Implementation Issues and Analysis of Cryptographic Algorithms based on different Security Parameters

K. Kalaiselvi
Asst. Professor, Dept of Computer Science
Kristu Jayanti College
Bangalore

Anand Kumar, Ph.D
Professor & Dean ,Dept of Computer Science & Engineering, M.S Engineering College,
Visvesvaraya Technological University

ABSTRACT

Cyber security plays a vital role in data communication in every aspect of information exchange through internet. Data has to be secured from unauthorized users and should be transmitted to the intended receiver with confidentiality and integrity. Cryptography is a technique which provides the security by encrypting and decrypting the data in a secured network. Many cryptographic algorithms are available which falls under either symmetric or Asymmetric techniques. To choose an algorithm for secure data communication ,the candidate algorithm should provide higher accuracy , security and efficiency. This paper presents the implementation limitations of existing cryptographic algorithms such as DES, TDES, AES, BLOWFISH, IDEA, RC6, CAST-128 of symmetric techniques and RSA of Asymmetric .This paper analyses parameters like Key exchange, flexibility and security issues of the algorithms which determines the efficiency of crypto system .

Keywords

Cryptography, symmetric ,Asymmetric, Architecture, Security, Limitations, AES, DES, RSA, Secure Key Management.

1. INTRODUCTION

Cryptography is a technique which is intended to transform the data and can be used to provide various security related services such as confidentiality, data integrity, authentication, authorization and non-repudiation [1]. It depends on two basic components: an *algorithm(*cryptographic technique) and a *key*. The algorithm is a numerical procedure and the key is a factor used for data transformation. These algorithms provides cryptographic protection to the data by using encryption and the reverse by decryption. These algorithms can be Symmetric key Algorithms or Asymmetric key algorithms. Symmetric algorithms(Secret key algorithms) :Uses a single key for both encryption and decryption. Some practically used symmetric algorithm includes DES, TDES, CAST5 , BLOWFISH, IDEA, RC6,AES. Asymmetric algorithms (public key algorithms):Uses a key public key and a private key pair which are related to each other which includes RSA, DH(Diffie-Hellman keys), SSH ,SSL.

In both the cases keys are generated by Random Number Generators. The cryptographic keys must be established between the sender and the receiver either manually or using trusted third party key management.

*Research Scholar ,Bharathiar University. ** Research Supervisor ,Bharathiar University.

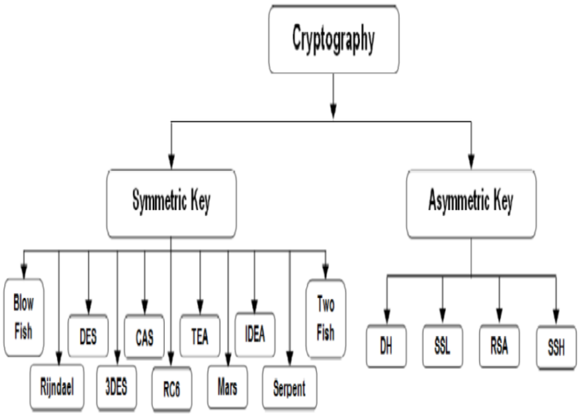

figure:1 classification of cryptographic algorithm

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 [11] . This paper compares these algorithms on the basis of parameters like key length and management, Security and limitations pertain to each algorithm.

2. COMPARISON BASED ON ARCHITECTURAL PARAMETER

The security of a cryptosystem depends on the architecture of the algorithm. This section analysis the cryptosystems in the basics of key generation ,key length ,block size and number of rounds used for encryption and decryption process [2].

2.1 Data Encryption Algorithm (DES) :

DES is the earliest symmetric key block cipher encryption algorithm developed by IBM and adopted by U.S federal government as a standard encryption technique. DES uses 64 bits plaintext blocks and the key length of 56 bits.DES uses the 8 bits as parity bit for error detection. DES is based on Fiestel function (f) which divides the blocks into two halves ,applies 16 rounds of processing [2] to encrypt the data. Function f involves 4 stages as expansion ,key mixing , substitution and permutation.

2.2 Triple DES:

TDES is derived from DES which uses 3 different keys of 56 bits (168 bits total).It has 3 keying options.

option 1: All three keys are independent which is the strongest with 168 independent key bits.

option 2:All three keys are identical which is the weakest and equivalent to DES.

option 3:First and third keys are identical.

It performs 48 rounds of processing to encrypt the data by applying DES three times.

2.3 CAST-128:

CAST-128 is a block cipher algorithm based on Feistel function and has 12 to 16 processing rounds [7].It uses 64 bit block and key length of 40-128 bit. If the key size is greater than 80 bits,16 rounds of processing is performed.

2.4 BLOWFISH:

Blowfish is an block encryption algorithm based on Feistel function which uses 64 bit block and key size ranges from 32-448 bits. Blowfish performs 16 processing rounds [2][6].Key expansion and Data Encryption are the two main functions performed by this algorithm. Substitution boxes are independent of the keys.

2.5 International Data Encryption Algorithm(IDEA):

IDEA is a symmetric key block algorithm based on substitution and permutation structure which performs 8.5 rounds of process where each round performs XOR , addition and multiplication. It is derived from Proposed Encryption Algorithm and uses 64 bit block,128 bit key for encryption.

2.6 Advanced Encryption Standard (AES):

AES is also an block cipher algorithm based on Fiestel network, which uses 128 bits block size and varying key length of 256 ,192 and 128 bits. Depend on the key length the number of rounds performed for encryption varies between 14,12, or 10 rounds. Each AES round performs Key-expansion ,Sub-byte generation, Column-mix and Add-round key.

2.7 RC6:

RC6 is based on Feistel Structure ,derived from RC5 which uses 128 bit block size and varying key size of 256,192 or 128 bits with 20 processing rounds.RC5 and RC6 differs by the number of registers used(2 and 4 respectively)[8].

2.8 RSA:

RSA is a public key cryptographic algorithm ,known as asymmetric cryptography. The asymmetry of the key is based on factoring the product of two large prime numbers. Messages encrypted with the public key can be decrypted in a reasonable amount of time using the private key. Modulus and exponent operations are performed to generate public and private key.

3. COMPARISON BASED ON SECURITY PARAMETER :

The rate at which a particular algorithm encrypts the data is an essential parameter in analyzing the performance of encryption algorithm [3]. An algorithm is considered to better if it provides strong security level. This section analyze the security levels of various cryptographic algorithms.

3.1 DES:

Security in DES is of major concern because of the 56 bit key length. Brute force attack becomes possible with a massively parallel machine of more than 2000 nodes with each node ,capable of a key search rate of 50 million keys/sec. Cryptanalysis is possible by exploiting the characteristics of DES. The weak S-boxes provides a possible mean for a cryptanalytic attack..

3.2 TDES :

TDES reduces the security issue of DES by combined key size of 168 bits(3 times of 56) which is beyond the reach of brute-force techniques .No serious flaws have been uncovered in TDES ,though it has always been regarded suspicious because of DES. Many internet protocols uses this cryptosystem.

3.3 CAST 128:

CAST increases the security strength by using variable key size of 128 and 256 bits. This increases the resistant against both linear and differential attacks[8].

3.4 BLOWFISH:

Blowfish required more processing time because of varying key length. The time consuming sub-key generation process increases the complexity for a brute-force attack. It provides long term data security without any known backdoor vulnerability .

3.5 IDEA:

IDEA is very strong against differential cryptanalysis under a specific hypothesis. The strength of IDEA against many attacks is increased by using multiple group operations. The 128 key size makes IDEA much stronger. IDEA is not yet cracked by linear or algebraic attacks.

3.6 RC6:

It is an evolutionary improvement of RC5 and is highly resistant to differential and cryptanalytic attack. It is a secure, compact simple block cipher whose code and data can readily fit in cache memory [8]. This increases the performance and provides flexibility. The security in RC6 is provided by the rotation amounts during processing. The brute-force attack appears to be infeasible if the key size large and the estimated round of 20 is recommended.

3.7 AES:

AES provides a high security level since uses variable length key bits. It uses operations similar to the RSA modulo arithmetic operations but it can be mathematically inverted. Security of the encryption depends on how long it takes to crack and how high cost will it take an attacker to find a key? Different types of attack to crack AES like Square attack, Key attack, Differential attack were tried ,but none of them cracked AES algorithm [7].

3.8 RSA:

The security of RSA cryptosystem is based on factoring large numbers and taking the eth root modulus of a composite n, finding a value m such that C=m^e(mod n) where (n,e) is a public key and C is the cipher text. If the attacker computes the secret exponent d from a public key(n,e) ,C can be decrypted using the standard procedure. But naturally it is time consuming to find the integer factorization in a polynomial time ,which still proves RSA to be a strong algorithm [9].

4. LIMITATIONS OF DIFFERENT CYPTOGRAPHIC ALGORITHMS

This section discuss the limitations of selected cryptographic algorithms.

4.1 DES:

DES is highly susceptible to linear cryptanalysis attacks. It is exposed to brute force attack because of the weak keys.

4.2 TDES:

TDES is vulnerable certain variation of meet-in-the-middle attacks. It is also exposed to differential and related-key attacks.

4.3 CAST 128:

CAST 128 can be broken by 2^17 chosen plaintexts. The 64 bit key version is susceptible to differential related-key attack.

4.4 BLOWFISH:

Reliability of Blowfish is damaged due to the use of large number of weak keys. The first 4 rounds of process is exposed to 2nd order of differential attacks.

4.5 IDEA:

IDEA is exposed to collision attack. The first 3 rounds among the 8 rounds of process are exposed to key-schedule attacks and key-related differential timing attacks.

4.6 RC6:

RC6 is vulnerable to differential and brute force attack if the key size is small. Time consumption for process in RC6 is high.

4.7 AES:

The combined boomerang and rectangle attack with related-key differentials uses the weakness of few non-linear transformations in key-schedule algorithms and can break some reduced round versions of AES[7]. It can break 192-bit , 9 rounds AES by using 256 different related keys.

4.8 RSA:

Using Small and relatively close primes: If the primes are small enough then factorizing n will be an easy task. If p and q are relatively close then ,finding out the common factors reveals the public key. It consumes longest encryption time and memory usage which ultimately slows down the speed of the algorithm[10].

5. GENERAL IMPLEMENTATION LIMITATIONS:

This section discuss the general limitations in implementing the cryptographic algorithms. There may always be a confusion whether to implement a hardware or a software cryptosystem, to use a symmetric or an Asymmetric algorithm, how to secure and manage the keys. The following section presents the general limitations in implementing [4] the cryptosystems.

5.1 Hardware vs. Software Solutions :

Cryptography can be implemented in hardware, software and/or firmware - each has its related security, cost, simplicity, efficiency, and ease of implementation. Generally software is less expensive ,but slower than hardware. The protection of key variables which provides security is difficult to achieve. Cryptographic algorithms are flexible ,portable and easier to modify. Practically cryptography is implemented in a hardware device but is controlled by algorithms by providing a hybrid solution.

5.2 Asymmetric vs. Symmetric Cryptography :

Symmetric and Asymmetric cryptography has already been discussed in the Introduction of this paper. Symmetric or secret key uses a single key for both encryption and decryption. Asymmetric or public key uses related pairs of keys, in which one pair is public and the other pair is private.

Considering the cryptographic relationships, symmetric and asymmetric cryptography [10] differ as follows:

- S*ymmetric cryptography:* For each sender and the receiver , and for each purpose , unique key needs to be generated. Transferring the key from sender to receiver must provide confidentiality and data integrity.

- *Asymmetric cryptography*: For each sender and receiver a private/public key pair needs to be generated to sign data, a separate key pair for key agreement process and a separate key pair to receive the transmitted keys. The private key is secured by the party who owns the key pair and the public key is shared to other parties .

The main advantage of symmetric cryptography is speed and security protection. Many symmetric key algorithms are faster than asymmetric key algorithms. The protection provided by public key cryptography has reduced due to the factoring efficiency and computational efficiency. In many cases both the key systems are combined to obtain the key management advantages of asymmetric systems and encryption speed advantages of symmetric systems. Symmetric cryptosystem is best suitable for single authority key management and asymmetric cryptography for multi-user environment.

5.3 Secure Key Management :

Key management is an essential factor which directly affects the security of cryptography. Therefore all keys needed to be protected and secured from unauthorized users , modification and replication. This provides secure key generation ,storage and distribution of keys. NIST (National Institute of Standard and Technology) has given some general recommendations [4] for proper key management, which are listed below.

1.The users must maintain control of their keys. Users should be aware of their liabilities and responsibilities, and that they understand the importance of keeping their keys secure.

2.A contingency plan should be made if the key is compromised or suspected compromised.

3.Algorithms and modules used in cryptography should be electronically signed and verified by the user in accordance with FIPS(Federal Information Processing Standard) [5]. This will prevent the unauthorized updating in the system.

4.The integrity of the centrally stored data should be maintained by digital signature and encrypted for confidentiality.

5.Back-up copies of keys should be provided ,since the compromise or loss of keys could deny access to keys in central database which in turn the decryption of data by the users.

6.Key recovery capabilities should be provided whenever the key is no longer used in encryption or decryption.

7.Specific crypto period should be maintained for each key, which means life time of the key used to generate a signature or to perform encryption.

6. ANALYSIS

Among the many existing cryptographic algorithms , DES,TDES,CAST,IDEA,BLOWFISH,AES,RC6 and RSA are selected and compared on the basis of structure , security , flexibility to expand in future and limitations [11][2].

Table :1 illustrates the comparative study on selected algorithms .Security in cryptography is based on how secure the algorithm is against various attacks. The performance of these cryptographic algorithms are based on structure, key length ,block size, number of rounds used, cryptographic time. Ultimately, these are the factors which affects the security of a particular algorithm.

The block size plays a vital role in encryption and decryption, which is the basic unit of data. Larger block size provides higher security when other factors were considered to be equal in some algorithms. AES uses block size of 128 bits which is twice bigger than all other symmetric algorithms in discussion.

Another critical evaluation is on number of rounds used for encryption / decryption process .Increase in processing rounds, strengthens the security as single Fiestel round provides inadequate security.DES and BLOWFISH has 16 rounds of process. TDES has 3 times of DES (48 rounds).AES has varying number of rounds depending of key size.RC6 is the best candidate which has 20 rounds of process as for as this criteria is concerned.

Major issue with symmetric key algorithms is brute force attack , where in the possible key are tried until the exact key is found to decrypt the message. Longer key lengths reduces the feasibility of attacks, since the number of key combination are increased. DES is with the weak key of 56 bits.CAST-125,IDEA uses 128 bits key which is considered to be average key strength .TDES has 168 bits key with good resistance against attack. RC6 and AES has variable key length of 128,256,192 which provides larger key combinations. BLOWFISH uses 448 bits key which is considered to be longest and strongest as brute force attack is concerned .Key management is the strongest parameter to resist against the common attacks.

In asymmetric RSA , key exchange is not needed which increases the security of the algorithm.RSA uses factorization for cryptographic process which significantly reduces the speed of the algorithm. The symmetric algorithms like AES,BLOWFISH,RC6 are much faster than RSA.

Security of the cryptosystem is defined by the secured encryption scheme against brute force attack and differential plaintext - cipher text attack. Though CAST,IDEA,DES , TDES are faster ,they are less secured due to weak keys.

The analysis shows, in case of symmetric algorithms RC6, Blowfish and AES are considered as the secure and efficient on the basis of high security and less limitations. The expansion and tunability of RC6, Blowfish and AES are high compared to other symmetric algorithm in discussion. The comparison of symmetric with that of the asymmetric, RSA is more secured than any symmetrical cryptographic algorithm.

7. CONCLUSION

This paper provides an analytical study on various symmetric encryption algorithms such as DES, TDES, CAST5, IDEA, BLOWFISH, RC6, AES and Asymmetric RSA Algorithm. The analysis is made on the basis of architecture of algorithm, security aspects and the limitation to which they pertain to. The comparison clearly states that though asymmetric algorithm are superior in security, they take more time for processing and requires more memory. Practically , asymmetric algorithms like RSA are used for the key exchange and symmetric algorithms are used for encryption / decryption. Further, general implementation limitations of cryptographic algorithm emphasis the selection between hardware and software cryptosystem, choosing among symmetric and Asymmetric key algorithm and the essential factors to be followed to have a secure key management.

Table 1: Comparison of algorithms based on various parameters

Algorithm & Developer	Structure	Key Size (bits)	Block size (bits)	Process Rounds	Flexibility & Modification	Known Attacks
DES (IBM)	Fiestel	56	64	16	NO	Brute force attack
TDES (IBM)	Fiestel	168	64	48	YES Extended from 56 to 168 bits	Brute force , chosen plaintext, known plain text
CAST-125(Carlisle Adams& Stafford Tavares)	Fiestel	40-128	64	12 or 16	YES, 128 & 256 bits	Chosen plain text attack
BLOWFISH(Bruce Schneier)	Fiestel	32-448	64	16	YES, 64-448 key length in multiples of 32	Dictionary attack
IDEA(Xuejia Lai & James Massey)	Substitution-Permutation	128	64	8.5	NO	Differential timing attacks, key-schedule attack
RC6 (Ron Rivest)	Fiestel	256,192, 128	128	20	YES 128-2048 key length in multiples of 32	Brute force, analytical attack
AES(Vincent Rijmen & Joan Daemen)	Substitution-Permutation	256,192, 128	128	10,12 0r 14	YES, 256 key length in multiples of 64	Side channel attack
RSA(Rivest,Shamir,Adleman)	Factorization	1024-4096	Variable	Not applicable	YES, Multi Prime RSA, Multi power RSA	Factoring the public key

Efficient cryptosystems can be provided by applying more than one algorithm as a hybrid cryptosystem which provides high security and secure data transfer .

8. PROPOSED WORK

The limitations which are analyzed in the previous sections can be minimized if these algorithms are treated with Evolutionary Computation like GA,PSO,ACO which can replicate the randomness of nature.EC can be applied in key generation process of cryptographic algorithm. The proposed work compares the computational complexity and run-time complexity of the developed cryptosystem, to check the optimized solution based on GA and also comparing it with other contemporary EC mechanism.

9. REFERENCES

[1] Stallings William, “Cryptography and Network Security Principles and Practice”, Fifth Edition, Pearson Education, Prentice Hall, 2011

[2] Aamer Nadeem and Dr M. Younus Javed , “A Performance Comparison of Data Encryption Algorithms”, IEEE, 2005.

[3] 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.

[4] Elaine B. Barker, William C. Barker, Annabelle Lee, "Guideline for Implementing Cryptography In the Federal Government ", NIST Special Publication 800-21 [Second Edition].

[5] Data Encryption Standard, Federal Information Processing Standard (FIPS) Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington, DC (January 1977).

[6] 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

[7] J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES algorithm submission, September 3, 1999.

[8] Apoorva, Kumar Yogesh, “Comparative Study of Different Symmetric Key Cryptography”, IJAIEM, vol. 2, Issue 7, July 2013, pp. 204-206

[9] Computers & Informatics (ISCI), 2012 IEEE Symposium on "Enhancing security features in RSA cryptosystem" .

[10] Ketu File white papers, “Symmetric vs Asymmetric Encryption”, a division of Midwest Research Corporation

[11] A.K.Mandal, C.Parakash and M.A.Tiwari, "Performance Evaluation of Cryptographic Algorithms :DES and AES",2012 IEEE Students Conference on Electrical , Electronics and Computer Science.