IJST EXPLORE International Journal of Science and Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-7318

International Journal of Science and Technology Volume 1 No. 3, March, 2012

A Survey on the Applications of Cryptography

Shivangi Goyal
University School Of Information Technology
Guru Gobind Singh Indraprastha University
16-C, Dwarka, Delhi

ABSTRACT

This paper gives a brief summary of cryptography, where it is applied and its usage in various forms. 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*

1. 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 naïve people it may seem to be not that necessary orincreased 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. Curious readers should check out some of the web pages and pdf in the bibliography below for further detailed — and interesting! — background information.

2. WHAT IS 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 allowsobtaining 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.

IJST © 2012 – IJST Publications UK. All rights reserved.

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.

3. 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 Using Proxy-Signcryption

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 signcryption is a public-key primitive that simultaneously performs the functions of both digital signature and encryption.

Integration of proxy signature and signcryption 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 Monitoring Communication

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. NIST has published the *Escrowed Encryption Standard* as FIPS 185.

3.3 Fractional Observing 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 (strongencryption 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. In this scheme the degree of translucency can be controlled by varyingparameter p.

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.

Technique Uses SSL Protocol

In this protocol server present its server identity to client. Process of authentication at server side includes public key encryption and digital signatures. Once it has been confirmed that it is server. After sever authentication, Client also present its identity to server. And once it’s also conformed both indulge in communication using symmetric-key encryption technique.

3.6 Digital Signature and Authentication

Authentication based on public key cryptography has an advantage over many other authentication scheme because no secret information has to be shared by the entities involved in the exchange. Authentication basically means something that is real or genuine. It is done in order to know the actual identity of a person. Authentication in private and public computer network including the internet is basically performed through the use of login passwords.

IJST © 2012 – IJST Publications UK. All rights reserved.

By the password it is assumed that the user is genuine, trustworthy or real.

A digital signature or we can also say digital certificate is an electronic signature that can be used to authenticate the identity of the sender of a message that has been sent is unchanged. A digital signature can be used with any kind of message like message send through electronic mail, whether it is encrypted or not so that the receiver can be sure of the sender's identity. A digital certificate contains the digital signature of the certificate- issuing authority so that anyone can verify that the certificate is real.

3.7 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.

One- Time Pad Protocol

One- Time Pad(OTP) algorithm is used to keep secrets. In binary string as a key, which is as long as message. The key is unknown to anyone else. At the sender side a cipher-text is generated by performing XOR operation between the key and the message. At receiver side, can reconstruct the message by performing XOR operation between the key and the cipher-text.

BB84 Protocol

BB84 was the first protocol implementing Quantum Key Distribution. It uses the concept of photon polarization. In this the key made up of number of bits that will be transmitted as photons. Each bit is encoded with a random polarization basis.

4. SUMMARIZATION

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

Table I. Summary of cryptographic applications

SNo.	Cryptography	Application area	Brief Description of the cryptography used	Examples
1.	Public Key Cryptography	Secure MessageTransmission using Proxy-Signcryption	Two pairs of keys used: Encryption and decryption key	Low power computers.
2.	Key Escrow Cryptography	Monitoring Communication	Third Party escrows the key	Used by Government agencies to monitor the content of the messages.
3.	Translucent Cryptography	Fractional Observing of Data	Partial viewing of data based on the parameter	Used by Government agencies where absolute monitoring is not required.
4.	Symmetric key cryptography	Transferring Files	Single key used at both ends	Document Files, Message authentication code
5.	Public key cryptography(SSL)	Certificates and Authentication	Uses two keys: public and private key	Password Authentication
6.	Public Key Cryptography	Digital Signature and Authentication	Two pairs of key used: public and private key	Electronic Mail
7.	Quantum Cryptography	Quantum Key Distribution	Single and Shared key is used at both ends	Used for secure communication over network

5. 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] http://msdn.microsoft.com/en-us/library/92f9ye3s.asp

[2] http://www.garykessler.net/library/crypto.html

[3] http://en.wikipedia.org/wiki/Cryptography

IJST © 2012 – IJST Publications UK. All rights reserved.

[4] http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter19.html

[5] http://searchsecurity.techtarget.com/definition/authentication

[6] http://en.wikipedia.org/wiki/Authentication

[7] http://en.wikipedia.org/wiki/Digital_signature#Digital_signatures_vs._ink_on_paper_signatures

[8] http://searchsecurity.techtarget.com/definition/digital-signature

[9] https://tspace.library.utoronto.ca/bitstream/1807/19307/1/Zhao_Yi_200911_PhD_Thesis.pdf

[10] http://www.academypublisher.com/proc/wisa09/papers/wisa09p363.pdf

[11] http://electronicsbus.com/?s=Application+Of+Cryptography+Include+Credit+Cards

[12] http://en.wikipedia.org/wiki/Encrypting_File_System

[13] http://technet.microsoft.com/en/us/library/cc700811.aspx

[14] https://developer.mozilla.org/en/Introduction_to_Public-Key_Cryptography

[15] http://www.garykessler.net/library/crypto.html

[16] http://www.ccavenue.com/content/faq_ecommerce.jsp

[17] http://en.wikipedia.org/wiki/Quantum_cryptography

[18] http://en.wikipedia.org/wiki/Quantum_key_distribution

[19] http://www.networkworld.com/news/2007/101007-quantum-cryptography-secure-ballots.html

[20] http://www.cki.au.dk/experiment/qrypto/doc/QuCrypt/b92coding.html

[21] http://www.networkworld.com/newsletters/optical/2004/0419optical2.html

[22] http://www.academypublisher.com/proc/wisa09/papers/wisa09p363.pdf

IJST © 2012 – IJST Publications UK. All rights reserved.