEEE

[5]. Wade Trappe Lawrence C Washington "Introduction to Cryptography with Coding Theory 2 Editio" Pearson Pretnice Hall 2006

http://en.wikipedia.org/wiki/Cryptography#
http://www.wisegeek.com/what-are-cryptographicalgorithms.htm#didyouknowout

http://en.wikipedia.org/wiki/Asymmetric_key_algorithm
http://en.wikipedia.org/wiki/Digital_Signature_Algorithm
http://en.wikipedia.org/wiki/Elliptic_curve_cryptography
http://en.wikipedia.org/wiki/Blowfish_(cipher)

AdilJamil Zaru "General Summary of Cryptography "International Journal of Engineering Research and Applications (IJERA) , vol. 8, no. 2, 2018, pp. 68-71