A Literature Review on RSA, DES and AES Encryption Algorithms

Roopali Sood, Harpreet Kaur

Appejay College of Fine Arts, Jalandhar

Corresponding author: Harpreet Kaur, Email: apharpreetbhatia@gmail.com

Nowadays, as more and more information is communicated via computers, the need is to ensure that this information is secure and information can be secured by the means of encryption algorithms. Securing information refers to the methodologies that are implemented to protect sensitive information from misuse or disclosure as it causes risk. Encryption is the process of conglomerating or scrambling a message so that only the intended recipient can read it. With the fast progression of digital data exchange in an electronic way, Information security is becoming much more important in data storage and transmission. With the evolution of human intelligence, the art of cryptography has become more complex in order to make information more secure. Various encryption algorithms are deployed to make information more secure. In this paper, a survey of RSA, DES and AES encryption algorithms are presented.

Keywords: Encryption, RSA, DES, AES.

2023. In Vikram Dhiman & Pooja Dhand (eds.), *Emerging Trends in Engineering and Management*, 57–63. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.56155/978-81-955020-3-5-07

1 Introduction

The In the recent years, many applications based on internet are emerged such as on-line shopping, stock trading, internet banking and electronic bill payment etc. Such transactions over network demand end to end secure connections which should be confidential to ensure data authentication and confidentiality, integrity and availability, also known as CIA trial [1].

Security is the mechanism by which information and services are protected from unintended or unauthorized access. Security in networking is based on cryptography (a word with Greek origins, means "secret writing"), the science and art of transforming messages to make them secure and immune to attack [2].

Encryption is one of the principal means to guarantee security of sensitive information. For eg. When you use your credit card on Amazon, your computer encrypts that information so that others cannot steal your personal data when it is being transferred. Similarly, if you have a file on your computer you want to keep it secret, you can encrypt that file so that no one can open that file without the password. It is great for everything from sending sensitive information to securing your email, keeping your cloud storage safe, and even hiding your entire operating system. Many encryption algorithms are widely available used for information security. Encryption algorithms are classified into two groups: Symmetric-Key and Asymmetric-Key encryption.

Symmetric key encryption is a form of cryptosystem in which encryption and decryption is performed using same key. It is also known as conventional encryption.

Asymmetric key encryption is a form of cryptosystem in which encryption and decryption is performed using the different keys i.e. public key and private key. It is also known as public key encryption. Asymmetric encryption techniques are about 1000 times slower than symmetric encryption which makes it impractical when trying to encrypt large amounts of data. Also to get the same security strength as symmetric, asymmetric must use a stronger key than symmetric encryption technique [4].

2 Related work

This subsection describes and examines previous work done in the field of data encryption. The metrics which are taken into the consideration are processing speed, throughput, power consumption, packet size, avalanche effect and data types.

Arora et al. [5] studied about the performance of different security algorithms on a cloud network and on a single processor for different input sizes. This paper aims to find in quantitative terms like speed up ratio that benefits of using cloud resources for implementing security algorithms (RSA, MD5 and AES) which is used by businesses to encrypt large volume of data.

Seth et al. [12] has done the comparative analysis of three algorithms; RSA, DES and AES while considering certain parameters such as computation time, memory usage and output byte. These parameters are the major issues of concern in any encryption algorithms. Experimental results show that DES algorithm consumes least encryption time and AES algorithm has least memory usagewhile encryption time difference is minor in case of AES and DES algorithm. RSA consumes longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm.

Abdul. Elminaam et al. [4] studied about the performance of symmetric encryption algorithms. This paper provides evaluation of six of the most common encryption algorithms: AES, DES, 3DES, RC2, Blowfish and RC6. A comparison had conducted at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. Experimental simulation shows experimental results. There is no significant difference when the results were displayed in hexadecimal base encoding or in base 64 encoding. When the size of packets were changed, it was found that RC6 requires less time than all other algorithms and when data type was changed such as image instead of text, it was found that RC2, RC6 and Blowfish has disadvantages over other algorithms in terms of time consumption. In addition, 3DES still has low performance as compared to DES. Finally, in the case of changing key size possibly only in AES and RC6 algorithms, it was seen that higher key size leads to clear change in the battery and time consumption.

Pavithra et al. [11] compares the performance evaluation of various cryptographic algorithms. On the basis of parameter taken as time, various cryptographic algorithms are evaluated on different video files. Different video files are having different processing speed on which various sizes of files are processed. Calculation of time for encryption and decryption in different video file format such as .vob and .dat, having size from 1MB to 1100 MB. Results shows that AES algorithm was executed in lesser processing time and more throughput level as compared to DES and Blowfish.

Alanazi et al.[6] has done the comparative analysis of three encryption algorithms(DES, 3DES and AES) within nine factors such as key length, cipher type, block size, security, possible keys at 50 billion keys per second etc. study shows that AES is better than DES and 3DES.

Mandal et al. [7] compared two most commonly used symmetric techniques i.e. Data Encryption Standard(DES) and Advanced Encryption Standard(AES) on the basis of avalanche effect due to one bit variation in plaintext constant, memory required for implementation and simulation time required for encryption. Avalanche effect is the property of any encryption algorithm in which small change in either the key or the plaintext should produce a significant change in the cipher text.

Avalanche Effect = Number of flipped bits in ciphered text/ number of bits in ciphered text
Avalanche effect is very high for AES as compared to DES whereas memory requirement and simulation time for DES is greater than that of AES, which shows AES is better than DES. AES is ideal for encrypting messages sent between objects via chat-channels, and is useful for objects that involve monetary transactions.

Kakkar et al. [8] studied various techniques and algorithms used for data security in MN (Multimode Network). It has been observed that strength of system depends upon the key management, type of cryptography (public or private keys), number of keys, number of bits used in a key. Longer key length and data length consumes more power and results in more heat dissipation. Larger the number of bits used in a key, the more secure the transmission. 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 system takes more time to encrypt the data.

3. Detailed Description of Algorithms

Some important encryption algorithms are discussed here:

3.1 Rivest – Shamir-Adleman (RSA)

Ron Rivest, Adi Shamir, and Leonard Adleman of Massachusetts design RSA in 1978. It is one of the best-known public key cryptosystems for key exchange or digital signature or encryption of blocks of data. RSA uses a variable size encryption block and a variable size key. It is an asymmetric (public key) cryptosystem on number theory, which is a block cipher system. It uses two prime numbers to generate the public and private keys. These two different keys are used for encryption and decryption purpose. Sender encrypts the message using receiver public key and when the message is received by the receiver, than receiver can decrypt it using his own private key[10,11]. RSA operations can be decomposed into three broad steps: key generation, encryption and decryption. RSA have many flaws in its design therefore not preferred for the commercial use. When the value of p and q is small for designing key then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand, if the values of p and q is large then it consumes more time and the performance is degraded in comparison to DES. Further, the algorithm requires of similar lengths for p and q, practically this is very tough condition to satisfy. Padding techniques are required in such cases increases the systems overheads by taking more processing time [8].

Key Generation Procedure [11]

1. Choose two distinct large random prime numbers p & q such that p is not equal to q.
2. Compute n=p*q.
3. Calculate: phi (n) = (p-1) * (q-1).
4. Choose an integer e such that 1<e<phi(n).
5. Compute d to satisfy the congruence relation d*e=1, mod phi (n); d is kept as private key exponent.
6. The public key is (n,e) and the private key is (n,d). Keep all the values d,p,q and phi secret.

For example:

1. Choose p=3 and q=11
2. Compute n= p*q= 3*11=33
3. Compute phi(n)=(p-1) * (q-1) = 2*10=20
4. Compute e such that 1<e<phi(n) and e and n are coprime. Let e=7
5. Compute a value for d such that (d*e)% phi(n)=1. One solution is d= 3[(3*7)%20=1]
6. Public key is (e,n) =>(7,33)
7. Private key is (d,n) =>(3,33)
8. The encryption of m = 2 is c= 2^7 %33=29
9. The decryption of c = 29 is m = 29^3 %33=2

3.2 Data Encryption Standard (DES)

The Data Encryption Standard was jointly developed by IBM and the U.S. governmentin 1974 to set a standard that everyone could use to securely communicate with each other. It operates on blocks of 64 bits using secret key that is 56 bits long. The original proposal used a secret key that was 64 bits long. The removal of 8 bits from the key was done to make it possible for the U.S. government agencies to secretly crack message. The US National Security Agency (NSA) made several modifications, after which it was adopted by Federal Information Processing Standard (FIPS) [9].

The data encryption standard is a block cipher that is designed to encrypt and decrypt blocks of data consisting of 64 bits by using a 64-bit key. The data encryption standard is a secret key encryption scheme adopted as standard in the USA in 1977. DES works on bits. Each group of four bits make up a hexadecimal number. Binary “0001” is equal to number”1”. DES works by encrypting groups of 64 message bits, which is same as 16 hexadecimal numbers. To do the encryption, DES uses “Keys” which are also apparently 16 hexadecimal numbers long. However, every 8th key bit is ignored in the DES algorithm, so that the effective key size is 46 bits. But in case, 64 bits(64 hexadecimal digits) is the round number upon which DES is organized.

For example:

If we take the plaintext message”8787878787878787” and encrypt it with DES key”0E329232EA6D0D73”, we end up with the ciphertext “0000000000000000”. If the cipher text is decrypted with the same secret DES key"0E329232EA6D0D73", the result is the original plaintext i.e."8787878787878787". this example is orderly because our plaintext as exactly 64 bits long. But most of the messages will not be exact multiple of 64 bits. For example, if we take the message "I am a good learner". This plaintext message is 21 bytes long. So this message must be padded with some extra bytes at the tail end for the encryption. Once the encrypted message has been decrypted, these extra bytes are thrown away. There are of course, different padding schemes, different ways to add extra bytes.

DES is a block cipher meaning it operates on the plaintext blocks of a given size(64 bits) and returns ciphertext blocks of the same size. Thus DES results in a permutation among the 2^64 possible arrangements of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each, a left half block L and the right half R.

For Example:

Let P be the plaintext message P=01234556789ABCDEF, where P is hexadecimal format. Rewriting P in the binary format, we get the 64-bit block of the text:

P=0000 0001 0010 0011 0100 0101 01100111 1000 1001 1010 1011 1100 1101 1110 1111
L = 0000 0001 0010 0011 0100 0101 0110 0111
R = 1000 1001 1010 1011 1100 1101 1110 1111

The first bit of m is "0". The last bit is "1". We read from left to right.
Before DES was adopted as a national standard, during the period NBS was soliciting comments on the proposed algorithm, the creators of public key cryptography. Diffie and Hellman than outlined a "brute force" attack on DES. By brute force means that you try as many of the 2^56 possible keys as you have to before decrypting the ciphertext into the sensible plaintext message [10, 11].

3.3 Advanced Encryption Standard (AES)

Advanced Encryption Standard was adopted by NIST in 2001 as FIPS-197, and replaced DES which was withdrawn in 2005. AES can support any combination of data (128 bits) and key length of 128, 192 and 256 bits, depending upon the key length. During encryption and decryption process, AES system goes through 10 rounds for 128-bit keys, 12 rounds for 192- bit keys and 14 rounds for 256-bit keys in order to deliver final cipher text or to retrieve the original plaintext. AES allows a 128-bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4 * 4 that is called the state. For both encryption and decryption, the cipher begins with an AddRoundKey stage. However, before reaching the final round, this output goes through nine main rounds, during each of those rounds four transformations are performed; **1)** Sub-Types **2)** Shift-Rows **3)** Mix-Coloumns **4)** Add Round Key. In the final round, there is no Mix-Column transformation. Decryption is the reverse process of encryption and using inverse functions: Inverse Substitute Bytes, Inverse Shift Rows and Inverse Mix Columns.

Each round of AES is governed by the following transformation [10,11]:

a) Substitute Byte Transformation
AES contains 128-bit data block, which means each of the data blocks has 16 bytes. In sub-type transformation, each byte of a data block is transformed into another block using an 8-bit substitution box, which is known as RijndaelS-box.

b) Shift Rows Transformation
In this, the bytes in the last three rows of the state, depending upon the row location are shifted cyclically. For the second row, 1 byte circular left shift is performed. For the third row 2 bytes left circular shift is performed and for the fourth row 3 bytes left circular shift is performed.

c) Mix Columns Transformation
It is equivalent to matrix multiplication of each column of the states. A fix matrix is multiplied to each column vector. In this operation, the bytes are taken as polynomials rather than numbers.

d) Add Round key Transformation
It is a bitwise XOR between the 128 bits of present state and 128 bits of round key. This transformation is its own inverse comparative study of security algorithms.

4 Comparative study of Security Algorithms

Table1. shows that asymmetric algorithms such as RSA is slower than symmetric algorithms such as AES, DES and RSA is least secure algorithm as compared to DES and AES.

Table1. Comparison of RSA, DES and AES

Factors	RSA	DES	AES
Created by	Ron Rivest, Adi Shamir and Leonard Adleman in 1978	IBM in 1975	Vincent Rijmen, Joan Daemen in 2001.
Key Length	Depends on the number of bits in the modulus n where n= p*q	56 bits	128, 192 or 256 bits.
Rounds	1	16	10-128 bit key, 12-192 bit key, 14-256 bit key.
Block size	Variable	64 bits	128 bits
Cipher type	Asymmetric Block Cipher	Symmetric Block cipher	Symmetric Block Cipher.
Speed	Slowest	Slow	Fast
Security	Least Secure	Not secure enough	Excellent Security

5. Conclusion and Scope of Future work

This paper presents a detailed study of the popular encryption algorithms such as RSA, DES and AES. The use of the internet and network is growing rapidly. Therefore, there are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network, different encryption methods are used. In this paper, a survey on the existing works on the encryption techniques has been done. So, all the techniques are useful for real time encryption. Each technique is unique in its own way which might be suitable for different applications and has its own advantages and disadvantages. According to literature survey, it has been found that AES algorithm is most efficient in terms of speed, time, throughput and avalanche effect. The security provided by these algorithms can be enhanced further, if more than one algorithm is applied to data. Future work will explore this concepts and combination of algorithms will be applied either sequentially or parallel to setup a more secure environment for data storage and retrieval.

References

[1] Nie, T., Song, C., & Zhi, X. (2010, April). Performance evaluation of DES and Blowfish algorithms. In *2010 International conference on biomedical engineering and computer science* (pp. 1-4). IEEE.

[2] Forouzan, B. A. (2007). *Data communications and networking*. Huga Media.

[3] Stallings, W. (2006). *Cryptography and network security, 4/E*. Pearson Education India.

[4] Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2008). Performance evaluation of symmetric encryption algorithms. *IJCSNS International Journal of Computer Science and Network Security*, *8*(12), 280-286.

[5] Arora, P., Singh, A., & Tyagi, H. (2012). Evaluation and comparison of security issues on cloud computing environment. *World of Computer Science and Information Technology Journal (WCSIT)*, *2*(5), 179-183.

[6] Alanazi, H., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M., & Al-Nabhani, Y. (2010). New comparative study between DES, 3DES and AES within nine factors. *arXiv preprint arXiv:1003.4085*.

[7] Mandal, A. K., Parakash, C., & Tiwari, A. (2012, March). Performance evaluation of cryptographic algorithms: DES and AES. In *2012 IEEE Students' Conference on Electrical, Electronics and Computer Science* (pp. 1-5). IEEE.

[8] Kakkar, A., Singh, M. L., & Bansal, P. K. (2012). Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication. In *in Multinode Network", International Journal of Engineering and Technology Volume*.

[9] Sutton, E. Latency, Packet Loss and Encryption using DES with a VPN.

[10] page.math.tu-berlin.de

[11]S. Pavithra, E. Ramadevi,(2012), Performance Evaluation of Symmetric Algorithmns.

[12] Luo, Z., Shen, K., Hu, R., Yang, Y., & Deng, R. (2022). Optimization of AES-128 Encryption Algorithm for Security Layer in ZigBee Networking of Internet of Things. *Computational Intelligence and Neuroscience*.

[13] Seth, S. M., & Mishra, R. (2011). Comparative analysis of encryption algorithms for data communication 1.