A Comparative Study of Cryptographic Algorithms

[1] Manzoor Hussain Dar, [2] Pardeep Mittal, [3] Vinod Kumar

[1] Research Scholar, DCSA, Kurukshetra University, Kurukshetra

[2, 3] Assistant Professor, DCSA, Kurukshetra University, Kurukshetra

Abstract- Cryptography is the art and science of keeping massages secure. It is the study of techniques related to aspects of information security such as information privacy, integrity, authentication and non-repudiation. Cryptography is almost synonymous with encryption i.e. the conversion of plain text to a cryptic text to secure it against unauthorized users. Encryption techniques are typically divided into two generic types: symmetric key encryption and asymmetric key encryption. Encryption methods in which both the sender and receiver share the same key are referred to as symmetric key encryption schemes. Encryption methods in which encryption and decryption are performed using the different keys, one a public key and one a private key are referred to as asymmetric key encryption schemes. This paper provides a performance comparison between four popular and commonly used encryption algorithms: DES, 3DES, AES, and RSA. DES, 3DES, and AES are symmetric key encryption algorithms while as RSA is an asymmetric key encryption algorithm.

Keywords- Cryptography, DES, 3DES, AES, RSA.

1. Introduction

In this era of universal electronic connectivity, the possibility of theft of information by hackers and eavesdroppers is very high. There is indeed no time at which security does not matter. The tremendous growth in computer systems and their interconnections via networks has increased the dependence of organizations and individuals on the information stored and communicated using these systems. There is a need to protect data and resources from disclosure and to protect systems from network based attacks [1].
Cryptography is a standard way of securing data and resources from network based attacks.

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted [2]. The main goal of cryptography is keeping data secure from unauthorized users. Original data that is readable and understandable either by a person or by a computer is called plain text whereas the data which is unreadable to human or machine is called cipher text. The technique to convert a plain text message into cipher text is called encryption. Decryption is the reverse process of encryption in which cipher text is converted back into the original text. A system or product that provides encryption and decryption is called cryptosystem [3]. The algorithms in cryptography are categorized into two classes: Symmetric and Asymmetric encryption. In symmetric encryption both the sender and receiver share the same secret key. Examples are: DES, 3DES, AES etc. In asymmetric encryption the sender and receiver use a pair of keys (one key for encryption and another for decryption). Examples are RSA, Diffie-Hellman etc.

The security level of an encryption algorithm is measured by the size of its key space. Large key size means greater security but may decrease encryption or decryption speed. The larger the size of the key, the more the attacker need to do the exhaustive search of the key space and thus higher the security level is. In encryption, the key is a piece of information (sequence of random bits) which specifies the particular transformation of plain text to cipher text, or vice versa during decryption. The larger the key space the more possible keys can be constructed [5]. The strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector and how they all work together [4].

2. Literature Review

The various encryption schemes that have been compared are discussed in the following section.

2.1 DES

DES stands for Data Encryption Standard. The DES algorithm was developed at IBM in 1972.DES is based on Lucifer which was developed by Horst Feistel. The National Bureau of Standards and Technology (NIST) approved this algorithm after assessment of DES strength and modifications by the national security agency (NSA) and became a federal standard in1977 [6]. For DES data are encrypted in 64-bit blocks using a 56-bit key. The algorithm converts a 64-bit input in a series of steps into a 64-bit output. The same steps, with same key are used in reverse to decrypt the message [1]. A key is usually chosen randomly from the available possible keys. DES uses eight predefined S-boxes which have been determined by the U.S National Security Agency (NSA).

Each of the S-boxes accepts 6-bits as input and produces 4-bits as output. These S-boxes are resistant against differential The following steps explain the DES encryption algorithm in brief [7]:

1. DES takes 64-bit input and transforms it into a 64-bit output.
2. DES consists of 16 rounds of processing of the plaintext with each round consisting of a "substitution" step followed by a "permutation" step.
3. The input block to each round is divided into two halves that we can denote L and R for the left half and the right half respectively.
4. In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key.
5. The permutation step at the end of each round consists of swapping the modified L and R. Therefore, the L for the next round would be R of the current round and R for the next round is the output L of the current round.

2.2 3DES

In cryptography 3DES is the common name for triple Data Encryption Algorithm (TDEA or triple DEA), which applies the Data Encryption Standard (DES) three times to each data block. Triple DES was the answer to many of the security vulnerabilities of DES. It is based on the DES algorithm, so it is very easy to modify the existing software to use triple DES. The larger key length eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES [8].Triple DES or 3DES uses three 56-bit DES keys which creates a key with the total length of 168 bits. The process of encryption using 3DES is exactly the same as DES, except that instead of single key three keys are used in the following order [9]:

1. First key is used for encryption.
2. Second key is used for decryption.
3. Third key is used for another encryption.

The process of decryption is the same as the encryption, except it is executed in reverse.

2.3 AES

On January 2, 1997 the National Institute of Standards (NIST) held a contest for a new encryption standard. The previous standard, DES, was no longer adequate for security. It had been the standard since November 23, 1976. Computing power had increased a lot since then and the algorithm was no longer considered safe. In 1998 DES was cryptanalysis, which was earlier known in the 1990s. The encryption process of DES is done in 16 rounds. cracked in less than three days by a specially made computer called the DES cracker. The DES cracker was created by the electronic frontier foundation for less than $250,000 and won the RSA DES challenge-II [10]. Current alternatives to a new encryption standard were triple DES and International Data Encryption algorithm (IDEA). The problem was IDEA and 3DES were too slow and IDEA was not free to implement due to patents. NIST wanted a free and easy to implement algorithm that would provide good security. Additionally they wanted the algorithm to be efficient and flexible [11].

After holding the contest for three years, NIST chose an algorithm created by two Belgian computer scientists, Vincent Rijmen and Joan Daemen. They named their algorithm Rijndeal after themselves [11]. Supposedly Rijndael can only be pronounced correctly by people who can speak Dutch and the closest English approximation is "Rhine Dahl" [12].

On November 26, 2001 the federal information processing standards 197 (FIPS 197) announced a standard form of the Rijndael algorithm as the new standard for encryption. This standard was called Advanced Encryption Standard and is currently the standard for encryption [13].

AES allows for block sizes of 128, 168, 192, 224 and 256 bits [11]. The key size varies between 128, 192 and 256 bits; but only the key size of 128 bits was approved as the AES standard [14]. At the basic level the Rijndael algorithm uses a number of rounds to transform the data for each block. The number of rounds used is 10, 12 or 14. The initial block (also known as state) is added to an expanded key derived from the initial cipher key. Then the round processing occurs consisting of operations of the S-box, shifts, and a MixColumn. The result state is then added to the next expanded key. This is done for all rounds, with the exception of the MixColumn operation of the final round. The final result is the encrypted cipher block [15].

2.4 RSA

In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman proposed a cryptographic algorithm, which was essentially to replace the less secure National Bureau of Standards (NBS) algorithm. Most importantly RSA implements a public key cryptosystem, as well as digital signature. RSA is motivated by the published works of Diffie and Hellman from several years before, who described the idea of such an algorithm, but never truly developed it [16].The RSA scheme is a block cipher in which the plain text and cipher text are integers between 0 and n-1 for some n. typically

the size for n is 1024 bits or 309 decimal digits. The following steps summarize the RSA algorithm [1]:

1. Select two prime numbers p and q.
2. Calculate n = p*q.
3. Calculate φ(n) = (p-1)(q-1) (Euler's Totient function)
4. Chose an integer e, such that I < e < φ (n) and GCD (e, φ(n)) =1.
5. Compute d ≡ e-1 mod [φ(n)].
6. Publish the public encryption key: (e, n).
7. Keep secret the decryption key: (d, n)
8. For encryption we need to calculate $C = M^e \bmod n$.
9. For decryption, we calculate $M = C^d \bmod n$.

Where C and M is cipher text and plain text respectively.

3. Comparison between DES, 3DES, AES and RSA.

Based on the reviews and research performed over the four encryption algorithm, the following is the brief outcome of this study.

Table 1 : Comparison of Cryptographic Algorithms on various parameters

Parameters	*DES*	*3DES*	*AES*	*RSA*
Abbreviation of	Data Encryption Standard	Triple Data Encryption Standard	Advanced Encryption Standard	Rivest, Shamir, Adleman
Developed by and Year	IBM (1972)	IBM	Rijmen and Daemen	R. Rivest, A Shamir, L.Adleman
Type	Symmetric	Symmetric	Symmetric	Asymmetric
Key size	56-bits	192-bits	128, 192 or 256-bits	Variable
Block size	64-bits	64-bits	128, 192, 224, 256-bit	Variable
Security	Proven insecure	Secure than DES	secure	Secure
Cryptanalytic Resistance	Vulner-able to differential and linear cryptanalysis.	Vulner-able to differential analysis and known-plaintext attack.	Strong against differential and linear crypt-analysis.	Strong against crypt-analysis.

4. Conclusions

This papers presents a comparative study of various encryption algorithms on various parameters. The selected algorithms are DES, 3DES, AES, and RSA. It can be concluded from the above study that AES has better performance than DES and 3DES. RSA is the most popular asymmetric encryption algorithm which provides security to various business applications. RSA gets its security from the difficulty of factoring large prime numbers. Howverer it requires large key size for providing good security which makes it quite slow.

References

[1] Stalling,W., "Cryptographyan Network Security: Principles and Practices". Prentice Hall, 2010.

[2] Elminaam, D.S.A., Kader, H.M.A., Hadhoud, M.M., "Evaluation of the Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, PP.216–222, May 2010.

[3] Naji, A.W., Zaidan, A.A., Zaidan, B.B., Khalifa, O.O., "Novel Approach of Hidden Data", International Journal of Computer Science and Information Security, 2009.

[4] Posch, K.C., Posch, R., "Designing a New Encryption Method for Optimum Parallel Performance", IEEE First International Conference on Algorithms and Architectures for Parallel Processing, Brisbane, Australia 1995.

[5] Kiesler, T., Harn, L., "Cryptographic Master Key Generation Scheme and its Applications to Public Key Distribution", IEEE Proceedings E-computers and Digital Techniques, 1992.

[6] Rouse, M., "Data Encryption Standard", 2006.

[7] Avinash, K., "Block Ciphers and the DES". http://www.engineering.purdue.edu/kak/compsec/.../lecture3.pdf.

[8] Triple DES Encryption. Tropical Software, 2014. http://www.tropsoft.com/strongenc/des.htm(accessed February, 9, 2014).

[9] Engelfriet, A., DES Encryption Algorithm. http://www.iusmentis.com/technology/encryption/des(accessed February, 10, 2014).

[10] DES Encryption. Tropical Software. 2014. http://www.tropoft.com/strongenc/des.htm (accessed February, 10, 2014)

[11] Kaufman, C., Perlman, R., Speciner, M., "Network Security: Private Communication in a Public World". 2nd ed. Upper Saddle River, N J.: Prentice Hall PTR, 2002.

[12] Rijndael. Knowledgerush. 2009. http://www.easybib.com/cite/form/website (accessed February, 10, 2014).

[13] Advanced Encryption Standard (AES). http://csrc.nist.gov/publications/fips/fips-197.pdf (accessed February, 10, 2014).

[14] Paar, C., Pelzi, J., "Understanding Cryptography: A Textbook for Students and Practioners", ISBN 978-3-642-04 101-3, 2010.

[15] Daemen, J., Rijmen, V., "AES Proposal:Rijndael". Sept. 3, 1999.http://www.comms.scitech.sussex.ac.uk/fft/crypo/rijndael.pdf (accessed February, 9, 2014).

[16] Evgeny, M., The RSA Algorithm. June 2009. http://www.math.washington.edu. (accessed February,11, 2012).

Bibliography

Manzoor Hussain Dar is a M. Tech. Scholar (Computer Sc. & Engineering), in the Dept. of Computer Science & Applications, Kurukshetra University, Kurukshetra. His research interests lies in Algorithms, Machine Learning, Systems Programming and Network Security.

Pardeep Mittal is working as an Assistant Professor in the Department of Computer Science & Applications, Kurukshetra University, Kurukshetra with a teaching experience of fifteen years. His research interest includes Networking, Optimization, Network Security, Simulation, Genetic Algorithms and Compilers. He has published thirteen research papers in international and national journals, conferences and seminars. He has attended many workshops and faculty development programme.

Vinod Kumar is working as an Assistant Professor in the Dept. of Computer Science & Applications, Kurukshetra University, Kurukshetra with a teaching and technical experience of sixteen years. His research interests includes Medical Image Mining, Data Mining, Web Mining and in the field of Networking. He has published various research papers in international journals and conferences. He has attended many workshops and faculty development program. He is a good counsellor and motivator to the cancer patients from last eighteen years.