International Journal of Advance Foundation and Research in Computer (IJAFRC)
Volume 1, Issue 6, June 2014. ISSN 2348 - 4853

Comparative Study of Symmetric and Asymmetric Cryptography Techniques

Ritu Tripathi[1], Sanjay Agrawal[2].
National Institute of Technical Teachers' Training and Research Bhopal, India [1,2]
ritutripathi13@gmail.com[1], sagrawal@nitttrbpl.ac.in[2]

ABSTRACT

Data security is the challenging issue of today that touches many areas including computers and communication. Modern cyber security attacks have surely played with the affects of the users. Cryptography is one such technique to create certain that, authentication, integrity, availability, confidentiality and identification of user data can be maintained as well as security and privacy of data can be provided to the user. The cryptography techniques and various algorithms are used to provide the needed security to the applications. This paper provides a comparison between some symmetric and asymmetric techniques. The factors are achieving an effectiveness, flexibility and security, which is a face of researchers. As a result, the better solution to the symmetric key encryption and the asymmetric key encryption is provided.

Index Terms: Cryptography; Encryption; AES; DES; 3DES; Symmetric key encryption; Asymmetric key encryption.

I. INTRODUCTION

The high growth in the networking technology leads a common culture for interchanging of the data very drastically. Hence it is more accessible of copy of data and reconstruct by hackers. Thus the information has to be secured though transmit it, Sensitive information like ATM cards, banking dealings and public security numbers require to be secured. Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very general method for promoting the information security. The development of encryption is moving towards a prospect of endless possibilities. Each day new methods of encryption techniques are discovered. This paper proposed some recent existing encryption techniques and their security issues.

A. Cryptography

Cryptography is the art and science of protecting information from unwanted person and converting it into a form undistinguishable by its attackers though stored and transmitted. The main aim of cryptography is keeping data secure form unauthorized persons. Data cryptography mostly is the scramble of the content of data, such as text data, image related data and audio, video related data to compose the data illegible, imperceptible or unintelligible during communication or storage called Encryption process. The reverse of data encryption process is called data Decryption.

B. Purpose of Cryptography

Cryptography provides a number of security goals to avoid a security issue. Due to security advantages of cryptography it is widely used today. Following are the different goals of cryptography discussed as:

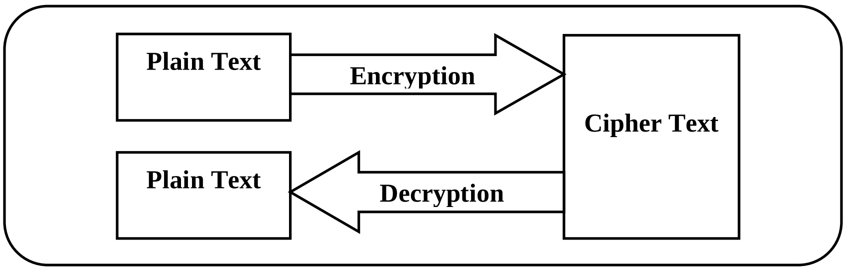

Figure 1: Overview of a Simple Cryptosystem

1. **Confidentiality**
   Nobody can read the message not including the future receiver. Information in computer information is transmitted and has to be contact only by the authorized party and not by unauthorized person [1].

2. **Authentication**
   This process is proving a one's identity. The information received by system then checks the identity of the sender that whether the information is incoming from a authorized person or unauthorized person or wrong identity.

3. **Integrity**
   Only the authorized party is modifying the transmitted information or message. Nobody can change the given message.

4. **Non Repudiation**
   This is a mechanism to prove that the sender really sent this message. So if any sender denies that he doesn't send the message; this method not allows doing such type of action to sender.

5. **Access Control**
   Only the authorized parties are capable to contact the given information.

C. SECURITY AGAINST ATTACK:

Cryptanalysis is an art and science of breaking the encrypted codes that are created by applying some cryptographic algorithm. Cryptanalysis attacks can classify the following:

1. **Cipher text-only attack**
   In cipher-text only attack, the attacker has a part of the cipher text using available information, the attacker tries to find out the corresponding key and decrypt the plain-text [2].

2. **Known-plaintext attack**

The known- plaintext attack (KPA) is an attack model for cryptanalytic wherever the criminal has samples of each the plain-text and its encrypted version cipher-text. These will be revealing any secret data like secret keys and code books.

3. **Chosen-plaintext attack**
   A chosen- plain-text attack (CPA) is an associate attack model for cryptography that presumes the potential to decide on arbitrary plain-text to be encrypted and procure the corresponding cipher-text.

4. **Chosen-cipher text attack**
   A chosen- cipher-text attack (CCA) is an attack model for scientific discipline within which the cryptologist gathers data, a minimum of partially, by selecting a cipher-text and getting its decipherment beneath an unknown key.

5. **Chosen-text attack**
   A chosen text attack is a combination of choosing plain-text and chosen cipher-text attack [2].

6. **Brute-force attack**
   This type of attack is a passive attack. The attacker can try all the possibilities of the key until the message is not broken. this is the very slow attack. Suppose that message is encrypted using the 56-bit key then the attacker can try all the possibilities up to 255 bit [1].

7. **Dictionary attack**
   The extension to the Brute-force attack is the Dictionary attack. In the Dictionary attack, it will try also same possibilities but take only those key bit whose chances of success is more [1].

8. **Timing attack**
   Timing Attack is a side channel attack in which the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms. Each consistent operation in a computer takes time to perform [1].

9. **Man-in-the-middle attack**
   This is the type of active attack. This differs from the above in that it involves tricking individuals into compromise their keys. The attacker is placed in the two parties through communication channel who wish to exchange their keys for secure communication [1].

II. RELATED WORK

In this section, the various methodologies and techniques for the encryption techniques used by various papers are provided.

In this paper [3] Mohit Mittal proposed a Performance Evaluation of different Cryptographic Algorithms On the basis of parameter taken as time various cryptographic algorithms are evaluated on different hardware's Such as intel i5 , intel i3 , intel dual core ,intel atom.

In this paper [4] Yogesh Kumar et al analyzed Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Counter measures comprises of brief description of RSA and DES cryptography algorithms.

In this paper [5] E .Thambiraja et al proposed a different kinds of encryption techniques that are accessible and comparative study of all the techniques simultaneously as a literature survey. The aim of an extensive experimental study of implementations of different available encryption techniques and also focuses on image encryption techniques, information encryption techniques. This study extends to the concert parameters used in the encryption processes and analyzing on their security issues.

In this paper [6] Hamdan.O.Alanazi et al proposed a New Comparative Study between three encryption algorithm such as DES, 3DES and AES within Nine Factors achieving an effectiveness, give and security, which is at the challenge of researchers.

In this paper [7] Mohit Marwaha et al have analyzed DES , Triple DES and RSA three algorithm. DES and Triple DES is symmetric key algorithm and RSA is an asymmetric key algorithm, they have been analyzed on their ability to secure data, time in use to encrypt data and throughput the algorithm requires. Performance of algorithms is different according to the inputs size.

In this paper [8] Harsh Kumar Verma et al proposed a Performance analysis of Blowfish, RC4 and DES block cipher algorithms have been done on the basis of resource utilization and execution time.

III. PROPOSED WORK

In this section, the overview of the cryptography algorithm and classification of the types of the cryptography algorithm (encryption algorithm) and the parameters that are verified for the algorithms and the security issues are briefly placed in the following sub sections.

A. Cryptography algorithm

A set of mathematical function and rules that takes plaintext and a key as a input and product cipher text as output. Cryptography is a process which is associated with scrambling plaintext into cipher text (a process called encryption), then back again (known as decryption).

B. Types Of Cryptography

There are several ways to classify the cryptography algorithms. The most common types are:

- Secret Key Cryptography this is also called as Symmetric Key Cryptography
- Public Key Cryptography this is also called as Asymmetric Key Cryptography

1. Symmetric Cryptography:

In the symmetric key encryption, same key is used for both encryption and decryption process. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encrypt them. The symmetric key encryption takes place in two modes either as the block ciphers or as the stream ciphers. In the block cipher mode the wholedata is divided into number of blocks. These data is based on the block length and the key is provided for encryption. In the case of the stream ciphers the data is divided as small as single bits and randomized then the encryption takes place. Symmetric key cryptosystems are much faster than the asymmetric key cryptosystems. The performance evaluation is taken place for the following symmetric key encryption techniques such as The DES Algorithm, Triple DES algorithm, the AES algorithm and Blowfish algorithm [3].

2. Data Encryption Standard

DES is a symmetric key algorithm which was developed by IBM in 1977.It uses block size 64 bit , key size 56 bits.. DES always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm. DES used 16 rounds of transposition and substitution to encrypt each group of 8(64 bit) plaintext letters and output from each round is one by one. The number of rounds is exponentially proportional to the amount of time and fined a key using a brute-force attack. Therefore the number of rounds increases then the security of the algorithm increases exponentially. DES was clearly no longer invulnerable to the attacks [4].

3. Triple DES

Triple DES is same as the DES operation. It uses three 64-bit keys and overall key length of 192 bits. We simply type in the entire 192-bit (24 character) key rather than entering each of the invidiously three keys. The procedure for encryption is exactly the same as DES, but this process is repeated three times. It is encrypted with the first key then decrypted with the second key, and finally encrypted again with the third key. This procedure for decrypting something is the same as the procedure for encryption, except it is accept same as reverse process [4].

4. Advanced Encryption Standard

Rijndael was selected as the AES in Oct-2000 Designed by Vincent Rijmen and Joan Daemen in Belgium. AES is a symmetric block cipher that can Block size128bit, Cipher keys 128,192and 256 bits. Basically, encryption algorithms are divided into three major categories – transposition, substitution, and transposition – substitution technique. AES algorithm uses a round function that is compared of four different byte-oriented transformation such as Sub byte, Shift row, Mix column ,Add round key. Number of rounds to be used depend on the length of key e.g. 10 round for 128 bit key, 12 rounds for 192-bit key and 14 rounds for 256 bit keys.

5. Blowfish Algorithm

Blowfish algorithm is the important type of the symmetric key encryption that has a 64 bit block size and a variable key length from 32 bits to 448 bits in general [5]. It is based on 16 round fiestel cipher network that uses the large key size. The key size is larger as it is difficult to break the code in the blowfish algorithm. Additionally it is exposed to all the attacks apart from the weak key class attack.

6. Asymmetric Cryptograph

Asymmetric key encryption is the technique, in which the different keys are for the encryption and the decryption process. One key is public (published) and second is kept private. They are also called as the public key encryption. If the lock/encryption key is first published then the system enables private communication from the public to the unlocking key's user [5]. If the unlock/decryption key is the one published then the system serves as a signature verifier of documents locked by the owner of the private key. Public key methods are important because they can be used for transmitting encryption keys or other data securely even when the both the users have no opportunity to agree on a secret key in private Algorithm. The keys used in public-key encryption algorithms are usually much longer that improves the security of the data being transmitted. For the following algorithms the performance factors are evaluate.

A. RSA:

Rivest-Shamir-Adleman is the most commonly used public key encryption algorithm. It can be able to be used for both encryption and digital signatures. The security of RSA is generally considered to factoring. RSA computation occurs with integers modulo n = p * q, for select two random secret primes p, q. To encrypt a message m, public key use a public key exponent e. so cipher text 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 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 that provides.

B. Diffie-Hellman Algorithm

It is that public key encryption algorithm, using discrete logarithms in a finite field .Two parties allow 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 cryptographically protocols, two parties wish to begin communicating. Diffie-Hellman protocols are exchange keys and allow the construction of common secret key over an unconfident contact channel. This problem is based on related to discrete logarithms; its name is Diffie-Hellman problem. This problem is hard, as compare to the discrete logarithm problem.

IV. PERFORMANCE FACTORS

In this paper, the following factors are used as the performance criteria, such as the tunability, computational speed, the key length value, the encryption ratio, the security issue, time and throughput of data against attacks.

A. Tunability

It is very popular to define a encrypted parts and the encryption parameters used to different applications and requirements.

B. Computational Speed

In many real-time applications, the encryption and decryption algorithms are fast sufficient to meet real time requirements.

C. Key Length Value

In the encryption methodologies, the key management is the important feature to shows the how the data is encrypted. The symmetric algorithm uses a variable key length which is longer. So, the key management is a huge aspect in encryption processing.

D. Encryption Ratio

The encryption ratio is the measurement of the amount of data that is to be encrypted. Encryption ratio must be minimizing to reduce the complexity on computation.

E. Security Issues

Cryptographic security defines whether encryption scheme is secure against brute force, time attack and different plaintext-cipher text attack. For highly important multimedia application to the encryption scheme should satisfy cryptography security. We measure cryptographic security in the three levels for example low, medium and high.

F. Time

The time essential by algorithm to total the operation depends on processor speed and algorithm complexity. Less time algorithm take to entire its operation improved it is.

G. Throughput

Throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm. Thus, if throughput increased the power consumption is decrease.

V. RESULTS AND DISCUSSIONS:

This section presents performance and comparison with respect to various parameters. The encryption ratio is measured in terms of minimum, moderate and maximum. The speed is defined by the following term such as fast, slow, moderate. We specify tenability as either yes or no. The key value is measured in terms of bit value used. Throughput is measured as high and less .power consumption (used memory) is defined as high and less. The experimental results are shown in TABLE 1.

Table:1 Comparision Between Symmetric And Asymmetric Encryption

Parameter	Symmetric encryption				Asymmetric encryption	
	DES	3DES	AES	BLOWFISH	RSA	DIFFIE-HELLMAN
KEY USED	Same key used for encryption and decryption	Same key used for encryption and decryption	Same key used for encryption and decryption	Same key used for encryption and decryption	Different key used for encryption and decryption	Key exchange
THROUGPUT	Lower than AES	Lower than DES	Lower than Blowfish	Very high	Low	Lower than RSA
ENCRYPTION RATIO	High	Moderate	High	High	High	High
TUNABILITY	No	No	No	Yes	Yes	Yes
POWER CONSUMPTION	Higher than AES	Higher than DES	Higher than Blowfish	Very Low	High	Lower than RSA
KEY LENGTH	56 bits	112 to 168 bits	128,192,or 256 bits	32 bits to 448 bits	>1024 bits	Key exchange management
SPEED	Fast	Fast	Fast	Fast	Fast	Slow
SECURITY AGAINST ATTACKS	Brute force attack	Brute force, chosen-plaintext, known plaintext	Chosen plain, known plain text	Dictionary attacks	Timing attacks	Eavesdropping

VI. CONCLUSION

This paper presents a performance evaluation of selected symmetric and asymmetric encryption algorithms such as DES, 3DES, AES, Blowfish, RSA and Diffie Hellmen. We can evaluate a table that the encryption ratio is high in using the both encryption techniques. The tunability and key length is higher at the Asymmetric encryption technique .The key length is high in asymmetric encryption algorithm to break the code is complex in RSA. In the aspect of throughput, Throughput is increased so power consumption is decreased. Throughput is high in blowfish and blowfish is less power consumption algorithm hence speed is fast in the Symmetric key encryption is viewed as good. Finally, in the symmetric key encryption techniques the blowfish algorithm is specified as the better solution. In the Asymmetric encryption technique the RSA algorithm is more secure since it uses the factoring of high prime number for key generation. Hence, the RSA algorithm is found as the better solution in this method.

VII. REFERENCES

[1] Satish N . chalurkari ,Nilesh khochare ,B.B. mashram, "Survey on Modular Attack on RSA Algorithm", International Journal of Computational Engineering & Management, ISSN: 2230-7893.

[2] Cryptography and network security, Express Learning, ITL Education Solution ltd.

[3] Mohit Mittal, "Performance Evaluation of Cryptographic Algorithms", International Journal of Computer Applications, ISSN 0975-8887.

[4] Yogesh Kumar, Rajiv Munjal, Harsh Sharma, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures", International Journal of Computer Science and Management Studies, ISSN: 2231-5268.

[5] E .Thambiraja ,G. Ramesh ,Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X.

[6] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal Of Computing, ISSN 2151-9617.

[7] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh "Comparative Analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology, E-ISSN 0976-3945.

[8] Harsh Kumar Verma , Ravindra Kumar Singh "Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms", International Journal of Computer Applications, ISSN: 0975-8887.