Analysis of Different Cryptography Algorithms

Dr. C.P.Agrawal[1], Zeenat Hasan[2]
[1]Professor Computer Science & Application Department MCNUJC, Bhopal, India
[2] Research Scholar Computer Science & Application Department MCNUJC, Bhopal ,India

Abstract

Cryptography is a very important tool for protecting information in Internet. Every time we connect to the Internet the browser uses appropriate cryptographic algorithms on our behalf. There are various cryptography techniques under the symmetric and asymmetric cryptosystem. The perfect selection of specific encryption scheme play important role to exchange the information and to enhance security objectives. The study is done some of the more popular cryptography algorithm currently in used. Practical cryptosystems are either symmetric or asymmetric in nature. This paper compares both the scheme on the basis of different parameter and also compares trendy encryption techniques for convinced selection of both key and cryptographic scheme. Finally this comprehensive analysis thrash outs the latest trends and research issues upon cryptographic elements to conclude forthcoming necessities related to cryptographic key, algorithm structure and enhanced privacy.

Keywords:*Cryptography,Cryptosystem,Symmetric Asymmetric*

1. Introduction

Cryptography is a powerful tool for securing data. It is used to ensure that the information is confidentially transmitted and would not be altered. Cryptography is the skill of devising methods that permit information to be sent in a secure form in such a way that the only person able to retrieve this information is the intended recipient. The highly use of internet leads to the data exchange over the network while communicating to one and another system. While communication it is very important to encrypt the message so that intruder cannot read the message Just to encrypt and decrypt the message cannot fulfill overall security requirements because the word security is itself relies on confidentially, integrity (authenticity, non-repudiation) and availability[1]. Confidentiality concerns with secrecy and privacy which means message should be visible to whom person for which it has been sent and integrity can be further classified into two terms: (1) authenticity – which means the identity of sender should be verified on delivering the message weather the information is coming from authentic sender, from whom we are expecting. (2) Non-repudiation – it means message should not be falsely modified with any kind of fake addition or deletion. Availability means information (message, key, Certificate Verification) and medium (Certification Authority Server, online services) should be timely available when needed. These security objectives births to key exchange methods (Diffie, Hellman, digital signature) and the asymmetric encryption which involves third trust party and the use of two key(s).

2. Cryptography Schemes

Major There are two types of cryptography:

1) Secret key cryptography or Symmetric-key cryptography: In SKC, the sender and the receiver know the same secret code, which is known as key. With the same key messages are encrypted by the sender and decrypted by the receiver. It can be of 2 types : Stream Buffer, Block Buffer.Stream Buffer: Stream buffer encrypts the digits of a message one at a time. Stream Cipher functions is used on a stream of data one at time by operating on it by bits. It consists of two components: a key stream

generator and mixing function. Mixing function uses XOR function, and key stream generator is unit in stream encryption algorithm.Block cipher : In Block cipher, it takes a number of bits and then encrypt them as a single unit[2]. Data is encrypted/decrypted if data is in the forms of blocks. In simple words , the plain text is divided into blocks which are used to produce blocks of cipher text padding the plaintext in blocks. 64 bits blocks have been commonly used.

2) Public key cryptography or Asymmetric-key cryptography: Asymmetric key (or public key) encryption is used to solve the problem of key distribution. In PKC, two keys are used; private keys and public keys. For encryption public key is used and for decryption private key is used . Public key is known to public and private key is known to the user.

Table 1 compares symmetric and asymmetric scheme

. Table 1:Comparison of Cryptography Scheme

Symmetric Encryption	Asymmetric Encryption
It uses single secret key to encrypt and decrypt data.	It deals with pair of key(s) Public key and Private key. Public key is used to encrypt the message and private key is used to decrypt the message .
key size and length is often smaller	Key size and length is often larger than symmetric key
In symmetric encryption process there is need to agree on same secret key before starting encryption [3].	There is no need to agree on same secret key before starting encryption process . Because public key is publically available but the verification of public is required.
It deals with operations like XOR, OR NOT, OR, substitution etc.	It deals with nontrivial mathematical computations, modular arithmetic functions, huge integers (512- 2048 bits) .
The symmetric based algorithms are 100 times faster than asymmetric ones [5].	Asymmetric based methods are 100 times slower than symmetric ones .
It requires less processing and electric power than asymmetric algorithms of equal length and complexity [6].	It requires more processing and electric power than symmetric algorithm of equal length and complexity .
It provides confidentiality [4].	It provides confidentiality .
It does provide integrity by itself .	It does not provide integrity by itself because it also relies on message digest and digital signature for this purpose [7].
It does not provide origin authentication [7].	It provides origin authentication [7] as it uses digital signature for this purpose.
Key must be remained secret in both sides because there is need to share private key.	Public key is publically available and each part has its own private key which needs not to be shared.
The life of key is not longer because it has shared with the other person so in case of any future secret transaction for any other person there is need to be changed it for security reasons.	The life time of key is longer because each party has its own private key which needs not be shared and it remains secret for both parties.
Group key generation formula for symmetric encryption scheme is n(n-1)/2 = ? keys is used to calculate required key(s) for n users.	There is no need to get and remember more and more secret keys because it has only 2 keys for any no. of users.
It does not involve third party.	It involves third party called Certification Authority (CA).
There is only one key which results less hedge to manage.	Managing of key(s) and certificate is complex and it is also time consuming to get touch with the trusted party.
It did not need any kind of certificate or extra registration charges because it did not deal with third party.	It requires extra registration charges due to third party involvement and renewal of certificates.
It did not share any other personal information except the secret key. So it has no miss use information vulnerabilities.	The public key contains much information about the person which may be wrongly used by the other person(s) to whom we are going to share it.
It did not require any extra validation time like client validation in asymmetric scheme.	Each time there is needs to validate the client's certificate which may be stopped or delayed if the CA's server is damaged or down.
It has not any danger of third party related political or spy miss use.	In case of highly secret information related to Governmental plans or any country's defense the involvement of third party may be risky due to political or spy based attack especially in case of Identity based Public Key Cryptography (ID-PKC) due to private key escrow problem which means third party knows the private keys of registered users.
It did not require any extra space to store or manage	For third trusted party the storage and management of

digital certificates like asymmetric scheme.	certificates is becoming critical due to the increase of large no. of demands.

3. Classification of Cryptography Algorithm

The basic classification of cryptographic algorithms is shown in figure 1.Many authors have compared these algorithm on the basis of time complexity and space complexity . This paper compares these algorithms on the basis of parameters like key length and management, Security and The basic classification of cryptographic algorithms is shown in figure 1.Many authors have compared these algorithm on the basis of time complexity and space complexity This paper compares these algorithms on the basis of parameters like key length and management, Security and limitations pertain to each algorithm limitations pertain to each algorithm This paper compares AES,DES,,3DES,RSA,DH, Blowfish algorithm on the basis of different parameter.

Fig.1 Classification of Algorithm

3.1 DES

It was developed in the early 1975 at IBM labs by Horst Fiestel. DES uses 56 bits key for encryption and decryption. It completes the 16 rounds of encryption on each 64 bits block of data. Data encryption standard works on a particular principle. Data encryption standard is a symmetric encryption system that uses 64-bit blocks, 8 bits (one octet) of which are used for parity checks (to verify the key's integrity). Each of the key's parity bits (1 every 8 bits) is used to check one of the key's octets by odd parity, that is, each of the parity bits is adjusted to have an odd number of '1's in the octet it belongs to. The key therefore has a real useful length of 56 3bits, which means that only 56 bits are actually used in the algorithm. So it would take a maximum of 256 or 72,057,594,037,927,936, attempts to find the correct key [7].

3.2 3DES

Triple-DES is also developed by IBM in 1978 as a substitute to DES. 3DES is simply the DES symmetric encryption algorithm, used three times on the same data .Triple Data Encryption Standard (3DES) is also known by Triple Data Encryption Algorithm (TDEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) encryption algorithm three times to each data block

3.3 **RSA**

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who developed and publicly described it in 1978. The RSA (Rivest-Shamir-Adleman) algorithm is the most important public-key cryptosystem. It is widely used public key scheme. It uses large integers like 1,024 bits in size. It has only one round of encryption. It uses asymmetric block cipher. RSA is an algorithm used by modern computers to encrypt and decrypt messages. RSA is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys are used in encryption and decryption process[8]. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. The main disadvantage of RSA is that it consumes lot of time to encrypt data. Actually this is disadvantage of asymmetric key algorithms because the use of two asymmetric keys. It provides good level of security but it is slow for encrypting files. Another threat in this algorithm is fake key insertion at decryption level so the secret key should be private and correct to achieve the encryption in successful manner.

3.4 AES

AES (Advanced Encryption standard) is developed by Vincent Rijmen, Joan Daeman in 2001. The Advanced Encryption Standard (AES) is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world for sensitive data encryption[9]. AES is actually, three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits and 256 bits, respectively. In Advanced encryption standard there are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

3.5 Blowfish

Blowfish was developed by bruce schneier in 1993. It is basically a symmetric block cipher having variable length key from 32 bits to 448 bits. It operates on block size 64 bits. It is a 16-round Feistel cipher .It uses simple operations that are efficient on microprocessors. e.g., exclusive-or, addition, table lookup, modular-multiplication. It does not use variable-length shifts or bit-wise permutations, or conditional jumps. It employs pre-computable subkeys. On large-memory systems, these sub keys can be pre-computed for faster operation. Not pre-computing the sub keys will result in slower operation, but it should still be possible to encrypt data without any pre-computations[10]. It consists of a variable number of iterations. For applications with a small key size, the trade-off between the complexity of a brute-force attack and a differential attack make a large number of iterations superfluous.

3.6 Diffie-Hellman

Diffie-Helman is a way of generating a shared secret between two people in such a way that the secret can't be seen by observing the communication. It does not share information during the key exchange, it creates a key together. The nature of the Diffie-Hellman key exchange does make it susceptible to man-in-the-middle attacks since it doesn't authenticate either party involved in the exchange. This is why Diffie-Hellman is used in combination with an additional authentication method, generally digital signatures. When using RSA, a 1,024-bit key is considered suitable both for generating digital signatures and for key exchange when used with bulk encryption, while a 2048-bit key is recommended when a digital signature must be kept secure for an extended period of time, such as a certificate authority’s key.

Table 2 compares these algorithms on the basis of different parameters

Parameters	DES	3DES	AES	RSA	DH	BLOWFISH
Cryptography scheme	Symmetric	Symmetric	Symmetric	Asymmetric	Asymmetric	Symmetric
Development	In early 1970 by IBM and Published in 1977.	IBM in 1978.	Vincent Rijmen, Joan Daeman in 2001	Ron Rivest, Shamir & Leonard Adleman in 1978	Hellman 1976	Bruce Schneier in 1993
Key length (bits)	64 (56 usable)	168,112	128,192, 256	Key length depends on no. of bits in the module	Variable key length	Variable key length i.e. 32 – 448
Rounds	16	48	10,12,14	1	-	16
Block size (bits)	64	64	18	Variable block size	512	64
Attacks Found	Exclusive Key search, Linear cryptanalysis, Differential analysis	Related Key attac k	Key recovery attack, Side channel attack	Brute force attack, timing attack	Man in Middle attack	Reflection attack.
Level of security	Adequate security	Adequate security	Excellent security	Good level of security	Adequate security	Highly secure
Encryption speed	Very slow	Very slow	Faster	Average	Slow	Very fast

Table 2:Comparison of Algorithm

4. Conclusions

This paper, analyzed various encryption algorithms. It is observed that each algorithm has its own benefits according to different parameters and the strength of the each encryption algorithm depends upon the key management, type of cryptography, number of keys, number of bits used in a key. Longer the key length and data length more will be the power consumption that will lead to more heat dissipation. So, it is not advisable to use short data sequence and key lengths. All the keys are based upon the mathematical properties and their strength decreases with respect to time. The keys having more number of bits requires more computation time which simply indicates that the system takes more time to encrypt the data. From above analysis we have found that Blowfish encryption algorithm is leading with the security level that they provide and faster encryption speed. Encryption algorithms are more secure and fast to work with and in future, there is wide scope of improvement in these both encryption algorithms

References

[1] Bement A. L. et. al., Standards for Security Categorization of Federal Information and Information Systems, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg,2004, MD 20899-8900.

[2]. Anjula Gupta, Navpreet Kaur Walia, " Cryptography Algorithms: A Review", International Journal of Engineering Development and Research. Volume 2, Issue 2,2014

[3] Fontaine. C. and Galand. F. , "A Survey of Homomorphic Encryption for Nonspecialists, EURASIP Journal on Information Security Volume", Article ID 13801, 10 pages, doi:10.1155/2007/13801, Hindawi Publishing Corporation.

[4] Kaliski. B. (1993), A Survey of Encryption Standards, IEEE Micro, 0272-1732/93/1200-0074. 1993 IEEE

[5] Schneier. B. Book- Applied cryptography: Protocols, algorithms, and source code in c, second edition,1996.

[6] Diaa Salama, Abdul. Elminaam, Hatem Mohamed, Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", International Journal of Computer Science and Network Security, vol.8 No.12, December 2008.

[7]D. Coppersmith, "The data encryption standard (DES) and its strength against attacks", IBM Journal Research Develop., vol. 38, no. 3, (1994), pp. 243 -250.

[8] L. Singh and R. K. Bharti, "Comparative perfomance analysis of cyptographic algorithms", International journal of advanced research in computer science and software engineering (IJARCSSE), vol. 3, no. 11, (2013).

[9] J. V. Shanta, "Evaluating the performance of Symmetric Key Algorithms: AES (Advanced Encryption Standard) and DES (Data Encryption Standard) " in IJCEM International Journal of Computational Engineering & Management, vol. 15, no. 4, 2012, pp.43-49.

[10] Monika Agrawal, Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882