

REVIEW AND CLASSIFICATION OF CRYPTOGRAPHY

Tarun Gupta¹, Anand Kumar², Shalini Tomar³

^{1,2,3}Hindu College of Engineering, Sonapat (India)

ABSTRACT

In the past cryptography was used in keeping military information, diplomatic correspondence secure and in protecting the national security. However, the use was limited. Nowadays, the range of cryptography applications have been expanded a lot in the modern area after the development of communication means cryptography is a way of safeguarding the crucial data from unauthorized access. It has emerged as a secure means for transmission of information. It mainly helps in curbing intrusion from third party. It provides data confidentiality, integrity, electronic signatures, and advanced user authentication. The methods of cryptography use mathematics for securing the data (encryption and decryption).

Keywords: *Cryptography, Data Confidentiality, Integrity, Electronic Signatures, Authentication, Encryption, Decryption*

I. INTRODUCTION

Information security plays a pivotal role during internet communication in today's era of technology. It is tremendously important for people committing e-transactions. For naive people it may seem to be not that necessary or increased security may provide comfort to paranoid 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 necessary for secure communications; it is not by itself sufficient. The reader of this paper will find variants of cryptography and their applications. This paper has two major purposes. The first is to provide some real examples of cryptography in use today. The second is to provide tabular summarization and conclusion.

II. CRYPTOGRAPHY

Cryptography is the practice and study of techniques for secure communication in the presence of adversaries. Typically, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. There are different types of cryptography. There is a sender, receiver, intruder of information and cryptographic tool that prevents intruder from trespass the sensitive information.

2.1 Types of Cryptography

2.1.1 Public Key Cryptography

It involves two pairs of keys: one for encryption and another for decryption. Key used for encryption is a public key and distributed. On the other hand key used for decryption is private key.

2.1.2 Key Escrow Cryptography

This technology allows the use of strong encryption, but also allows obtaining decryption keys held by escrow agents (third party-entrusted key escrow). The decryption keys are split into parts and given to separate escrow authorities. Access to one part of the key does not help decrypt the data; both keys must be obtained.

2.1.3 Translucent Cryptography

In this scheme the government can decrypt some of the messages, but not all. Only p fraction of message can be decrypted and $1-p$ cannot be decrypted. This is advantageous over key escrow or no key escrow cryptography as entire information is not at security risk.

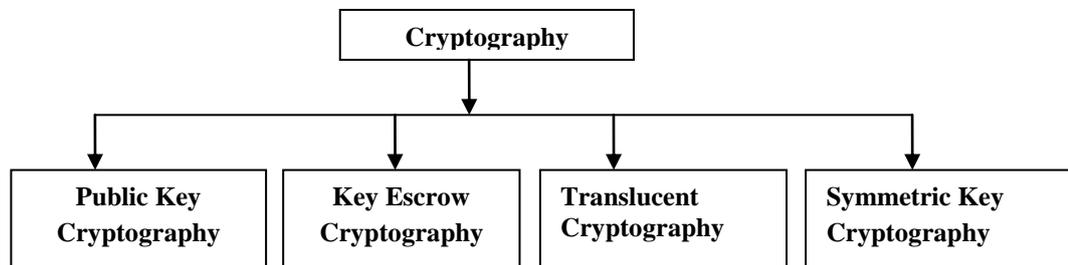


Figure 1: Classification of Cryptography Techniques

2.1.4 Symmetric Key Cryptography

Technique uses same key for encoding and decoding information. The sender and recipient of data must share same key and keep information secret preventing data access from outside.

III. APPLICATIONS OF CRYPTOGRAPHY

Cryptographic algorithms are widely being used to solve problems belonging 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.

3.1 Secure Message Transmission

The proxy signature schemes allow proxy signers to sign messages on behalf of an original signer, a company or an organization. It is based on the discrete logarithm problem. The sign encryption is a public-key primitive that simultaneously performs the functions of both digital signature and encryption. Integration of proxy signature and sign encryption public key paradigms provides secure transmission. It is efficient in terms of computation and communication costs. It is used for low power computers in which a given device may transmit and receive messages from an arbitrarily large number of other computers.

3.2 Communication Monitoring

Cryptography can provide tremendously robust encryption; it can impede the government's efforts to legitimately perform electronic reconnaissance. 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.

3.3 Fractional Observation of Data

Sometimes sender wants only part of the message to be monitored but not all. In that case Translucent cryptography is used that explores the space between opaque (strong encryption with no key escrow) and transparent (no encryption or encryption with key escrow). With translucent scheme, the government can decrypt some of the messages, but not all. Just as a translucent door on a shower stall provides some privacy, but not perfect privacy, translucent cryptography provides some communications privacy, but not perfect privacy.

3.4 Transferring Files on Network

Files that are to be exchanged between users need to be protected against malicious users and attackers. Symmetric Key cryptographic uses only single key for both encryption and decryption. In this technology symmetric key is then encrypted with public key which is associated with sender of file to obtain encrypted file and this encrypted file is then send to receiver. To decrypt the file, encrypted file system component driver uses private key which is associated with receiver to decrypt the symmetric key used to encrypt file. The encrypted file system component driver is then uses symmetric key to decrypt the file.

3.5 Certificates and Authentication

A certificate is an electronic document which identifies an individual, a server, a company, or some other entity and to associate that identity with a public key. Certificate authorities (CAs) issued certificate which binds a particular public key to the name of the entity that the certificate identifies (the name of an employee or a server). In addition to it, a certificate includes a serial number, name of certificate authority who issued it. And also it includes digital signatures of the issuing CA. Certificates help prevent the use of fake public keys for impersonation. Only the public key certified by the certificate will work with the corresponding private key possessed by the entity identified by the certificate.

3.6 Quantum Key Distribution

It is the best known application of quantum cryptography. It is a process to establish quantum communication between two parties for sharing a key (usually Alice and Bob), the third party don't know anything about the key. This can be achieved when Alice encode the bits before sending it to the Bob.

IV. SUMMARIZATION

In Table 1 a brief summary of the applications discussed in this research paper have been summarized.

Table 1: Brief Summary of Cryptography Techniques

S. No.	Cryptography	Brief description of the cryptography used
1.	Public Key Cryptography	Two pairs of keys used: Encryption and decryption key
2.	Key Escrow Cryptography	Third Party escrows the key
3.	Translucent Cryptography	Partial viewing of data based on the parameter
4.	Symmetric key cryptography	Single key used at both ends
5.	Quantum Cryptography	Single and Shared key is used at both ends

V. CONCLUSION

In this research paper the applicability of cryptography in data security has been studied and summarized. Also the various cryptographic techniques have been observed and their specific areas of applicability have been found out and a summarized table has been developed.

REFERENCES

- [1]. Survey Paper: Cryptography Is The Science Of Information Security. Mohammed AbuTaha, Mousa Farajallah, Radwan Tahboub, and Mohammad Odeh.2011, International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (3)
- [2]. Data Hiding in Image using least significant bit with cryptography. Mr. Vikas Tyagi. 2012 , International Journal of Advanced Research in Computer Science and Software Engineering, pp. 120-123.
- [3]. An overview of modern cryptography. Ahmed Al-Vahed and Haddad Sakhavi.2011, World Applied Programming, Vol (1), No (1), 55-61.
- [4]. A Survey on the Applications of Cryptography. Shivangi Goyal. 2012, International Journal of Science and Technology Volume 1 No. 3, 137-140.
- [5]. Advance cryptography algorithm for improving data security. Vishwa gupta, Gajendra Singh ,Ravindra Gupta. 2012, International Journal of Advanced Research in Computer Science and Software Engineering.