Cryptography: Boon or Bane – A Review

B.Mohinder Singh, P.Balaji, K.Umamaheswari

Abstract - In this present world, everything is being digitalized. The most important thing is the data. Everything is represented as data. Sometimes the data is considered to be the sensitive or private ones. Sensitive data contains the data that is not to be shared to others without proper permissions. But, in this present world the data is theft by unauthorized ones. In these situations, to save the privacy of the data - it is to be encrypted to make it unreadable before digitalizing and needs to be decrypted to make the same readable. This can be achieved by "cryptography". This paper is a review paper about the data security and for whom it is a boon and bane for whom.

Index Terms – Authentication, Block cipher, Cryptography, Data, Decryption, Encryption, Hashing, Security, Stream cipher, Unauthorized

1 INTRODUCTION

1.1 Data

Data can be defined as a representation of facts, concepts or instructions in a formalized manner which should be suitable for communication, interpretation, or processing by human or electronic machine.

The latin word data is the plural of datum. Data is a set of values of qualitative or quantitative variables. Data is measured, collected and reported, and analysed, visualized using graphs or other analysis tools whenever required.

Before the development of computing devices and machines, only people could collect data and impose patterns on it. Since the development of computing devices and machines, these devices can also collect data. In the 2010s, computers are widely used in many fields to collect data and sort or process it, in disciplines ranging from marketing, analysis of social services usage by citizens to scientific research. Data is represented with the help of characters like alphabets (A-Z,a-z), digits (0-9) or special characters(+,-,/,*,<,>,= etc.).

Figure 1

1.2 Types of data

There are many types of data. Data like geographical data, cultural data, scientific data, financial data, statistical data, natural data, transport data, climatological data, personal data and other. The data can be of any format. But mostly it is in the text format – either as a text document or as data in table.

Figure 2

1.3 Need to secure the data

Sometimes the data should be secured from unauthorised persons. For example, A wants to send a sensitive information to B and it should not be accessed by anyone other than B. To make it secure some provisions are to be used.

The data can be secured by hiding the data or making the data impossible to read. This can be achieved by encrypting the data. The process of encrypting the data is called encryption or enciphering. There are many ways to encrypt the data. The encrypted data cannot be read or understand. To make the encrypted data readable it should be decrypted i.e., the reverse process of encryption. This is called decryption or deciphering. These can be achieved by "Cryptography".

2 CRYPTOGRAPHY

Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services.

- *B. Mohinder Singh is currently working as Assistant professor in Dept. of MCA, SIETK, Puttur, Chittoor Dt., AP,INDIA. PH-+919550978125. E-mail: mohindersingh83@gmail.com*
- *P. Balaji is currently working as Assistant professor in Dept. of CSE, SISTK, Puttur, Chittoor Dt., AP,INDIA. PH-+919885482633. E-mail: sistkcse.balaji@gmail.com*
- *K. Umamaheswari is currently pursuing masters degree program in Computer Applications in SIETK, Puttur, Chittoor Dt., AP,INDIA.*

Human being from ages had two inherent needs

- To communicate and share information and
- To communicate selectively.

These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand.

The age old cryptography is classical cryptography and the present one is called the Modern cryptography. Modern cryptography is the cornerstone of computer and communications security. Its foundation is based on various concepts of mathematics such as number theory, computational-complexity. It operates on binary bit sequences. It relies on publicly known mathematical algorithms for coding the information. Secrecy is obtained through a secrete key which is used as the input for the algorithms. The computational difficulty of algorithms, absence of secret key, etc., make it impossible for an attacker to obtain the original information even if he/she knows the algorithm used for coding. Modern cryptography requires parties interested in secure communication to possess the secret key only.

2.1 Objectives

The primary objective of using cryptography is to provide confidentiality, Data integrity, Authentication, Non-repudiation.

Confidentiality - It is a security service that keeps the information from an unauthorized person. Confidentiality can be achieved through numerous means starting from physical securing to the use of mathematical algorithms for data encryption.

Data Integrity - It is security service that deals with identifying any alteration to the data. Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized manner.

Authentication - Authentication provides the identification of the originator.

Non-repudiation - It is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action.

The various components of a basic cryptosystem are as follows −

- Plaintext.
- Encryption Algorithm.
- Cipher text.
- Decryption Algorithm.
- Encryption Key.
- Decryption Key.

2.2 Types of cryptosystems

There are several ways of classifying cryptographic algorithms. They are categorized based on the number of keys that are employed for encryption and decryption. The three types of algorithms are

- 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 irreversibly "encrypt" information, providing a digital fingerprint. Primarily used for message integrity.

3 SECRET KEY CRYPTOGRAPHY OR SYMMETRIC KEY ENCRYPTION

Secret key cryptography methods employ a single key for both encryption and decryption. Secret key cryptography is also called symmetric encryption, because a single key is used for both encryption and decryption functions.

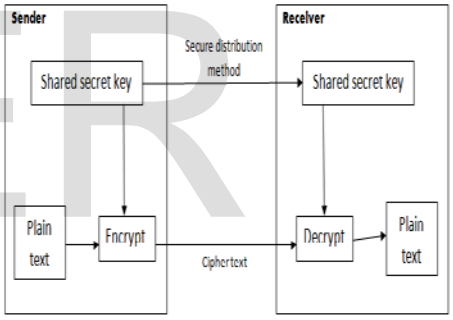

Figure 3

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. Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers.

3.1 Stream Ciphers

Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. Stream ciphers come in several flavors but two are worth mentioning here.

Self-synchronizing stream ciphers calculate each bit in the keystream as a function of the previous n bits in the keystream. It is termed "self-synchronizing" because the decryption process can stay synchronized with the encryption process merely by knowing how far into the n-bit keystream it is. One problem is error propagation; a

garbled bit in transmission will result in n garbled bits at the receiving side.

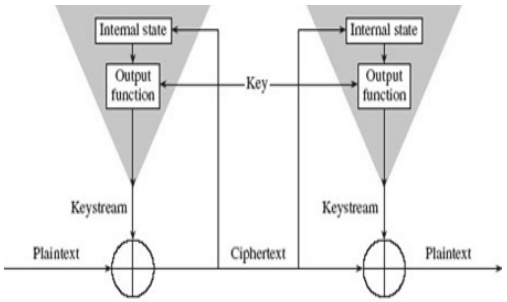

Figure 4

Synchronous stream ciphers generate the keystream in a fashion independent of the message stream but by using the same keystream generation function at sender and receiver. While stream ciphers do not propagate transmission errors, they are, by their nature, periodic so that the keystream will eventually repeat.

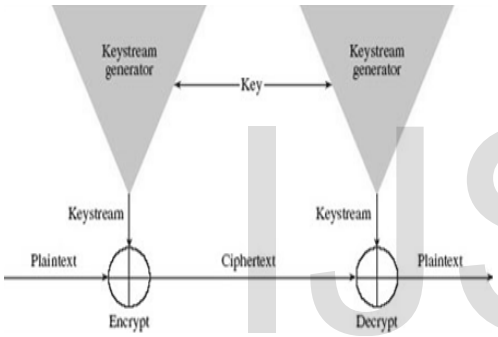

Figure 5

3.2 Block ciphers

A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher. The most common construct for block encryption algorithms is the Feistel cipher, named for cryptographer Horst Feistel (IBM). As shown in Figure 6, a Feistel cipher combines elements of substitution, permutation (transposition), and key expansion; these features create a large amount of "confusion and diffusion" in the cipher. One advantage of the Feistel design is that the encryption and decryption stages are similar, sometimes identical, requiring only a reversal of the key operation, thus dramatically reducing the size of the code (software) developed to implement the cipher.

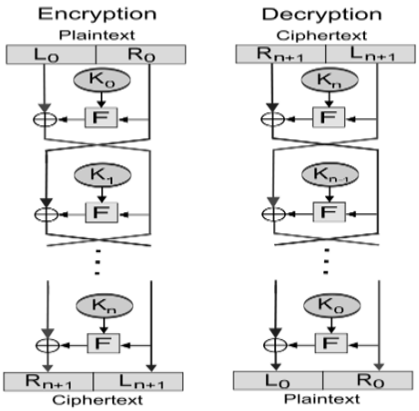

Figure 6

Block ciphers can operate in one of several modes; the following are the most important:

- *Electronic Codebook (ECB)* mode is the simplest, most obvious application: the secret key is used to encrypt the plaintext block to form a ciphertext block.
- *Cipher Block Chaining (CBC)* mode adds a feedback mechanism to the encryption scheme; the plaintext is exclusively-ORed (XORed) with the previous ciphertext block prior to encryption so that two identical plaintext blocks will encrypt differently.
- *Cipher Feedback (CFB)* mode is a block cipher implementation as a self-synchronizing stream cipher. CFB mode allows data to be encrypted in units smaller than the block size, which might be useful in some applications such as encrypting interactive terminal input.
- *Output Feedback (OFB)* mode is a block cipher implementation conceptually similar to a synchronous stream cipher. OFB prevents the same plaintext block from generating the same ciphertext block by using an internal feedback mechanism that generates the keystream independently of both the plaintext and ciphertext bitstreams.
- *Counter (CTR)* mode is a relatively modern addition to block ciphers. Like CFB and OFB, CTR mode operates on the blocks as in a stream cipher; like ECB, CTR mode operates on the blocks independently. Unlike ECB, however, CTR uses different key inputs to different blocks so that two identical blocks of plaintext will not reuslt in the same ciphertext. Finally, each block of ciphertext has specific location within the encrypted message. CTR mode, then, allows blocks to be processed in parallel – thus offering performance advantages when parallel processing and multiple processors are available.

Some of the secret key cryptography algorithms are:

Data Encryption Standard (DES): One of the most well-known and well-studied SKC schemes, DES was designed by IBM in the 1970s and adopted by the National Bureau of Standards (NBS) in 1977 for commercial and unclassified

government applications. DES is a Feistel block-cipher employing a 56-bit key that operates on 64-bit blocks. The National Security Agency (NSA) also proposed a number of tweaks to DES that many thought were introduced in order to weaken the cipher, but analysis in the 1990s showed that the NSA suggestions actually strengthed DES.
Two important variants that strengthen DES are:

- Triple-DES (3DES): A variant of DES that employs up to three 56-bit keys and makes three encryption/decryption passes over the block; 3DES is also described in FIPS 46-3 and is the recommended replacement to DES.
- *DESX*: A variant devised by Ron Rivest. By combining 64 additional key bits to the plaintext prior to encryption, effectively increases the keylength to 120 bits.

Advanced Encryption Standard (AES): In 1997, NIST initiated a very public, 4-1/2 year process to develop a new secure cryptosystem for U.S. government applications. The result, the Advanced Encryption Standard, became the official successor to DES in December 2001. AES uses an SKC scheme called Rijndael, a block cipher designed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The algorithm can use a variable block length and key length.

International Data Encryption Algorithm (IDEA): Secret-key cryptosystem written by Xuejia Lai and James Massey, in 1992 and patented by Ascom; a 64-bit SKC block cipher using a 128-bit key.

Rivest Ciphers (aka Ron's Code): Named for Ron Rivest, a series of SKC algorithms.

- RC1: Designed on paper but never implemented.
- RC2: A 64-bit block cipher using variable-sized keys designed to replace DES. It's code has not been made public although many companies have licensed RC2 for use in their products.
- RC3: Found to be breakable during development.
- RC4: A stream cipher using variable-sized keys; it is widely used in commercial cryptography products.
- RC5: A block-cipher supporting a variety of block sizes (32, 64, or 128 bits), key sizes, and number of encryption passes over the data.
- RC6: A 128-bit block cipher based upon, and an improvement over, RC5; RC6 was one of the AES Round 2 algorithms.

4 PUBLIC KEY CRYPTOGRAPHY or ASYMMETRIC KEY ENCRYPTION

Public key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key.

PKC depends upon the existence of so-called one-way functions, or mathematical functions that are easy to compute whereas their inverse function is relatively difficult to compute. Generic PKC employs two keys that are mathematically related although knowledge of one key does not allow someone to easily determine the other key. One key is used to encrypt the plaintext and the other key is used to decrypt the ciphertext. The important point here is that it does not matter which key is applied first, but that both keys are required for the process to work. Because pair of keys is required, this approach is also called asymmetric cryptography.

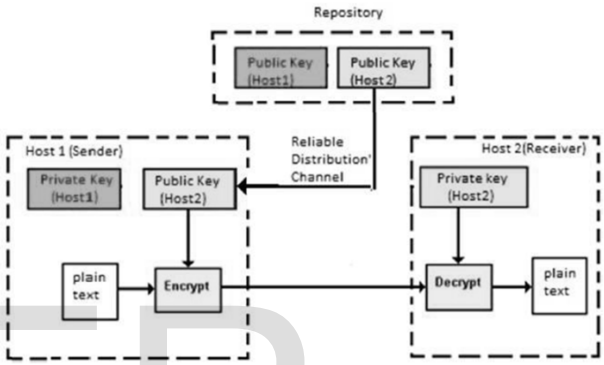

Figure 7

Some of the Public key cryptography algorithms include:

RSA: The first, and still most common, PKC implementation, 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. The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors. The public key information includes n and a derivative of one of the factors of n; an attacker cannot determine the prime factors of n (and, therefore, the private key) from this information alone and that is what makes the RSA algorithm so secure.

Digital Signature Algorithm (DSA): The algorithm specified in NIST's Digital Signature Standard (DSS), provides digital signature capability for the authentication of messages.

Elliptic Curve Cryptography (ECC): A PKC algorithm based upon elliptic curves. ECC can offer levels of security with small keys comparable to RSA and other PKC methods. It was designed for devices with limited compute power and/or memory, such as smartcards and PDAs.

	Symmetric Cryptosystems	Public Key Cryptosystems
Relation between Keys	Same	Different, but mathematically related
Encryption Key	Symmetric	Public
Decryption Key	Symmetric	Private

Figure 8

5 HASH FUNCTIONS

Hash functions, also called message digests and one-way encryption, are algorithms that, in essence, 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.

Hash algorithms that are in common use today include:

Message Digest (MD) algorithms: A series of byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message.

- MD2 (RFC 1319): Designed for systems with limited memory, such as smart cards. (MD2 has been relegated to historical status, per RFC 6149.)
- MD4 (RFC 1320): Developed by Rivest, similar to MD2 but designed specifically for fast processing in software. (MD4 has been relegated to historical status, per RFC 6150.)
- MD5 (RFC 1321): Also developed by Rivest after potential weaknesses were reported in MD4; this scheme is similar to MD4 but is slower because more manipulation is made to the original data.

Secure Hash Algorithm (SHA): Algorithm for NIST's Secure Hash Standard (SHS).

- SHA-1 produces a 160-bit hash value and was originally published as FIPS PUB 180-1 and RFC 3174. It was deprecated by NIST as of the end of 2013 although it is still widely used.
- SHA-2, originally described in FIPS PUB 180-2 and eventually replaced by FIPS PUB 180-3 (and FIPS PUB 180-4), comprises five algorithms in the SHS: SHA-1 plus SHA-224, SHA-256, SHA-384, and SHA-512 which can produce hash values that are 224, 256, 384, or 512 bits in length, respectively. SHA-2 recommends use of SHA-1, SHA-224, and SHA-256 for messages less than 264 bits in length, and employs a 512 bit block size; SHA-384 and SHA-512 are recommended for messages less than 2128 bits in length, and employs a 1,024 bit block size. FIPS PUB 180-4 also introduces the concept of a truncated hash in SHA-512/t, a generic name referring to a hash value based upon the SHA-512 algorithm that has been truncated to t bits; SHA-512/224 and SHA-512/256 are specifically described. SHA-224, -256, -384, and -512 are also described in RFC 4634.
- SHA-3 is the current SHS algorithm. Although there had not been any successful attacks on SHA-2, NIST decided that having an alternative to SHA-2 using a different algorithm would be prudent. The NIST version can support hash output sizes of 256 and 512 bits.

6 CONCLUSION

The data that are digitalized can be secured from unauthorized accessing by encrypting the data. The different encryptions were briefed above. Surely, this is a *boon* for the ones who have their data digitized, want their data secure and *bane* for those who want to access the data unauthorizedly.

7 REFERENCES

[1] R. J. Anderson, ed., Information hiding: rst international workshop, vol. 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, May 1996, Springer-Verlag, Berlin, Germany, ISBN 3-540-61996-8.

[2] D. Kahn, The Codebreakers The Story of Secret Writing. New York, New York, U.S.A.: Scribner, 1996, ISBN 0-684-83130-9.

[3] B. Figg. (2004). Cryptography and Network Security. Internet:

[4] http:/www.homepages.dsu.edu/figgw/Cryptography%20&%20Network%2 0Security.ppt. [March 16, 2010].

[5] Kahate, Cryptography and Network Security (2nd ed.). New Delhi: Tata McGraw Hill, 2008.

[6] M. Milenkovic. Operating System: Concepts and Design, New York: McGrew-Hill, Inc., 1992.

[7] P.R. Zimmermann. An Introduction to Cryptography. Germany: MIT press. Available: http://www.pgpi.org/doc/pgpintro, 1995, [March 16, 2009].

[8] W. Stallings. Cryptography and Network Security (4th ed.). Englewood (NJ):Prentice Hall, 1995.

[9] V. Potdar and E. Chang. "Disguising Text Cryptography Using Image Cryptography," International Network Conference, United Kingdom: Plymouth, 2004.

[10] S.A.M. Diaa, M.A.K. Hatem, and M.H. Mohiy (2010). "Evaluating The Performance of Symmetric Encryption Algorithms" International

Journal of Network Security, 2010, 10(3), pp.213-219

[11] T. Ritter. "Crypto Glossary and Dictionary of Technical Cryptography'. Internet: www.ciphersbyritter.com/GLOSSARY.HTM , 2007, [August 17, 2009]

[12] K.M. Alallayah, W.F.M. Abd El-Wahed, and A.H. Alhamani."Attack Of Against Simplified Data Encryption Standard Cipher System Using Neural Networks". Journal of Computer Science,2010, 6(1), pp. 29-35.

[13] D. Rudolf. "Development and Analysis of Block Cipher and DES System". Internet: http://www.cs.usask..ca/~dtr467/400/, 2000, [April 24, 2009]

[14] H. Wang. (2002). Security Architecture for The Teamdee System. An unpublished MSc Thesis submitted to Polytechnic Institution and State University, Virginia, USA.

[15] G.W. Moore. (2001). Cryptography Mini-Tutorial. Lecture notes University of Maryland School of Medicine. Internet: http://www.medparse.com/whatcryp.htm [March 16, 2009].

[16] T. Jakobsen and L.R. Knudsen. (2001). Attack on Block of Ciphers of Low Algebraic Degree. Journal of Cryptography, New York, 14(3), pp.197-210.

[17] N. Su, R.N. Zobel, and F.O. Iwu. "Simulation in Cryptographic Protocol Design and Analysis." Proceedings 15th European Simulation Symposium, University of Manchester, UK., 2003.