International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 10, October - 2013

Cryptography and Cryptanalysis: A Review

Gangadhar Tiwari
NIT, Durgapur

Debashis Nandi
NIT, Durgapur

Madhusudhan Mishra
NERIST, Itanagar

Abstract

At times it is important to communicate secret information to an individual or to a group of selected people and if it is intercepted and changed by an intruder may lead to undesired problems. To protect confidential information and to communicate it to the person(s) concerned is a crucial task. One of the techniques used for this is Cryptography that ciphers the information based on certain algorithm that makes it human unreadable unless decrypted in a predefined method set by the information sender. A large variety of cryptographic techniques are used which have their own strengths and weaknesses. Digital data especially image files are widely used over internet. This paper is an effort to give an overview of multimedia data cryptography and cryptanalysis and employing chaotic sequences as possible solution for image encryption over traditional cryptographic algorithms.

I. Introduction

Cryptography is a means for secret communication where the messages are scrambled through an encryption process to produce an unreadable cipher text that needs to undergo decryption to retrieve back the original message. It protects messages from unauthorized access where there is no access control.

Various Cryptography terminologies are projected in Table-I. In this paper the section II discusses the security requirements for cryptographic applications and various Cryptographic techniques based on key usage. Section III briefs about Chaos theory and its application to cryptography with special reference to image encryption. Section IV is devoted on Cryptanalysis and Section V draws the conclusion and future scope in this field.

Table-I

Keywords	Definition
Plaintext	Digital data to be protected denoted by *M*.
Cipher text	It is an encrypted message denoted by *C*
Key	It refers to numeric value used by an algorithm to cipher information making it recoverable by corresponding key.
Encryption	Method of hiding a message *M*. If *E* denotes the encryption function and *k* is key, then $\boldsymbol{E_k}\ (\boldsymbol{M}) = \boldsymbol{C}$
Decryption	Recovering encrypted text back. If *D* denotes the decryption function and *k* is key then $\boldsymbol{D_k}\ (\boldsymbol{C}) = \boldsymbol{M}$

II. Cryptography- Requirements and Techniques

A. Requirements

With respect to application based communication, there exists certain security requirements which includes: V**alidation (**the method of ensuring the user's identity), **Confidentiality (**Ensuring that the message can be read by the intended user only), C**onsistency (**Assuring the receiver that the message gets original message) and **Non-refutation (**A system to ensure that the sender really sent the message received by the user) **[2, 3]**.

B. Types of Cryptography based on the Key Usage

It includes hash functions, symmetric key cryptography and public key cryptography. The variant and there security analysis is discussed as below:

1. Hash Functions: Also called message digests and one-way encryption, it uses a mathematical transformation to irreversibly encrypt information. Rather than using keys; a fixed-length one-way hash value is computed based upon the plaintext. It is well-

suited for ensuring data integrity. Some of the common Hash algorithms include:

Message Digest (MD) algorithms: It is a series of byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message. The different version includes-

MD2-It is defined in **RFC 1319** and is designed for systems with small memory. However, it is insecure against collisions attack (Rogier et al, 97) and preimage attack (Muller, 04).

MD4: It is defined by **RFC 1320** and designed specifically for fast processing in software. The digest length is 128 bits. But its security is breached by full collision attack (Dobbertin, 1995 and, Wang et al, 2004,) and theoretical preimage attack (Leurent, 2008).

MD5: It is defined in **RFC 1321**. It is similar but slower to MD4 as more manipulation is made to the original data. It produces a 128-bit hash value. Key usage includes checking data integrity. However, MD5 is not secure against collision attack.

Secure Hash Algorithm (SHA): The three SHA algorithms are structured differently and are **SHA-0**, SHA-**1** and **SHA-2**.

SHA-1: It is produces a 160-bit hash value and was originally published as FIPS 180-1 and is described in **RFC 3174**. However in 2005, security flaws were identified in SHA-1.

SHA-2: It describes four algorithms in the SHA: SHA-224, SHA-256, SHA-384, and SHA-512 which can produce 224, 256, 384, or 512 bits long hash values, respectively. SHA-224, -256, -384, and -512 are defined in **RFC 4634**. SHA-256 and SHA-512 are computed with 32- and 64-bit words, respectively. It uses different shift amounts and additive constants but have similar structure differing in number of iterations. SHA-224 and SHA-384 are curtailed versions of the first two, computed with different initial values. The best public cryptanalysis shows attack breaking pre-image resistance for 46 out of 80 rounds of SHA-512, and 41 out of 64 rounds of SHA-256. Efforts are underway to develop improved alternatives and SHA-3, is currently under development.

RIPEMD: It is a series of message digests that initially came from the RIPE (RACE Integrity Primitives Evaluation) project. The 256 and 320-bit versions reduces accidental collision, but don't provide better security (against preimage attack) as compared to RIPEMD-128 and RIPEMD-160.

HAVAL (HAsh of VAriable Length): Designed by Zheng et al, it is a hash algorithm with many levels of security. It can create hash values that are 128, 160, 192, 224, or 256 bits in length. HAVAL also allows users to specify the number of rounds (3-5) to be used to generate the hash. The HAVAL hashes are represented by 32, 40, 48, 56 or 64-digit hexadecimal numbers. However, HAVAL is no more secure after collision attack by Wang et al, 2004.

Whirlpool: It operates on messages with length less than 2^{256} bits, and generates 512 bits hash. However, in 2009 a rebound attack was announced that presents full collisions against 4.5 rounds of Whirlpool in 2^{120} operations making it insecure.

Tiger: Designed by Anderson et al, it is secure and works efficiently on 64-bit processors. Tiger-192 produces a 192-bit output. However, cryptanalysis attacks (Kelsey et al, Mendel et al, collision finding attack,) shows that it is no more secure.

2. Secret key cryptography (SKC)

It uses a single key for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. The main problem with it is how to create, store and transmit key to those who need to decrypt messages. Mathematically, equation pair (1-2)

$$\boldsymbol{E_k}\ (\boldsymbol{M}) = \boldsymbol{C} \qquad (\mathbf{1})$$

$$\boldsymbol{D_k}\ (\boldsymbol{C}) = \boldsymbol{M} \qquad (\mathbf{2})$$

represents encryption and decryption process. It is obvious that the key must be known to both sender and receiver; that is the secret. It is categorized into **stream ciphers** and **block ciphers**.

Stream ciphers operate on a single bit at a time and implement some form of feedback mechanism so that the key is constantly changing. **A block cipher** scheme encrypts one block of data at a time using the same key on each block. Here, the same plaintext block will always encrypt to the same cipher text when using same key in a block cipher. Block ciphers can operate in four modes viz. Electronic Codebook mode, Cipher Block Chaining mode, Cipher Feedback mode and Output Feedback mode.

Some of the secret key algorithms are described as below:

Data Encryption Standard (DES): It is a block-cipher employing a 56-bit key that operates on 64-bit blocks **[1].** The number of rounds employed is 16 and has a structure of Balanced Feistel network. It employs Shift permute operation for key generation and the mathematical operation is XOR. DES was designed specifically to yield fast hardware implementations and slow software implementations. However, DES is insecure due to the 56-bit key size being too small and hence obsolete. Further cryptanalysis shows that a brute force attack is possible. As of 2008, linear cryptanalysis attack requires 2^{43} known plaintexts (Junod, 2001).

Triple DES: It is a block cipher that applies the DES cipher algorithm three times to each data block. The key size is 112/168 with 48 numbers of rounds and sub keys. The shift permute method is employed for key generation and has a Feistel network structure. The cryptanalysis attacks are 2^{32} known plaintexts (Lucks) and 2^{28} target keys with chosen plaintexts per key (Biham). However, this is not currently practical and NIST considers it to be appropriate.

International Data Encryption Algorithm: It is a block cipher based algorithm that operates on 64-bit blocks using a 128-bit key, and consists of a series of eight similar transformations and an output transformation. The encryption and decryption schemes are similar. It derives security by interleaving operations from different groups. The cryptanalysis shows a high-order differential-linear attack requiring $2^{64} - 2^{52}$ and chosen plaintexts breaking 6 rounds with a complexity of $2^{126.8}$ encryptions (Biham et al., 2007). Till now IDEA is secure.

Advanced Encryption Standard: It is based on a substitution-permutation network but does not use a Feistel network **[5]**. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. AES has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. It operates on a 4×4 column-major order matrix of bytes. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of ciphertext. The first key-recovery attacks on full AES were by Bogdanov et al 2011. However, all known attacks are computationally infeasible.

Blowfish is a keyed, symmetric block cipher. The key design features include key-dependent S-boxes and a highly complex key schedule. Blowfish has a 64-bit block size with variable key length ranging from 32-448 bits. It employs 16-round Feistel cipher and large key-dependent S-boxes. The cryptanalysis shows that four rounds of Blowfish are susceptible to a 2^{nd} -order differential attack (Rijmen, 1997).

3. Public key Cryptosystems (PKC)

PKC depends upon the existence of *one-way functions* that are easy to compute whereas their inverse function is relatively difficult to compute. It has two different keys for data transmission. There exists a mathematical relation between the two keys so that if one is used to encryption other can be used for decryption. It includes a Private Key (known only to owner) and a public key distributed to any user who requests it. Mathematically, the following equations

$$\boldsymbol{E_{k1}}\ (\boldsymbol{M}) = \boldsymbol{C} \qquad (3)$$
$$\boldsymbol{D_{k2}}\ (\boldsymbol{C}) = \boldsymbol{M} \qquad (4)$$

represent the encryption and decryption process where we have a key pair **(k1, k2**), **k1** being public and **k2** private. This method could be best used for **non-repudiation**. Some PKC are:

RSA: It employs Chinese Remainder Theorem for key generation while the mathematical operation is factoring problem. RSA uses a variable size encryption block and a variable size key (1024 to 4096). The cryptanalysis shows that a 768 bit key has been broken **[12]**. RSA is used in software products, for digital signatures, key exchange, and encryption of small data blocks.

Diffie-Hellman: It allows two parties to jointly establish a shared secret key over an insecure communications channel that can be for encrypting ensuing communications using a symmetric key cipher. The Diffie–Hellman key agreement provides the basis for authenticated protocols, and is used to provide perfect forward secrecy in Transport Layer Security's ephemeral modes.

Digital Signature Algorithm-The algorithm specified in NIST's Digital Signature Standard, provides digital signature capability for the authentication of messages. Key generation has two phases. The first phase is choice of algorithm parameters while the second phase computes public and private keys for a single user.

Elliptic Curve Cryptography: A PKC algorithm based upon elliptic curves over finite fields. It offers levels of security with small keys comparable to RSA. It is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible.

Even though Triple-DES and IDEA etc. can achieve high security, it is not suitable for multimedia applications due to its large data sizes and real time constraint. In SKC, secure key exchange between two parties is a major limitation. Using PKC for encryption is very slow. Hence these systems are not up to mark and we need to find alternate solution. A solution to this can be to use chaotic encryption where, the encryption algorithm manipulates the pixels of an image instead of manipulating the bits of the image.

III. Chaotic Cryptography for Image Encryption

A. Theory of Chaos

It means "a state of disorder". It becomes non-linear if its parameter, internal variable, external signals, control variable, or even initial value is chosen in a specific way. This unpredictability of a deterministic system is termed as chaos. It is based on the fact that simple rules when iterated can give rise to complex behaviour. For a dynamical system to be chaotic, it must have the following properties:

1. It must be **sensitive to initial conditions exponentially**: It means that each point in such a system is arbitrarily closely approximated by other points with different future trajectories.
2. It must be **topologically mixing**: It means that the system will evolve over time so that any given region or open set of its phase space will eventually overlap with other region.
3. Its **periodic orbits must be dense**: It means that every point in the space is approached closely by periodic orbits.

B. Similarities in Chaotic maps and cryptography

This includes sensitivity to a change in initial conditions and parameters, unstable periodic orbits with long periods and random-like behaviour **[4]**. The diffusion and confusion properties required in a cryptographic algorithm are achieved through the iteration. The iterations of a chaotic map spread the initial region over the entire phase space **[11]**. The parameters of the chaotic map may represent the key of the encryption algorithm. Chaotic systems are very sensitive to initial conditions and system parameters. For a given set of parameters in chaotic regime, two close initial conditions lead the system into divergent trajectories. Therefore encryption/ decryption scheme can be obtained if the parameters are chosen as “Keys” and “Trajectories” are used for the same. Since the same parameters are used for encryption and decryption, the chaos scheme is symmetric **[9]**. The parameters and the initial conditions form a very large key space thereby enhancing the security of the code. This review discusses some of the recent chaotic encryption techniques in brief:

C. Existing Methods for Chaotic Image Encryption

Baptista Method: Baptista uses logistic map in which the iterates are generated using the equation:

$$\mathbf{x_{n+1} = r x_n (1 - x_n)} \qquad (5)$$

by choosing the parameter r for chaotic regime and with initial condition $x_0 \in [0,1]$. However the security analysis shows following four defects in it **[6]**. The distribution of the cipher text is non-uniform, the encryption is speed very slow, the cipher text size is larger than the plaintext size and it is insecure against some different attacks **[7]**. Therefore we need to look for some new algorithm.

Zhang et al (2011) proposed a method based on logistic map and cheat image where he chooses the initial condition and control parameter of logistic map as the secret key **[8]**. But there exists weakness, such as small key space making it insecure.

Yong et al (2011) proposed another image encryption methods using PN Sequence in chaotic maps **[10]**. Here a secret key is defined as initial conditions for a chaotic map such as logistic map. The security analysis shows that for any pixel of the plain image, encryption and decryption scheme is unreasonable and that decryption scheme is incorrect.

IV. Cryptanalysis

It is the reverse process of cryptography. The objective of cryptanalyst is to be able to decrypt cipher text.

A. Attacks on Key based Cryptography

Cipher text Only Attack- Here the attacker obtains a sample of cipher text without the plaintext associated with it.

Known Plaintext Attack- The attacker obtains the sample of cipher text and the corresponding plaintext.

Chosen Plaintext Attack-The attacker can choose the quantity of plaintext and then obtain the corresponding encrypted cipher text.

Adaptive Chosen plaintext attack- A cryptanalyst can mount this attack when he has decryption hardware but is unable to extract the decryption key from it.

Brute Force Attack: Here key size provides a lower bound on the security of the cryptosystem.

Related Key Attack: Here the attacker can observe the operation of cipher under different keys whose values are initially unknown but where some mathematical relationship connecting the keys is known to the attacker.

Differential Attacks: This attack traces the differences through transformations discovering the cipher exhibiting non random behaviour and exploiting them to recover secret key.

B. Hash functions and Attacks

Collision attack- It acts on a cryptographic hash by trying to find two arbitrary inputs that having same hash value.

Pre-image attack is attack for finding a message that has a specific hash value.

Birthday attack -The attack depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations.

Rainbow table is a pre-computed table for inverting hash functions, especially for cracking password hashes.

Distinguishing attack –here the attacker can extract some information from encrypted data sufficient to distinguish it from random data.

Side channel attack is based on information available from physical implementation of cryptosystem.

Dictionary attack is a technique for defeating a cipher by trying to determine its decryption key or pass phrase by searching likely possibilities.

V. CONCLUSION

Cryptography is a powerful tool to protect information. In the recent years cryptography and cryptanalysis had seen a lot of research. However due to varying requirements of applications and different types of digital data there does not exist a single cryptographic algorithm that could meet all requirements. Conventional cryptographic methods are suitable for textual data however it is not suitable for Images and chaotic cryptography seems to be the best solution for image and video encryption since it is fast and computationally feasible for large data sizes. However since computer are finite state machines and implementing true chaos on them is not possible. Implementing chaos for cryptography using logistic maps and difference equations are only solutions which do have their limitations. Hence developing a fully secure chaotic encryption algorithm is still a challenge.

References

[1] W. Ehrsam, et al, "A cryptographic key management scheme for implementing the DES," *IBM Systems Journal*, 2010, vol. 17, pp. 106-125.

[2] J. Katz and Y. Lindell, Introduction to modern cryptography: Chapman & Hall,CRC, 2008.

[3] W. Stallings, Cryptography and network security: principles and practice: *Prentice Hall*, 2010.

[4] J. Amigo, *et al.*, "Theory and practice of chaotic cryptography," *Physics Letters A*, 2007, vol. 366, pp.211-216.

[5] Zhang et al, "Implementation approaches for AES algorithm," *Circuits and Systems Magazine, IEEE*, 2003, vol. 2, pp. 24-46.

[6] "Chaos based cryptography: A new. Approach to secure communications", BARC, July-2005, http:// *www.**barc**.gov.in/publications/nl/2005/200507-1.pdf*

[7] Li et al, "Baptista-type chaotic cryptosystems: Problems and countermeasures:, *Physics Letters A, Elsevier Science*, 2007, pp.368-375.

[8] Zhang Yong, "Image Encryption with Logistic Map and Cheat Image", *Computer Research and Development (ICCRD), 3rd International Conference, IEEE*, 2011, Vol. 1, pp. 97 - 101

[9] Gao et al, "A new chaotic algorithm for image encryption:" *Elsevier Ltd.* 2005

[10] Yong Zhang "Comments on -An image encryption scheme with a pseudorandom permutation based on chaotic maps", *Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, IEEE Conferences*, 2011 Vol. 2, pp. 1251 - 1255

[11] T. Xiang, *et al.*, "A novel block cryptosystem based on iterating a chaotic map," *Physics Letters A*, 2006, Vol. 349, pp. 109-115.

[12] Diffie, "The First Ten Years of Public-Key Cryptography", *Proceedings of the IEEE*, 1988, **Vol.**76 , pp. 560 - 577