Survey on Cryptography Algorithms

Brijesh Kumar Patel, Mukti Pathak

Abstract— : Cryptography is that discover and study of methods and procedures for secure communication within the existence of third parties. There is a great number of techniques used in order to achieve the integrity, availability and data protection to secure information. This paper will present a viewpoint on the current state of play in the field of cryptography algorithms. Cryptography offers a lot of techniques which nowadays are difficult to fail. In this paper, we want to prove competency of different techniques by comparing the different types of crypto algorithms like DES, TDES, AES, Blowfish, PGP , RSA and also by presenting their weaknesses and strengths.

Keywords— Cryptography, AES, DES, TDES, Blowfish, PGP, RSA

I. INTRODUCTION

In presence, Internet has turned into a convenient way for data transmission due to a rapid development; ease of use and of modern technology. Cryptography [1] is a technique to scramble confidential information to make it "unreadable." It is commonly used in Internet communications to transmit data in secure way. Some potential problems during data communication on networking like unauthorized access, disclosure, interruption, use, modification, inspection, recording or destruction. The main ideas that a security system has to respect are: confidentiality, data integrity, availability and authentication. These concepts characterize the data security achievement and must be accomplished by every secure communication that aims to be functional. Most security systems use cryptography because it offers various algorithms and techniques practically impossible to break because of their complexity [2]. Cryptography, not only secure data from unauthorized access or modification, but it can also be used for user authentication. In this paper we present two main types of cryptographic algorithms used to achieve these goals: symmetric key (or secret) cryptography, asymmetric(or public-key) cryptography. After we present each of different algorithms with their weakness and strength we will summarize the main attacks that an efficient security system has to solve in each case.

Ease of Use

A. Basic Terms Used in Cryptography

- Plain Text

The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. e.g.., Alice is a person wishes to send “Hello Friend how are you” message to the person Bob.

Manuscript Received on December 2014.

Brijesh Kumar Patel, 3rd Sem M.E., Department of Computer Engineering, Hasmukh Goswami College of Engineering, Vehlal, Ahmedabad, India.

Mukti Pathak, Asst. Prof., Department of Computer Engineering, Hasmukh Goswami College of Engineering, Vehlal, Ahmedabad, India.

Here “Hello Friend how are you” is a plain text message.

- Cipher Text

The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into unreadable message before the transmission of actual message. e.g..,“Ajd672#@91ukl8*^5%” is a Cipher Text produced for “Hello Friend how are you”.

- Encryption

A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure network. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

- Decryption

A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

- Key

A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. For example, if the Alice uses a key of 3 to encrypt the Plain Text “President” then Cipher Text produced will be “Suhvlghqw”.

B. Purpose of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

- Confidentiality

Information in computer is transmitted and has to be accessed only by the authorized person and not by anyone else.

- Integrity

Only the authorized person is allowed to alter the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

- Non Repudiation

Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

- Access Control

Only the authorized person are able to access the given information.

C. Classification of Cryptography algorithms

Cryptography Algorithm can be classified into two part:

- *Symmetric cryptography*

This type of cryptography practices only one key for both encryption and decryption, and it is also called secret key cryptography [3]. This technique works by the following principles:

1. The plaintext is encrypted with the key to produce cipher text and it is sent to the receiver.
2. The receiver uses the same key to decrypt the cipher text and finds the original plaintext.

In Symmetric key cryptography both the sender and the receiver must know the same key in order to use the technique. There are two common patterns in this method stream cipher and Block cipher. The stream ciphers generate a sequence of bits used as a key called a key stream, and the encryption is accomplished by combining the key stream with the plaintext. This is usually done with the bitwise XOR operation. The key stream is not dependent on the plaintext and cipher text, in which case the stream cipher is synchronous, or it can depend of the data and its encryption, in which case the stream cipher is self-synchronizing. A block cipher converts a fixed-length block of plaintext into a block of cipher text which is of the same length. In decryption, same secret key is used by applying the reverse transformation of the cipher text block and original plain text is produced[4].

- *Asymmetric (Public Key) Cryptography (PKC)*

This technique requires two types of keys: one to encrypt the plaintext and one to decrypt the cipher text, and it doesn't work without one or another. It is called asymmetric cryptography because it is used a pair of keys: one is the public key that can be advertised by the owner to whoever he wants, and the other one is the private key and it is known only by the owner. The most common public key algorithm is the RSA algorithm, used for key exchange, digital signatures, or encryption of small blocks of data. It uses a variable size key and a variable size encryption block. The security of the RSA algorithm is based on the factorization of very large numbers. Two prime numbers are generated by a special set of rules, and the product of these numbers is a very large number, from which it derives the key-set [5].

D. Classification of Cryptography techniques

Cryptography technique can be classified into two technique- Substitution and transposition technique. There are two techniques of encryption: Substitution Technique and Transposition Technique. In substitution technique, the letters of plain text are replaced by other character or any number or by symbols. e.g.., Caesar cipher, hill cipher, monoalphabetic cipher etc. In transposition technique, some sort of permutation is performed on plaintext. e.g.., rail fence method, columnar method etc.

II. PREPARE OVERVIEW OF CRYPTOGRAPHY ALGORITHMS FOR DATA SECURITY

The given below are the five basic encryption algorithms:

- DES
- Triple DES
- AES
- Blowfish
- PGP
- RSA

A. DES

DES Stands for data encryption standard It is block cipher algorithm which takes fixed-length string of plaintext bits and transforms it through a sequence of complex operations into cipher text of the same length. DES is symmetric algorithm which takes single key for both encryption and decryption the block size is 64 bits. The key consists of 64 bits but only 56 of these are actually used by the algorithm. Eight bits are used only for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits,.Most commonly used encryption algorithm is DES [6].in DES Each round uses a 48 bit key derived from the 56 bit key. The inverse transformation, DES decryption uses the same 56 bit key with 48 bit keys applied in reverse order.

B. Triple DES

In case of DES, Encryption key size was only 56bits this key size of 56 bits was generally enough when that algorithm was designed, because of increasing computational complexity brute force attack is Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.Triple DES is the modification of DES. It performs DES thrice. It is also a block cipher having three keys each of 56 bits and all are independent.

C. AES

AES works on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. It operates on a 4×4 column-major order matrix of bytes, identified as the state, although some versions of Rijndael have a larger block size and have additional columns in the state. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. The numbers of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

A round for the AES algorithm consists of four operations: the Sub Bytes operation, the Shift Rows operation, the Mix Columns operation, and AddRoundKey operation. The Sub Bytes operation substitutes bytes independently, in a black-box fashion, using a nonlinear substitution table called the S-box The Shift Rows Operation

- The ShiftRows operation shifts the last three rows of the state cyclically, effectively scrambling row data
- The MixColumns operation has the purpose of scrambling the data of each column. This operation is done by performing a matrix multiplication upon each column vector
- The AddRoundKey operation determines the current round key from the key schedule, where the register arg0 serves as the argument. As an optimization we can also combine the MixColumns and AddRoundKey operations.
- The final round has no MixColumns operation.

D. Blowfish

Blowfish is symmetric block cipher encryption There are two parts to this algorithm;

- A part that handles the expansion of the key.
- A part that handles the encryption of the data.

Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. It consist of 16-round Feistel cipher and uses large key-dependent fixed S-boxes. The expansion of the key: break the original key into a set of different subkeys. The encryption of the data: 64-bit input is denoted with an x, while the P-array is denoted with a Pi (where i is the iteration).Security of data with blowfish Cipher is excellent.

E. RSA

RSA is one of the first practicable cryptographic algorithms and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it wasn't declassified until 1997.[8]. A user of RSA creates and then publishes a public key based on the two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.[8].

Breaking RSA encryption is known as the RSA problem. It is an open question whether it is as hard as the factoring problem[7].

The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Compute n = pq.
   - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
1. Compute $\varphi(n) = (p-1)(q-1) = n - (p+q-1)$, where φ is Euler's totient function.
2. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.
   - e is released as the public key exponent.
   - e having a short bit-length and
   3. Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).
      - This is more clearly stated as: solve for d given $d=e \equiv 1 \pmod{\varphi(n)}$
      - This is often computed using the extended Euclidean algorithm. Using the pseudo code in the Modular integers section, inputs a and n correspond to e and $\varphi(n)$, respectively.
      - d is kept as the private key exponent.[9]

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.

F. PGP

Pretty Good Privacy (PGP) is a data encryption and decryption program thatprovides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail The first step in PGP's encryption process is to compress the text that is to be encrypted, called plaintext. Next, the International Data Encryption Algorithm is used to generate a random session key, which is used to encrypt the compressed file, producing what is called the ciphertext. Continuing, the well-known RSA (Rivest, Shamir, and Adleman) public key encryption algorithm is used to encrypt the session key using the recipient's public key. This encrypted session key is then placed at the front of the cipher text file, which is now ready for sending. To decrypt messages, this process is essentially reversed using the private key though, instead of the public key.

III. COMPARATIVE ANALYSIS TABLE

	Private Key				PUBLIC KEY	
	DES	TDES	AES	Blowfish	PGP	RSA
Block Size	64 bits	64 bits	128 bits	64 bits	64 bits	*1+floor((x-1)/8) x= key size*
Key Size	56 bits	168 bits	128, 192,256 bits	32- 448 bits	64 bits	1,024 to 4,096 bit typical
Created By	IBM in 1975	IBM in 1978	Joan Daeman in 1998	Bruce Schneier in 1998	Phil Zimmermann in 1991	Ron Rivest, Adi Shamir in 1977
Algorithm Structure	Fiestel Network	Fiestel Network	Substitution Permutation Network	Fiestel Network	Lai-Massey scheme	
Rounds	16	48	9, 11 ,13	16	8.5	1
Attacks	Brute Force Attack	Theoretically possible	Side Channel	Not Yet	Brute Force Attack	chosen ciphertext attack

IV. CONCLUSION

In this paper a detailed analysis of symmetric and asymmetric algorithms is presented on the basis of different parameters. The main objective was to analyze the performance of the most popular symmetric and asymmetric algorithms in terms of Authentication, Flexibility, Reliability, Robustness, Scalability, Security, and to highlight the major weakness of the mentioned algorithms, making each algorithm's strength and limitation transparent for application. Blowfish has yet no attack. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security.

REFERENCES

1. Behroz A. Forouzan, "Cryptography & Network Security", McGraw Hill Publication,2008, New Delhi.
2. Georgiana Mateescuc, Marius Vladescu "A Hybrid Approach of System Securityfor Small and Medium Enterprises: combining different Cryptography techniques", Federated Conference on Computer Science and Information Systems pp. 659–662,IEEE 2013
3. Gary C. Kessler, An overview of Cryptography, 28 April 2013http://www.garykessler.net/library/crypto.html
4. RSA Laboratories- Chryptographic tools; section 2.1.5. unpublished;http://www.rsa.com/rsalabs/node.asp?id=2174
5. Ing. Cristian MARINESCU, prof.dr.ing. Nicolae ŢĂPUŞ ; "An Overview of the Attack Methods Directed Against the RSA Algorithm"; Revista Informatica Economica, nr. 2(30)/2004
6. Othman O. Khalifa, MD Rafiqul Islam, S. Khan and Mohammed S.Shebani, "Communication Cryptography",2004 RF and Microwave Conference, Oct 5-6, Subang, Selangor, Malaysia.
7. G. Fang and H. Liu, "The research of database encryption based on hybrid cipher system", Journal of Harbin University of Science and Technology, 2008,13(5): 33-35.
8. Rivest, R.; Shamir, A.; Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems".Communications of the ACM 21 (2): 120–126.
9. Robinson, Sara (June 2003). "Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders". SIAM News 36(5).