International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Cryptography – A Technical Review

Shobha Bhatt

Ambedkar Institute of Advanced Communication Technologies and Research, Delhi, India

ABSTRACT

This paper presents a technical review on cryptography. The paper starts with different goals of security. Modern cryptography techniques such as symmetric key, asymmetric key were discussed. The hash function and digital signature were explored. A comparative list of different methods for implementation of cryptosystem was presented with merits and demerits. For the deep understanding of cryptography, important concepts which are widely used were summarized. Further essential subset of knowledge required for cryptography described . As random numbers play very important role in cryptography. Use of random numbers in cryptography explained. A modest effort has been made to cover maximum important aspects related to cryptography. Finally studies were concluded with the importance of cryptography and related issues. This research work will definitely help new researchers to understand various concepts of cryptography.

Keywords : Cryptography, Symmetric , Asymmetric, Digital Signature, Hash Function, Random Number

I. INTRODUCTION

Cryptography is an art of secret writing and message hiding. The purpose of making a secure system [1] has three important goals mainly confidentiality, integrity and availability.

Confidentiality is protecting the information from disclosure to an unauthorized party. Nowadays we work with networked systems. We need to protect our valuable information such as password, credit, debit card. Hiding sensitive information in military mission is an essential requirement.

Integrity refers to consistency in message, methods, behavior, and outputs . Data base system incorporates integrity by allowing the only valid user may change his password with defined steps.

Availability means data is available as per need. It may be very frustrating when the user is not able to get money when it is urgently required.

Earlier Cryptography was used for military purpose. Commercial use [6] was introduced by the automatic teller machine (ATM) manufacturers. ATM Security application inspired other areas to use cryptography for commercial application.

Historical cryptographic system used the letter for encrypting the messages. Encryption is the process of encoding the message and decoding process is called decryption. Encryption is reversible process. The message [3] before the encryption is named as plain text and the encrypted message is named as cipher text. Cipher is an algorithm which is used to encrypt the plain text.

A cryptographic system can be divided into encryption and hashing. A hash function is an algorithm which converts the message into shorter fixed length character. Digital signatures are used to authenticate message senders.

Modern cryptographic algorithms are required to enhance data security. Different encryption algorithms are being used as per requirement of level of security concern.

As nowadays technology and internet usage is increasing day by day deep understanding of cryptography will be useful for developing different ways to protect valuable information over the internet automatically[21].

Paper is structured as follows. Section II is about different elements of modern cryptography. In this section symmetric key, asymmetric key, the hash function and digital signature explained. Lastly, this section was ended with the comparison of these techniques on the basis of different parameters. Section III describes important concepts widely used in cryptography. Section IV illustrates the subset of the knowledge required for developing a good cryptographic system. Section V describes the use of random numbers for secure system design. Lastly, Section VI concludes with the need of cryptography and related issues.

II. TYPES OF CRYPTOGRAPHY

There are three types of cryptographic techniques in literature as per modern cryptography namely the following.

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Hash Function

A. Symmetric Key Cryptography

In this method sender encrypts the message with key and receiver decodes the message with the same key. This process is reversible. Biggest problem is in this method is key distribution. But it is fast.

Symmetric key cryptography uses two techniques for encryption namely block and stream cipher. Block ciphers work on data block. Stream ciphers work on one bit at one time. Some popular symmetric key algorithms are Data Encryption Standard(DES), Triple DES, Blowfish, Two Fish[7], International Data Encryption Algorithm(IDEA), Serpent, Mars, RC6, and Rijndael[9] . These algorithms differ [1] in terms of architecture, security, flexibility, scalability . Most of the symmetric key block cipher have Feistal network and round function.

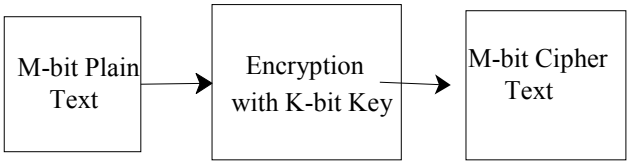

Figure 1: Encryption Process with Symmetric Key

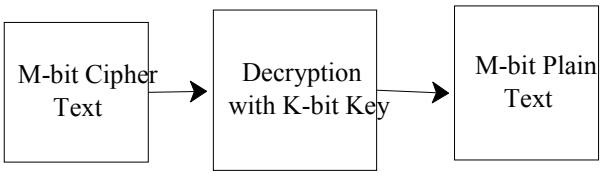

Figure 2: Decryption Process with Symmetric Key

B. Asymmetric Key Cryptography

It is two key cryptography technique. Sender encrypts the data with public key of the receiver and receiver decrypts the message with his private key. Asymmetric key has two uses authentication and confidentiality. Major algorithms used for asymmetric key cryptography are the following.

- Diffie-Hellman Key agreement
- Rivest Shamir Adleman(RSA)
- Elliptic curve cryptography(ECC)
- El Gamal
- Digital Signature Algorithms (DSA).

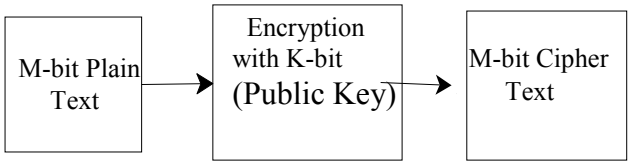

Figure 3: Encryption Process with Asymmetric Key

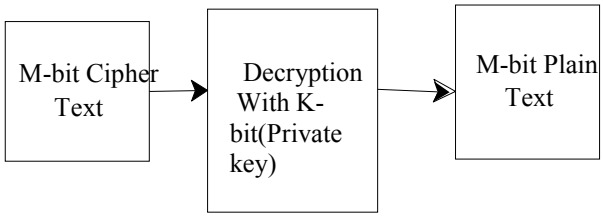

Figure 4 : Decryption Process with Asymmetric Key

Asymmetric cryptography is also used for digitally sign the document. Document is signed digitally with private key and it is verified with public key.

C. Hash Function

It is process which does not use any key. Small value is computed with hash function from plain text. This value is named as 'hash value', 'message digest' or 'checksum'. This works as signature for the data. Passwords in the data base are stored after applying hash function. For security passwords are not stored in the plain text format. Use of hash function is done for authentication and identity verification.

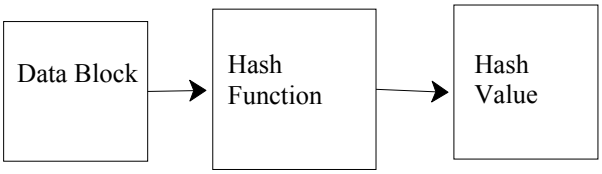

Figure 4: Hash Function

Popular hashing functions are.

- Message Digest(MD5)
- Secure Hash function (SHA)
- RACE Integrity Primitives Evaluation Message
- Digest(RIPEND)
- Whirlpool

D. Digital Signature

In digital signature sender creates a message digest from the message. This created message digest is encrypted with private key of the sender. After completing encryption we get the encrypted digest which is called signature. Sender sends the message with signature. Receiver decrypts the signature with public key of sender to get the original message digest. Receiver also computes new message digest from the message with the same hash function which was used by sender to generate message digest. This new message digest is now compared with original message which was got after decrypting the signature by receiver. If both the message digest are same then the message is not altered.

This way digital signature performs identification and message authentication. Identity of a user is done by sender on decryption of signature and message authentication is done by comparing the original message digest and new message digest [14],[18].

E. Differences among Symmetric, Asymmetric and Hash function

Every technique has its own merits and demerits. The following compares symmetric, asymmetric and hash function on the basis of methods used, reversibility of the operations, challenges, implementation, resource usage, application, speed and finally techniques for implementing these methods [19].

TABLE I
COMPARISON OF SYMMETRIC,ASYMMETRIC AND HASH FUNCTION

Feature	**Modern Cryptography Techniques**		
	Symmetric	**Asymmetric**	**Hash**
Method	Encryption and Decryption with same Key	Encryption and Decryption with different Keys called public and private	Hashing converts message in to small digest
Reversibility	Reversible	Reversible	Very hard to reverse
Problem	Problem with handling of the key	Proper handling of public key is required	Collision Problem
Implementation	Simple	Hard	Simple
Resource use	Use less resources	More resources	Less resources
application	Encryption	Encryption and Authentication	Integrity Checking and password storing
Speed	Fast	Slow	Fast
Popular Techniques	DES, Triple DES, Blowfish, Two Fish, IDEA, Serpent, Mars, RC6, and Rijndael	Diffie-Hellman Key agreement Rivest Shamir Adleman(RSA) Elliptic curve cryptography	Message Digest(MD5) Secure Hash function (SHA) RACE Integrity Primitives Evaluation

		(ECC) El Gamal Digital Signature Algorithms (DSA).	Message Digest(RIPEND) Whirlpool

III. IMPORTANT CONCEPTS IN CRYPTOGRAPHY

In this section different concepts regarding cryptography has been explored. First concept is cryptosystem. A cryptosystem consists of set of plaintexts, set of cipher texts, possible keys, encryption and decryption methods.

Other important work is Claude Shannon's article on the Communication Theory of Secrecy Systems" . This paper laid foundation for many concepts in modern cryptography. A cryptosystem has perfect secrecy if Pr[P | C] = Pr[P] . It mean that the a posteriori probability that the plaintext is P, where cipher text C is also observed, is identical to the a priori probability that the plaintext is P without observing cipher text is C[20].

Shanon characteristics of good cipher are as given below.

- Amount of secrecy needed should determine the amount of effort appropriate for encryption/decryption.
- Set of keys and enciphering algorithm should be free from complexity.
- Implementation should be simple
- Errors in ciphering should not propagate.

In developing cryptographic algorithms concept of confusion and diffusion is also used. The logic behind confusion is hiding the relation between the key and cipher text. By using this concept intruder is not able to guess the effect of cipher text changing on the key. Diffusion hides the relationship of cipher text and plaintext. Intruder will have hard time to find any relationship between plain text and cipher text.

One more concept is Kerckhoff's [14]principle, which states that cryptosystem should be secure even if all system details are public except key.

In cryptography the avalanche effect refers to the property that a minor change in plaintext or key should lead to major change in cipher text.

Key Handling [3] is also very essential task in key distribution in cryptographic system. Key Management can be implemented in several ways.

- Authenticated Key Management
- Deriving from a base Key using Key Derivation foundation (KDF)
- Creating a Key from Key parts held by different persons.

IV.SUBSET of KNOWLEDGE REQUIRED for CRYPTOGRAPHY

Cryptography is multidisciplinary fields. To develop a cryptographic system one needs to study mathematical concepts which include probability theory especially permutation and combination, number theory from abstract algebra, set theory, ring theory, group theory, finite fields, modular arithmetic concepts. Concepts of Fermat's little theorem, Euler's theorem, Euclidean theorem, discrete logarithms. Knowledge of algorithms for finding a prime number, greatest common divisor, multiplicative inverses, hash functions is essential for a deep understanding of the system.

Other fields include information theory concepts like entropy of the system and secrecy systems. Modular arithmetic operations, concepts of Boolean algebra like XOR operations are mostly used in cryptographic algorithms.

Some cryptographic algorithms are based on polynomials and elliptical curves.

Understanding of number theory is vital requirement for development of asymmetric cryptographic system.

One way function with trapdoor is used for implementation of asymmetric key cryptography. One way function is easy to compute in one direction and the reverse is very difficult. The trapdoor is the special information which makes computation easier in reverse direction.

Probability theory concepts are used in symmetric cryptography. Hashed functions are used for message authentication.

Well Known algorithms like Data Encryption Standard (DES) use probability concepts and XOR operations and Advanced Encryption Standard(AES) use GALOIS field.

V. CRYPTOGRAPHY AND RANDOM NUMBERS

Random numbers are essential for developing any secure system. Random numbers can be generated either from nature or from deterministic algorithms. Numbers generated from natural resources are called true random numbers and generated from deterministic algorithms [14] are called pseudorandom numbers. These numbers behave as random numbers.

Some popular [17]algorithms are the following.

- Blum Blum Shub
- Blum–Micali algorithm
- Complementary-multiply-with-arry
- Counter-based random number generator (CBRNG)
- Inversive congruential generator,
- Linear feedback shift register,
- Middle-square method
- Linear congruential generator
- ISAAC (cipher)
- Mersenne Twister

VI.CONCLUSION AND DISCUSSION

In the time of the computer and internet technology, secure transmission of information has become important concern for everyone. Today we do lot of business using on line systems over the internet. For military purpose security is a top concern. Cryptography plays important role for achieving the security goals. For achieving different aspects of secure system such as integrity, authentication and confidentiality various cryptographic algorithms have been invented. Every algorithm has its own advantages and disadvantages. This paper presents an insight view in to various important aspects of popular cryptographic techniques. This paper will surely benefit researchers to deeply understand the different cryptographic concepts and techniques for developing better cryptosystems.

VII. REFERENCES

[1]. Mansoor Ebrahim et.all: Symmetric Algorithm Survey: A comparative Analysis, International Journal of Computer Application (IJCA) Volume 61 no. 20, January (2013)

[2]. Saranayak et.al., "A Review on Symmetric Key Encryption Technology uses in Cryptography ", International Journal of Science,: Engineering and Technology and Research (IJSETR), Volume 3, Issue 3, March(2014)

[3]. Manoj Kumar Pandey, et.all.,: "Survey Paper: Crytography The art of Hiding Information", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: 2278-1323, Volume 2, Issue 12, December 2013.

[4]. William Stalling: Cryptography and Network Security: Principles and Practices", PHI Learning Private Limited, Fourth Edition (2009)

[5]. Christ of Paar, JanPelzl, amd Bartpreneel: "Understanding Cryptography: A Text book for student and Practitioners", Springer, (2010).

[6]. Ross J. Anderson,: "Why Cryptosystems Fail" Communications of the ACM, New York, USA, pp. 32-40, (1994.)

[7]. Bruce Schneier et al.,: "A Twofish Retreat:Related-Key Attacks Against Reduced-Round Twofish", Twofish Technical Report #6, February 14, 2000.

[8]. Frank Lin, Crypto: graphic's past, present and future role in society, Dec (2010.)

[9]. Daeman J Rijmen v: "The Rijandael block cipher", AES Proposal ,Belgica (1999)

[10]. Carolyn Burwick et all: The MARS Encryption Algoritmm August(1999)

[11]. Ronald L Rivest : The security of the RC6 Block Cipher, August(1998)

[12]. Dharitri Talukdar: Study on International Journal of Applied Research(2015)

[13]. Bruce Schneier,: "A self-Study Course in Block-Cipher Cryptanalysis

[14]. Bruce Schneier TwoFish, http://www.counterpane.com/twofish

[15]. Burke, Jerome, John McDonald, and Todd Austin. "Architectural support for fast symmetric-key cryptography." ACM SIGARCH

Computer Architecture News 28.5 (2000): 178-189
[16]. Sarris, Paraskevas, Lewis Mackenzie, and Soumyadeb Chowdhury. Novel Authentication Scheme for Online Transactions ." Proceedings of the 7th International Conference on Security of Information and Networks. ACM , 2014.
[17]. Forouzan, Behrouz A., and Debdeep Mukhopadhyay," Cryptography and Network Security (Sie)." McGraw-Hill Education, 2011
[18]. https://en.wikipedia.org/wiki/Random_number_generation accessed on 6/08/17
[19]. http://www.youdzone.com/signature.html last accessed on 5/08/17
[20]. Panda, S. N. "A proportional analysis on cryptography techniques, functions and relative performance issues." Journal of Global Research in Computer Science 2.6 (2011): 130-136.
[21]. http://www.ccs.neu.edu/home/riccardo/courses/csg252-fa06/lecture2.pdf(accessed on 6/08/17)
[22]. McDonald, Nicholas G.. "Past, Present, and Future Methods of Cryptography and Data Encryption." (2009).