COMPARATIVE STUDY OF CRYPTOGRAPHY TECHNIQUES

By

Mohye Elddin Alami
Professor of Computer Information Systems
Faculty of Specific Education
Mansoura University

Ahmed Elsayed Amin
Lecturer of Computer
Faculty of Specific Education
Mansoura University

Ahmed Abdelbadie Abdallah
Assistant lecturer of Computer
Faculty of Specific Education
Mansoura University

Research Journal Specific Education
Faculty of Specific Education
Mansoura University

ISSUE NO. 35, JULY. 2014

مجلة بحوث التربية النوعية – جامعة المنصورة
العدد الخامس والثلاثون – يوليو ٢٠١٤

Comparative Study of Cryptography Techniques

Mohye Elddin Alami[*] *Ahmed Elsayed Amin*[**]

Ahmed Abdelbadie Abdallah[***]

Abstract

Today is the era of internet and networks applications. So information security has become an important issue in data communication. Cryptography has come up as a solution, and plays an important role in information security system. It is the study of secret writing that is one such way to make sure that confidentiality, authentication, integrity, availability and identification of user data can be maintained as well as security and privacy of data can be provided to the user.

This paper performs a fair comparative study of three most common cryptography techniques; DES, AES is symmetric key cryptographic technique and RSA is an asymmetric key cryptographic technique. The comparison is made on the basis of these parameters: developed, type, rounds, key length, possible keys, block size, key used, scalability, encryption & decryption speed, security, deposit of keys, encryption & decryption algorithm, throughput, algorithm structure, encryption ratio and cryptanalysis Resistance.

Performance of Cryptography techniques based on the analysis of its stimulated time at the time of encryption and decryption. Experiments results are given to analyses the effectiveness of each techniques and how that AES is more suitable than other techniques.

Keywords:Cryptography, Data Security, Information Security, Embedding Data, DES, AES, RSA.

1. Introduction

Considerable risk frequently arises from the intrinsic nature of data itself. Some data are attractive to criminals through the potential for identity fraud; some may be confidential or a trade secret and therefore attractive in

[*] Professor of Computer Information Systems Faculty of Specific Education Mansoura University

[**] Lecturer of Computer Faculty of Specific Education Mansoura University

[***] Assistant lecturer of Computer Faculty of Specific Education Mansoura University

the context of industrial espionage. Further, when risk is viewed from an informational perspective it often becomes clear that the vulnerability of non-personal data may lead to a secondary exposure for personal data.

The term cryptography is derived from the Greek words “krypt´os” standing for “hidden”, and “gr´aphein,” standing for “write.” [1]. cryptography, which is the study of methods for sending messages in secret [2]. The original message is called the plain text; the disguised text is called the cipher text [3].

1.1. Cryptography Goals

There are five main goals of cryptography. Every security system must provide a bundle of security functions that can assure the secrecy of the system [4][5].

- Authentication: This means that before sending and receiving data using the system, the receiver and sender identity should be verified.
- Privacy/Confidentiality: keeping data secret from all but those authorized to see.
- Data integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: is a service which prevents an entity from denying previous commitments or actions.
- Service Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems provide a way to grant their users the quality of service they expect.

1.2 cryptographic algorithms

In general, cryptographic algorithms are often grouped into two broad categories symmetric and asymmetric but in practice, today’s popular cryptosystems use a hybrid combination of symmetric and asymmetric algorithms. Symmetric and asymmetric algorithms are distinguis-hed by the types of keys they use for encryption and dqecryption operations [6][7].

A. Symmetric Encryption

Encryption methodologies that require the same secret key to encipher and decipher the message are using what is called private key encryption or symmetric encryption.

Symmetric encryption methods use mathematical operations that can be programmed into extremely fast computing algorithms so that the encryption and decryption processes are executed quickly by even small computers.

B. Asymmetric Encryption

While symmetric encryption systems use a single key to both encrypt and decrypt a message, asymmetric encryption uses two different but related keys, and either key can be used to encrypt or decrypt the message. If, however, key A is used to encrypt the message, only key B can decrypt it, and if key B is used to encrypt a message, only key A can decrypt it. Asymmetric encryption can be used to provide elegant solutions to problems of secrecy and verification.

2. Data Encryption Standard Technique

Data Encryption Standard (DES). A complete description of DES is given in the Federal Information Processing Standards Publication 46, dated January 15, 1977. DES is a block cipher, with a 64-bit block size and a 56-bit key.

DES consists of a16-round series of substitution and permutation. In each round, data and key bits are shifted, permutated, XORed, and sent through, 8 s-boxes, a set of lookup tables that are essential to the DES technique. Decryption is essentially the same process, performed in reverse [8][9][10]. Figure 1: shows the diagram of DES technique.

Algorithm

[1] DES takes an input of 64-bit long plaintext and 56-bit key (8 bits of parity) and generates output of 64 bit block.
[2] The plaintext block is subject to an shift the bits around.
[3] The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
[4] The plaintext and key are processed in 16 rounds consisting of:
   a. The key is split into two 28 bit halves.
   b. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
   c. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed key is used to encrypt this round's plaintext block.

d. The rotated key halves from step 2 are used in next round.
e. The data block is split into two 32-bit halves.
f. One half is subject to an Expansion Permutation to increase its size to 48 bits.
g. Output of step 6 is exclusive-OR'ed with the 48-it compressed key from step 3.
h. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
i. Output of step 8 is subject to a P-box to permute the bits.
j. The output from the P-box is exclusive- OR'ed with other half of the data block.
k. The two data halves are swapped and become the next round's input.

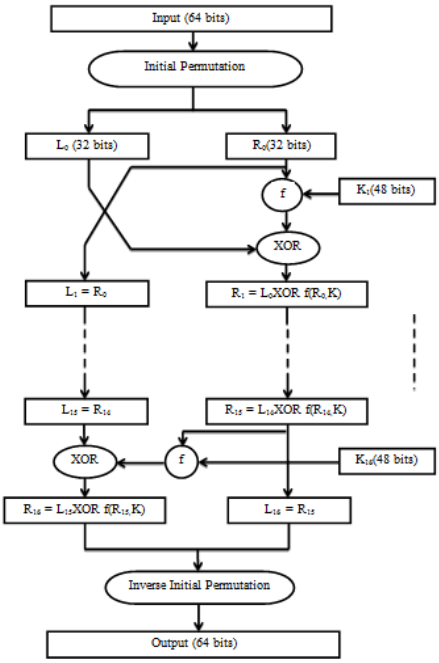

Figure 1: Diagram of DES Algorithm

3. Advanced Encryption Standard Technique

Advanced Encryption Standard (AES) technique not only for security but also for great speed. Both hardware and software implementation are faster still.

AES uses 10, 12, or 14 rounds. The key size that can be 128,192 or 256 bits depends on the number of rounds. AES uses several rounds in which each round is made of several stages. It is carefully tested for many security applications[11].

To provide security AES uses types of transformation. Substitution permutat-ion, mixing and key adding each round of AES except the last uses the four transformations [1][12][13]. Figure 2 shows the AES encryption and decryption.

Algorithm

Following steps used to encrypt a 128-bit block:

[1] Derive the set of round keys from the cipher key.
[2] Initialize the state array with the block data (plaintext).
[3] Add the initial round key to the starting state array.
[4] Perform nine rounds of state manipulation.
[5] Perform the tenth and final round of state manipulation.
[6] Copy the final state array out as the encrypted data (cipher text).

Each round of the encryption process requires a series of steps to alter the state of array. These steps involve four types of operations . They are:

a. Sub Bytes: This operation is a simple substitution that converts every bite into a different value.
b. ShiftRows: Each row is rotated to the right by a certain number of bytes.
c. MixColumns: Each column of the state array is processed separately to produce a new column. The new column replaces the old one.
d. XorRoundKey :This operation simply takes the existing state array.

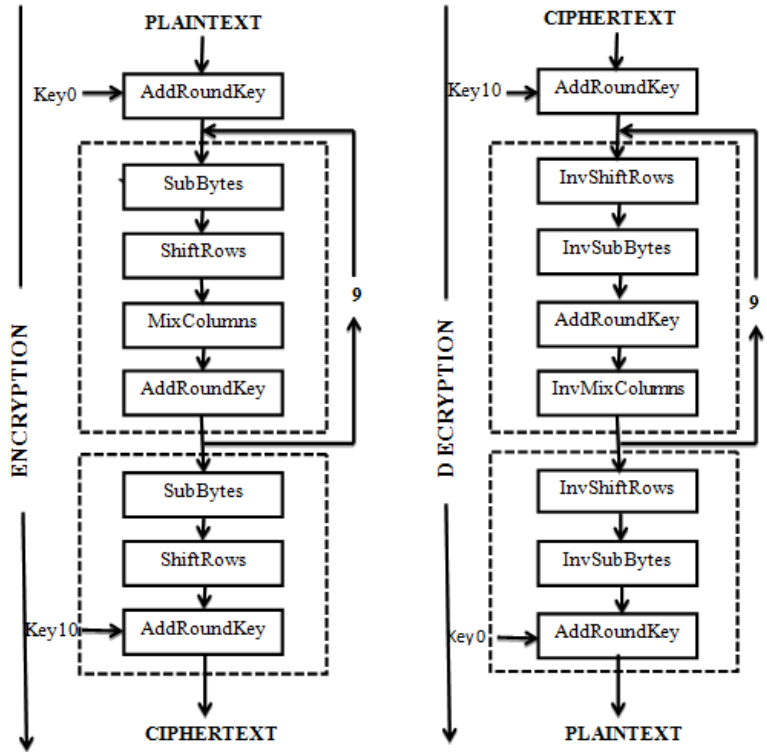

Figure 2: AES Encryption and Decryption

4. RSA Technique

The RSA technique was publicly described in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT; the letters RSA are the initials of their surnames. RSA is an internet encryption and verification scheme and is the most commonly used technique. The mathematical information of the technique is employed in acquiring the public and private keys [14][15]. The technique engrosses multiplying two big prime numbers and by means of additional operations derives a set of two numbers in which one set comprises the public key and other set comprises the private key. Both the public and the private keys are desired for encryption and decryption purposes but only the holder of private key desires to recognize it. By using the RSA system, the private key by no means requires to be sent across the Internet [14][15][16]. Figure 3 shows the RSA encryption and decrypt-ion.

Algorithm

Choose large prime numbers p and q such that p~=q.

Compute n=p*q

Compute J (pq) = (p-1)*(q-1)

Choose the public key e such that

gcd (J (n), e) =1; 1<e< J (n)

Select the private key d such that

d*e mod J (n) =1

So in RSA algorithm encryption and decryption are performed as-

Encryption

Calculate cipher text C from plaintext message M such that

C=M ^e mod n

Decryption

M=C^d mod n=M^ed mod n

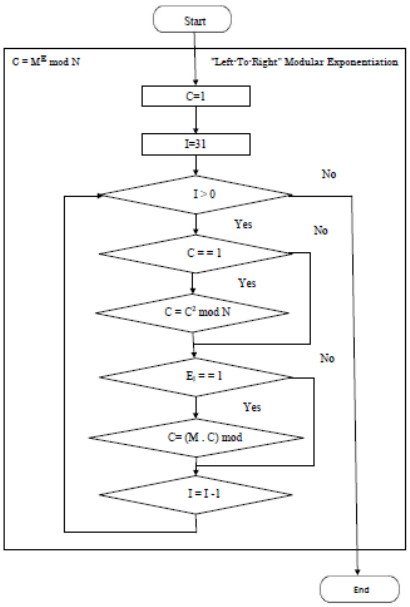

Figure 3: RSA Encryption and Decryption

5. Comparative Study

Each of the encryption technique has their own strong and weak points. In the table below shows a comparative study between DES, AES and RSA is presented in to sixteen factors, which are developed, type, rounds, key length, possible keys, block size, key used, scalability, encryption & decryption speed, security, deposit of keys, encryption & decryption algorithm, throughput, algorithm structure, encryption ratio and cryptanalysis Resistance.

- Developed: It states about the timeline of algorithm.
- Type: symmetric (secret key or one-key) or asymmetric (public key or two-key).
- Key length: It plays a vital role that shows how data is encrypted.
- Key Used: To specify whether same key is used for encryption and decryption process or different key.
- Scalability: Key size and block size variation is referred as scalability.
- Security: Encryption technique must satisfy cryptographic security like plaintext – cipher text attack.
- Throughput: Throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm.
- Encryption ratio: Measures amount of data that is to be encrypted. It should be minimized to reduce complexity. In our analysis we stated three levels like low , medium ,high.

Table 1 Comparative Study of Cryptography Techniques

Factors	DES	AES	RSA
Developed	1977	2000	1978
Type	Symmetric	Symmetric	Asymmetric
Rounds	16	10,12,14	Not Applicable
Key Length	56 bits	128, 192, 256 bits	>=1024 bits
Possible Keys	256	2128, 2192, 2256	>=21024
Block size	64 bits	128, 192, 256 bits	Any byte length
Key Used	Same key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt	Different key used for Encrypt and Decrypt
Scalability	It is scalable algorithm due to varying the key size and Block size.	Not Scalable	Not Scalable
Encryption & Decryption Speed	Moderate	Faster	Slower
Security	Not Secure Enough	Excellent Secured	Least Secure
Deposit of keys	Needed	Needed	Needed
Encryption & Decryption Algorithm	Different	Different	Same
Throughput	Very high	High	Low
Algorithm structure	Feistel network	Feistel network	-----
Encryption ratio	Low	High	High
Cryptanalysis Resistance	Vulnerable to differential and linear cryptanalysis; weak substitution tables	Strong against differential, truncated differential, linear, interpolation and square attacks	Strong against differential, truncated differential, linear, interpolation and square attacks

6. Experimental Results

The five text files of different sizes are used to conduct five experiments, where a comparison of three techniques AES, DES and RSA is performed Performance of encryption algorithm is evaluated considering the following parameters.

- Encryption time: is considered the time that an encryption algorithm takes to produces a cipher text from a plain text.
- Decryption time: is considered the time that an decryption algorithm takes to produces a plain text from a cipher text.

The calculation and analysis purpose for above, customized computer application program is developed in VB.NET platform. From the simulation

result, we evaluated that AES technique is much better than DES and RSA techniques.

All The results show below in tables and graphs.

Table 2 Encryption time

Sample size in KB	Encryption Time in Sec		
	DES	AES	RSA
1	3.0	1.6	7.3
2	3.2	1.7	10.
3	2.0	1.7	8.5
4	4.0	2	8.2
5	3.0	1.8	7.8
Total Time	15.2	8.8	41.8
Average Time	3.04	1.76	8.36

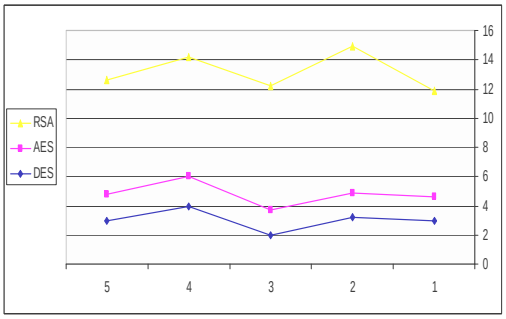

Figure 1 Encryption time

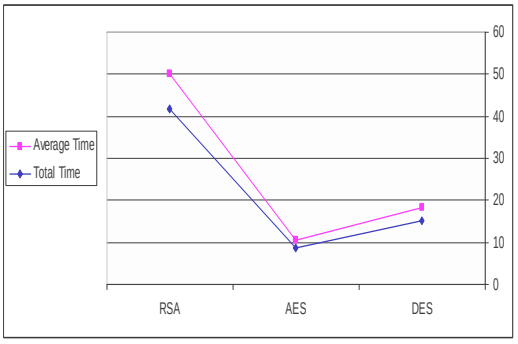

Figure 2 Total and average time for encryption

Table 3 Decryption time

Sample size in KB	Decryption Time in Sec		
	DES	AES	RSA
1	1	1.1	4.9
2	1.2	1.2	5.0
3	1.4	1.2	5.9
4	1.8	1.2	5.1
5	1.6	1.3	5.1
Total Time	7	6	26
Average Time	1.4	1.2	5.2

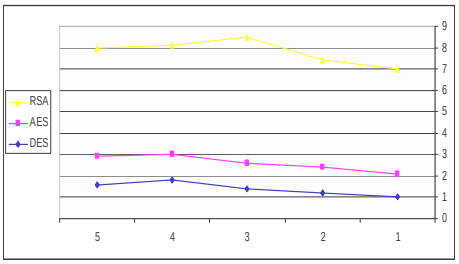

Figure 3 Decryption time

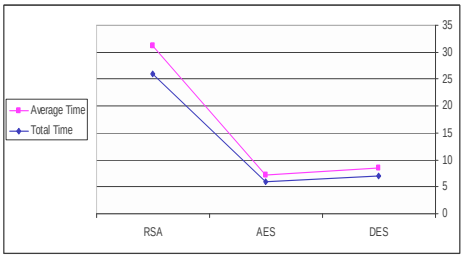

Figure 4 Total and average time for decryption

7. Conclusion

Cryptography techniques play an important role in communication security where encryption time, Memory usages output byte and battery power are the major issue of concern.

In this paper comparative study of different cryptography techniques The selected AES, DES and RSA techniques are used for performance evaluation. Based on the text files used and the experimental result it was concluded that DES technique consumes least encryption time and AES technique has least memory usage while encryption time difference is very minor in case of AES technique and DES technique. RSA consume longest

encryption time and memory usage is also very high but output byte is least in case of RSA technique.

From the simulation result, we evaluated that AES technique is much better than DES and RSA techniques.

Acknowledgment

The authors thanks and gratefully acknowledges the support of Prof: A.Elalfe (Mansoura University).

References:

1. Oppliger, Rolf. (2005): Contemporary Cryptography, ARTECH HOUSE. INC, Norwood.
2. RICHARD A. MOLLIN (2007): An INTRODUCTION to CRYPTOGRAPHY ,2nd Edition, Chapman & Hall/CRC, USA.
3. DAREL W. HARDY and etc (2009): APPLIED ALGEBRA CODES, CIPHERS, AND DISCRETE ALGORITHMS, 2nd Edition, Chapman & Hall/CRC, USA..
4. Jawahar Thakur, Nagesh Kumar (2011): DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis, International Journal of Emerging Technology and Advanced Engineering, Volume (1), Issue (2), PP 6-12.
5. A.Menezes and etc (1997): Handbook of Applied Cryptography, 5th Edition, CRC Press, Inc, USA.
6. Darrel Hankerson and etc (2004): Guide to Elliptic Curve Cryptography, Springer-Verlag New York, Inc, USA.
7. Michael E. Whitman, Herbert J. Mattord (2012): Principles of Information Security, 4th Edition, Course Technology, Cengage Learning, Boston, USA.
8. Douglas Stinson (2010): Cryptography - Theory And Practice, CRC Press LLC, USA.
9. Shafi Goldwasser and Mihir Bellare (2008): Lecture Notes on Cryptography, Cambridge, Massachusetts.
10. Wade Trappe, Lawrence C. Washington (2006): Introduction to Cryptography with Coding Theory, 2nd Edition, Pearson Education Inc, USA.
11. Jonathan Katz and Yehuda Lindell (2008): Introduction to Modern Cryptography ,Chapman & Hall/CRC, USA.
12. Apoorva, Yogesh Kumar (2013): Comparative Study of Different Symmetric Key Cryptography Algorithms, International Journal of Application or Innovation in Engineering & Management, Volume (2), Issue (7), PP 204-206.
13. 13- William Stallings (2005): Cryptography and Network Security Principles and Practice, 4th Edition ,Prentice Hall, USA.
14. Peter Thorsteinson, G. Gnana Arun Ganesh(2003): .NET Security and Cryptography, Prentice Hall, USA.
15. MICHAEL WELSCHENBACH (2005): Cryptography in C and C++, 2nd Edition, Springer-Verlag New York, Inc., USA.
16. BRUCE SCHNEIER (2010): Ptography, Protocols, Algorthms, and Source Code in C, 2nd Edition, Prentice Hall, USA.