Review on Cryptography Classification and its applications

TajinderKaur*
Sainik Institue,Ropar
tajindersaini1992@gmail.com

Abstract— In the past decades cryptography was only assumed to be used for military information and political communication secure and in protecting the national security. However, the use of cryptography was limited those days. But nowadays, the range of cryptography applications has been evolved. They are expanded a lot in the modern area as safety guards after the development of communication means as it is a way of safeguarding the crucial data from unauthorized access. It has appeared as a secure means for transmission of information from source to destination. It mainly helps in restricting intrusion from third party. It provides data confidentiality, electronic signatures, integrity, and advanced user authentication. The methods of cryptography use mathematics for securing the data (encryption and decryption).

Keywords— Cryptography, Encryption, Decryption, Cryptography applications

I. Introduction

Information security, sometimes shortened to **InfoSec**, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).[1]

Nowadays Information security plays a pivotal role during internet communication in today's era of technology. It is extremely important for people committing e-transactions. For naive people it may seem to be not that necessary or increased security may provide comfort to fearful people but the truth is that it is absolutely essential when communication is carried between tens of millions of people daily. There are various cryptography methods that provide a means for secure commerce and payment to private communications and protecting passwords. Cryptography is essential for secure communications; it is not by itself sufficient.

This paper will explain classification of cryptography and their applications. This paper elaborates about the classification and applicability of cryptography in our modern life.

II. CRYPTOGRAPHY

CRYPTOGRAPHY,IS ABOUT HIDING INFORMATION FROM THIRD PARTY ACCESS. IT IS THE SCIENCE USED TO TRY TO KEEP INFORMATION SECRET AND SAFE. MODERN CRYPTOGRAPHY IS A MIX OF MATHEMATICS, COMPUTER SCIENCE, AND ELECTRICAL ENGINEERING. CRYPTOGRAPHY IS USED IN ATM (BANK) CARDS, COMPUTER PASSWORDS, AND SHOPPING ON THE INTERNET.[2]

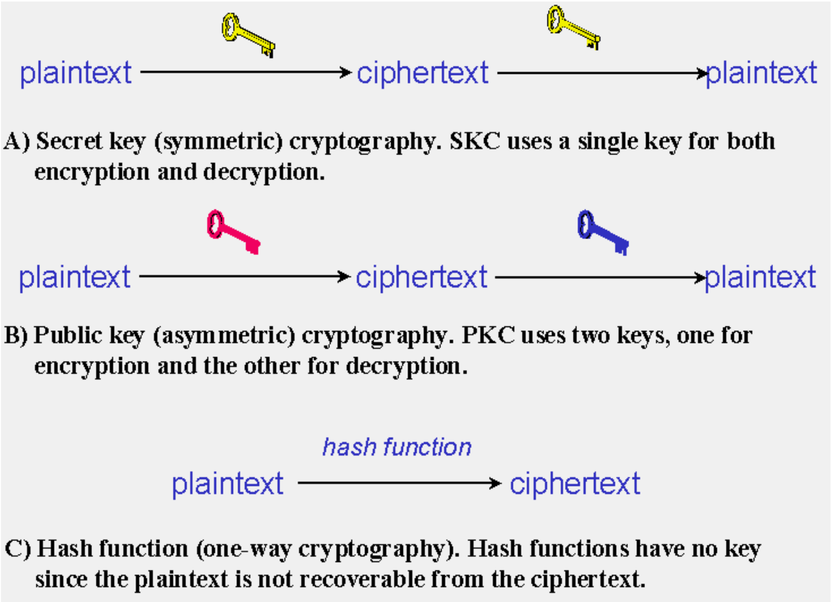
WHEN A MESSAGE IS SENT USING CRYPTOGRAPHY, IT IS CHANGED (OR ENCRYPTED) BEFORE IT IS SENT. THE METHOD OF CHANGING TEXT IS CALLED A "CODE" OR, MORE PRECISELY, A "CIPHER". THE CHANGED TEXT IS CALLED "CIPHER TEXT". THE CHANGE MAKES THE MESSAGE HARD TO READ. SOMEONE WHO WANTS TO READ IT MUST CHANGE IT BACK (OR DECRYPT IT). HOW TO CHANGE IT BACK IS A SECRET. BOTH THE PERSON THAT SENDS THE MESSAGE AND THE ONE THAT GETS IT SHOULD KNOW THE SECRET WAY TO CHANGE IT, BUT OTHER PEOPLE SHOULD NOT BE ABLE TO.

DIFFERENT TYPES OF CRYPTOGRAPHY CAN BE EASIER OR HARDER TO USE AND CAN HIDE THE SECRET MESSAGE BETTER OR WORSE. CIPHERS USE A "KEY" WHICH IS A SECRET THAT HIDES THE SECRET MESSAGES. THE CRYPTOGRAPHIC METHOD NEEDN'T BE SECRET. VARIOUS PEOPLE CAN USE THE SAME METHOD BUT DIFFERENT KEYS, SO THEY CANNOT READ EACH OTHER'S MESSAGES. SINCE THE CAESAR CIPHER HAS ONLY AS MANY KEYS AS THE NUMBER OF LETTERS IN THE ALPHABET, IT IS EASILY CRACKED BY TRYING ALL THE KEYS. CIPHERS THAT ALLOW BILLIONS OF KEYS ARE CRACKED BY MORE COMPLEX METHODS.

2.1 TYPES OF CRYPTOGRAPY ALGORITHMS

There are several ways of categorizing cryptographic algorithms. But I this paper they will be categorized based on the number of keys that are used for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are (Figure 1):

- *Secret Key Cryptography (SKC):* Uses a single key for both encryption and decryption; also called *symmetric encryption*. Primarily used for privacy and confidentiality.
- *Public Key Cryptography (PKC):* Uses one key for encryption and another for decryption; also called *asymmetric encryption*. Primarily used for authentication, non-repudiation, and key exchange.
- *Hash Functions:* Uses a mathematical transformation to permanently "encrypt" information, providing a digital fingerprint. Primarily used for message integrity.[3]



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Fig -1 Cryptography Techniques

A) Secret Key Cryptography(Symmetric Encryption)

In this method SKC method,only a same key for both encryption and decryption is used. As shown in Figure 1A, the sender uses the key to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key 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*.

With this type of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret.

Secret key cryptography algorithms in use today include:

- *Data Encryption Standard (DES)*
- *Advanced Encryption Standard (AES)*
- *International Data Encryption Algorithm (IDEA)*
- *GSM (Global System for Mobile Communications, originally Groupe Spécial Mobile) encryption and many more.*
-

B) Public Key Cryptography (Asymmetric Encryption)

In this type of cryptography, one key is used to encrypt, and a matching key is used to decrypt. These two keys together are called a **key pair**. One of these keys is called the **secret key** or **private key**, and should be kept secure. The *public key* is advertised as widely as the owner wants. The other key is designated the *private key* and is never revealed to another party. It is straight forward to send messages under this scheme. Suppose Alice wants to send Bob a message. Alice encrypts some information using Bob's public key; Bob decrypts the ciphertext using his private key. This method could be also used to prove who sent a message; Alice, for example, could encrypt some plaintext with her private key; when Bob decrypts using Alice's public key, he knows that Alice sent the message (*authentication*) and Alice cannot deny having sent the message (*non-repudiation*).

Public key cryptography algorithms that are in use today for key exchange or digital signatures include:

- *RSA:* named for the three MIT mathematicians who developed it — Ronald Rivest, Adi Shamir, and Leonard Adleman. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key.
- *Diffie-Hellman:* After the RSA algorithm was published, Diffie and Hellman came up with their own algorithm. D-H is used for secret-key key exchange only, and not for authentication or digital signatures.
- *Digital Signature Algorithm (DSA):* Digital Signature Standard (DSS), provides digital signature capability for the authentication of messages. And many more.

C) Hash Functions

Hash functions, also called *message digests* and *one-way encryption*, are algorithms that, in essence, use no key (Figure 1C). 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. Hash function which takes an input (or 'message') and returns a fixed-size alphanumeric string. The string is called the 'hash value', 'message digest', 'digital fingerprint', 'digest' or 'checksum').[4]

III. APPLICATIONS OF CRYPTOGRAPHY

Cryptography algorithms are widely being used to solve problems related to data confidentiality, data integrity, data secrecy and authentication and various other domains. It uses various cryptographic algorithms as
mentioned above as per requirement of the action. In the following section, the areas of applicability of
cryptography and its variants have been explained. The amount of distinction among all the variants of
cryptography is less because the entity in all the algorithms is information that needs to be secured.[5]
Some of the applications of Cryptography are as following:-

a) Communication Monitoring

Cryptography can provide extremely robust encryption; it can hold up the government's efforts to
legitimately perform electronic investigation. In order to meet this need, key is escrowed via entrusted third
party .This technology allows the use of strong encryption, but also allows the government when legally
authorized to obtain decryption keys held by escrow agents.

b) Secure Message Transmission

Most current secrecy systems for transmission use a private key system for transforming transmitted information because it is the fastest method that operates with reasonable assurance and low overhead.

If the number of communicating parties is small, key distribution is done periodically with a courier service and key maintenance is based on physical security of the keys over the period of use and destruction after new keys are distributed.
If the number of parties is large, electronic key distribution is usually used. Historically, key distribution was done with a special key-distribution-key (also known as a master-key) maintained by all parties in secrecy over a longer period of time than the keys used for a particular transaction. The "session-key" is generated at random either by one of the parties or by a trusted third party and distributed using the master-key.

c) Secrecy in Storage

Secrecy in storage is usually maintained by a one-key system where the user provides the key to the computer at the beginning of a session, and the system then takes care of encryption and decryption throughout the course of normal use. As an example, many hardware devices are available for personal computers to automatically encrypt all information stored on disk. When the computer is turned on, the user must supply a key to the encryption hardware. The information cannot be read meaningfully without this key, so even if the disk is stolen, the information on it will not be useable.

d) Integrity in Transmission

1) A typical technique for assuring integrity is to perform a checksum of the information being transmitted and transmit the checksum in encrypted form. Once the information and encrypted checksum are received, the information is again check summed and compared to the transmitted checksum after decryption. If the checksums agree, there is a high probability that the message is unaltered. Unfortunately, this scheme is too simple to be of practical value as it is easily forged.

e) Authentication of Identity

Authenticating the identity of individuals or systems to each other has been a problem for a very long time. Simple passwords have been used for thousands of years to prove identity. More complex protocols such as sequences of keywords exchanged between sets of parties are often shown in the movies or on television. Cryptography is closely linked to the theory and practice of using passwords, and modern systems often use strong cryptographic transforms in conjunction with physical properties of individuals and shared secrets to provide highly reliable authentication of identity.

f) Credentialing Systems

A credential is typically a document that introduces one party to another by referencing a commonly known trusted party. For example, when credit is applied for, references are usualy requested. The credit of the references is checked and they are contacted to determine the creditworthiness of the applicant. Credit cards are often used to credential an individual to attain further credit cards. A driver's license is a form of credential, as is a passport.

g) Electronic Signatures

Electronic signatures, like their physical counterparts, are a means of providing a legally binding transaction between two or more parties. To be as useful as a physical signature, electronic signatures must be at least as hard to forge, at least as easy to use, and accepted in a court of law as binding upon all parties to the transaction. The need for these electronic signatures is especially used in business dealings.

h) Electronic Cash

There are patents under force throughout the world today to allow electronic information to replace cash money for financial transactions between individuals. Such a system involves using cryptography to keep the assets of nations in electronic form. Clearly the ability to forge such a system would allow national economies to be destroyed in an instant. The pressure for integrity in such a system is staggering.

IV. Summary

Nowadays cryptography is widely used. Not only is it used over the Internet, but also it is used in phones, televisions, and a variety of other common household items. Without cryptography, hackers could get into our e-mail, listen in on our phone conversations, tap into our cable companies and acquire free cable service, or break into our bank/brokerage accounts.
Cryptography allows people to carry over the confidence found in the physical world to the electronic world, thus allowing people to do business electronically without worries of deceit and deception.

V. CONCLUSION

In this research paper the classifications and applications of cryptography in data security has been studied. Also the various cryptographic techniques have been observed and their specific areas of applicability have been found.

References

[1] https://en.wikipedia.org/wiki/Information_security

[2] https://simple.wikipedia.org/wiki/Cryptography

[3] www.garykessler.net/library/crypto.html#types

[4] https://simple.wikipedia.org/wiki/Cryptographic_hash_function

[5] http://all.net/edu/curr/ip/Chap2-4.html