ISSN:0975-9646

Suriya kala.L et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1204-1206

A Study on different Image Encryption Algorithms

Suriya kala.L[1] , Dr. R. Thangaraj[2]

[1]*Research Scholar,*
Mother Theresa Women's University, Kodaikanal, Tamilnadu, India

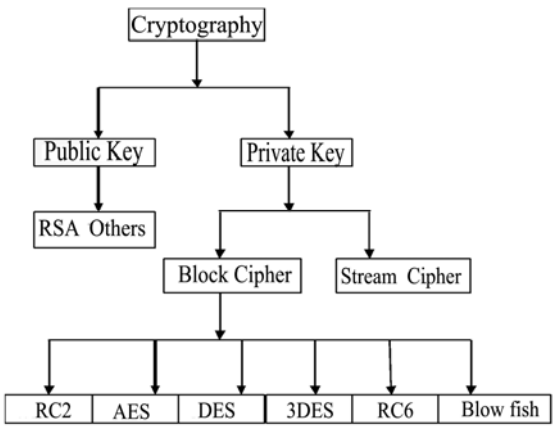
[2]*Department of CSE,*
Bannari Amman Institute of Technology, Sathiyamangalam, Tamilnadu, India

***Abstract*- Image encryption and decryption has become an important research area for secured information transformation in this network era.. Encryption is the process of transforming the information for its security, and decryption is the reverse process of encryption. Through these years so many encryption algorithms have been developed and implemented. In this article we analyzed the different encryption and decryption algorithms and their features.**

Key words:
cryptography, encryption , decryption, symmetric, asymmetric.

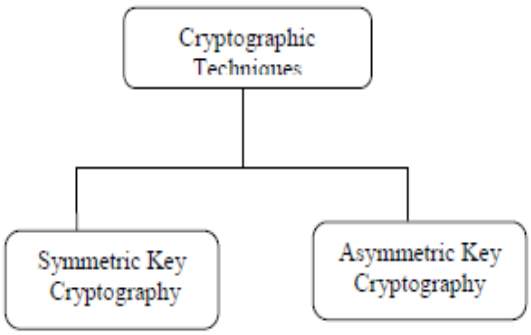
1. INTRODUCTION

Earlier security was a major issue for military applications but now the area of applications has been enhanced since most of the communication takes place over the web. Cryptography is an area of computer science which is developed to provide security for the senders and receivers to transmit and receive confidential data through an insecure channel by a means of process called
Encryption/ Decryption. It provides a number of security goals to ensure the privacy and integrity of data. Due to these security advantages, cryptography it is mostly used today for the images processed across the web.



2. CRYPTOGRAPHY

Cryptography provides the added advantages such as Access Control, Authentication, Confidentiality, Non Repudiation for image security. Cryptography is the art of achieving security by encoding messages to make them non-readable, hiding information.
Cryptography involves converting a message text into an unreadable cipher. A large number of cryptography algorithms have been created till date with the primary objective of converting information into unreadable ciphers Cryptography systems can be broadly classified into symmetric-key systems and public key systems.
Cryptography involves converting a message text into an unreadable cipher. A large number of cryptography algorithms have been created till date with the primary objective of converting information into unreadable ciphers Cryptography systems can be broadly classified into symmetric -
key systems and public key systems.
The symmetric key systems uses a common key for encryption and decryption of the message. This key is shared privately by the sender and the receiver. The sender encrypts the data using the joint key and then sends it to the receiver who decrypts the data using the same key to retrieve the original message. The public -key systems that use a different key for encryption as the one used for decryption. Public key systems require each user to have two keys –a public key and a private key (secret key). The sender of the data encrypts the message using the receiver's public key. The receiver the n decrypts this message using his private key. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. Even though both methods
provide security, a study is made to combine both cryptography and Steganography methods into one system for better confidentiality and security.



2.1 SYMMETRIC ALGORITHM

In symmetric algorithms, both parties share the same key for encryption- and decryption. To provide privacy, this key needs to be kept secret. Once somebody else gets to know the key, it is not safe any more. Symmetric algorithms have the

advantage of not consuming too much computing power. The examples for symmetry algorithm are : DES, Triple-DES (3DES), IDEA, CAST5, BLOWFISH, TWOFISH.

Data Encryption Standard (DES):

DES (Data Encryption Standard) was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It was developed by an IBM team around 1974 and adopted as a national standard in 1997. DES is a 64-bit block cipher under 56-bit key. The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation. DES application is very popular in commercial, military, and other domains in the last decades. Although the DES standard is public, the design criteria used are classified. There has been considerable controversy over the design, particularly in the choice of a 56-bit key.

Triple Des (TDES):

The triple DES (3DES) algorithm was needed as a replacement for DES due to advances in key searching. TDES uses three round message. This provides TDES as a strongest encryption algorithm since it is extremely hard to break 2^168 possible combinations. Another option is to use two different keys for the encryption algorithm. This reduces the memory requirement of keys in TDES. The disadvantage of this algorithm is thatcit is too time consuming.

Advanced Encryption Standard (Aes):

AES was developed by two scientists Joan and Vincent Rijmen in 2000. AES uses the Rijndael block cipher. Rijndael key and block length can be 128, 192 or 256-bits. If both the key-length and block length is 128-bit, Rijndael will perform 9 processing rounds. If the block or key is 192-bit, it performs 11 processing rounds. If either is 256-bit, Rijndael performs 13 processing rounds.

2.2 ASYMMETRIC ALGORITHM

In Asymmetric algorithms the secret key does not have to be shared. Every user only needs to keep one secret key in secrecy and a collection of public keys, that only need to be protected against being changed. It is used in real life for authentication examples for symmetry algorithm are: RSA, Diffie-Hellman, Digital Signature Algorithm, ElGamal, ECDSA, XTR

Asymmetric Algorithms Examples

RSA Asymmetric algorithm Rivest-Shamir-Adleman is the most commonly used asymmetric algorithm (public key algorithm). It can be used both for encryption and for digital signatures. The security of RSA is generally considered equivalent to factoring, although this has not been proved.

RSA computation occurs with integers modulo n = p * q, for two large secret primes p, q. To encrypt a message m, it is exponentiated with a small public exponent e. For decryption, the recipient of the ciphertext c = me (mod n) computes the multiplicative reverse d = e-1 (mod (p-1)*(q-1)) (we require that e is selected suitably for it to exist) and obtains cd = m e * d = m (mod n). The private key consists of n, p, q, e, d (where p and q can be omitted); the public key contains only n and e. The problem for the attacker is that computing the reverse d of e is assumed to be no easier than factorizing n.

The key size should be greater than 1024 bits for a reasonable level of security. Keys of size, say, 2048 bits should allow security for decades. There are actually multiple incarnations of this algorithm; RC5 is one of the most common in use, and RC6 was a finalist algorithm for AES.

Diffie-Hellman

Diffie-Hellman is the first asymmetric encryption algorithm, invented in 1976, using discrete logarithms in a finite field. Allows two users to exchange a secret key over an insecure medium without any prior secrets. Diffie-Hellman (DH) is a widely used key exchange algorithm. In many cryptographical protocols, two parties wish to begin communicating. However, let's assume they do not initially possess any common secret and thus cannot use secret key cryptosystems. The key exchange by Diffie-Hellman protocol remedies this situation by allowing the construction of a common secret key over an insecure communication channel. It is based on a problem related to discrete logarithms, namely the Diffie-Hellman problem. This problem is considered hard, and it is in some instances as hard as the discrete logarithm problem.

The Diffie-Hellman protocol is generally considered to be secure when an appropriate mathematical group is used. In particular, the generator element used in the exponentiations should have a large period (i.e. order). Usually, Diffie-Hellman is not implemented on hardware.

Digital Signature Algorithm

Digital Signature Algorithm (DSA) is a United States Federal Government standard or FIPS for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Algorithm (DSA), specified in FIPS 186 [1], adopted in 1993. A minor revision was issued in 1996 as FIPS 186-1 [2], and the standard was expanded further in 2000 as FIPS 186-2 [3]. Digital Signature Algorithm (DSA) is similar to the one used by ElGamal signature algorithm. It is fairly efficient though not as efficient as RSA for signature verification. The standard defines DSS to use the SHA-1 hash function exclusively to compute message digests.

The main problem with DSA is the fixed subgroup size (the order of the generator element), which limits the security to around only 80 bits. Hardware attacks can be menacing to some implementations of DSS. However, it is widely used and accepted as a good algorithm.

ElGamal

The ElGamal is a public key cipher - an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement. ElGamal is the predecessor of DSA.

ECDSA

Elliptic Curve DSA (ECDSA) is a variant of the Digital Signature Algorithm (DSA) which operates on elliptic curve groups. As with Elliptic Curve Cryptography in general, the bit size of the public key believed to be needed for ECDSA is about twice the size of the security level, in bits.

XTR

XTR is an algorithm for asymmetric encryption (public-key encryption). XTR is a novel method that makes use of traces to represent and calculate powers of elements of a subgroup of a finite field. It is based on the primitive underlying the very first public key cryptosystem, the Diffie-Hellman key agreement protocol.

From a security point of view, XTR security relies on the difficulty of solving discrete logarithm related problems in the multiplicative group of a finite field. Some advantages of XTR are its fast key generation (much faster than RSA), small key sizes (much smaller than RSA, comparable with ECC for current security settings), and speed (overall comparable with ECC for current security settings).

3. COMPARATIVE ANALYSIS

The symmetric algorithms such as DES, 3DES, AES (Rijndael) most widely used.

INPUT DATA SIZE- Different algorithm required different memory space to perform the operation. The memory space required by any algorithm is determined on the basis of input data size, number of rounds etc. The algorithm is considered best which use small memory and perform best task.

TIME- The time required by algorithm to complete the operation depends on processor speed, algorithm complexity. Less the time algorithm takes to complete its operation better it is.

THROUGHPUT-Throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm.

4. CONCLUSION

This paper tries to present a study on cryptography and its categories symmetric and asymmetric with its algorithms. The above analysis gives a quick overview of cryptography. In addition to that it will explain some of the most used terms in cryptography along with a brief description of some popular algorithms to allow the reader to understand the key differences between them.

ACKNOWLEDGEMENT

I would like to thank my Research Supervisor Dr. R. Thangaraj for his valuable assistance and I thank Mother Teresa Women's University, Kodaikanal for giving the opportunity to present this paper. I express my gratitude to Don Bosco College, Dharmapuri for their support and encouragement.

REFERENCES

[1] Wikipedia, "*Encryption*", http://en.wikipedia.org/wiki/Encryption, modified on 13 December 2006.

[2] Freeman J., Neely R., and Megalo L. "*Developing Secure Systems: Issues and Solutions*". IEEE Journal of Computer and Communication, Vol. 89, PP. 36-45. 1998

[3] Agnew G. B., Mullin R. C., Onyszchuk I. M., and Vqanstone S. A. "*An Implementation for a Fast Public-Key Cryptosystems*". Journal of Cryptology, Vol.3, No 2, PP. 63-79. 1995.

[4] Beth T. and Gollmann D. "*Algorithm Engineering for Public Key Algorithms*". IEEE Journal on Selected Areas in Communications; Vol. 7, No 4, PP. 458-466. 1989

[5] IBM. "*The Data Encryption Standard (DES) and its strength against attacks*". IBM Journal of Research and Development, Vol. 38, PP. 243-250. 1994

[6] Wikipedia , "*Bitwise operation*" , http://en.wikipedia.org/wiki/Bitwise_operation , last modified on10 December 2006.

[7] Andy Wilson , "*Tips and Tricks: XOR En*

AUTHOR PROFILE

L. Suriya kala has completed MCA., M. Phil.,and working as Assistant Professor in Don Bosco College, Dharmapuri, Tamilnadu, India. She is a research scholar in the specialization of Digital Image processing at Mother Theresa Women's University, Kodaikanal, Tamilnadu, India.