Study on Symmetric and Asymmetric Cryptographic Techniques

May Aye Chan Aung, Myat Su Wai
University of Computer Studies, Mandalay
mayayechanaung@gmail.com, missmyatsuwai@gmail.com

Abstract

Data security is the challenging issue in todays world that touches many areas using computer communication. Recent cyber security attacks have certainly played with the sentiments of the users [9]. Encryption is one of the ways to protect data from unauthorized access and is used in many fields such as medical science, military and diplomatic communication. To achieve data security, different cryptographic algorithms (symmetric and asymmetric) are used that jumbles data into scribbled format that can only be reversed by the user that has to decrypt key. This paper study on existing cryptographic algorithms and also gives the advantages and disadvantages of symmetric and asymmetric encryption techniques.

1. Introduction

Communication is the backbone of any enterprise. Without exchanging of data, communication is unimaginable. The high growth in networking technology leads to interchanging large amount of data. Hence, it is more accessible for hackers to copy data and reconstruct it. Thus, the information has to be secured throughout the transmission of sensitive information like ATM cards, bank dealings and public security numbers.

KrptÕs (“hidden”) is a Greek word gives birth to English word called cryptography- an art of changing the actual face look of information and converting it into unreadable form [5]. The process of encoding plain text messages into cipher text messages is called encryption process [5]. The reverse process of transforming cipher text back to plain text is called decryption process [5]. Encryption is a very general method for promoting information security. “The development of encryption is moving towards a prospect of endless possibilities” [11]. Each day new methods of encryption techniques are discovered [11].

In general, cryptography can be classified as symmetric key algorithm and asymmetric key algorithm [8]. Symmetric-key algorithm also known as single- key, one-key and private-key encryption is a class of algorithms for cryptography [8]. It uses a private (shared secret) key and a public (non-secret) key to execute encryption/ decryption process [8]. Some popular and well-respected symmetric algorithms includes DES, 3DES, Blow Fish, IDEA, TEA, CAST 5, Rijndael, RC6, Serpent, Two Fish and MARS [8]. Asymmetric-key algorithm also known as public key encryption is a form of crypto system in which encryption and decryption are modern encryption technology mathematically [8]. Some popular and well-respected asymmetric algorithms include RSA, DH, ECC and DSA [11]. This paper is an overview of the architecture and security of recent existing encryption techniques.

This paper is structured as follows: In the next section, symmetric encryption is described. Asymmetric encryption is presented in section 3. The final conclusion is drawn in section 4.

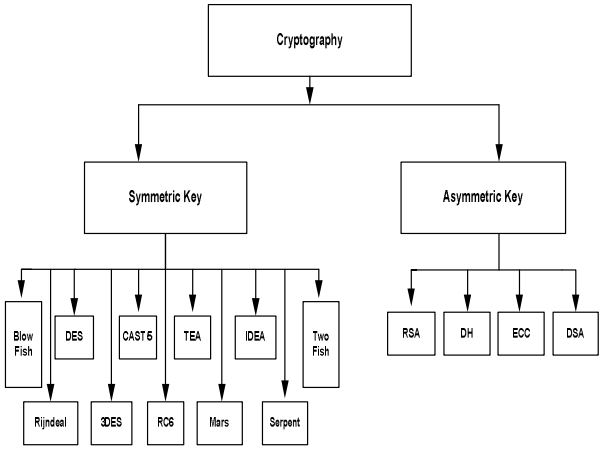

Figure 1.Different Symmetric & Asymmetric Cryptographic Algorithms

2. Symmetric Encryption

In the symmetric key encryption, same key is used for both encryption and decryption process. Symmetric key cryptosystems are much faster than the asymmetric key cryptosystems. It is used to provide confidentiality of the messages [11]. The following symmetric algorithms such as DES, 3DES, Blow Fish, IDEA, TEA, CAST 5, Rijndael, RC6, Serpent, Two Fish and MARS are described in details according to their overview of architecture and security.

2.1. DES

DES is a symmetric key algorithm which was developed by IBM in 1977 [11]. It uses blocks size 64 bits and key size 56 bits. It always operates on blocks of equal size and uses both permutations and substitutions in the algorithm. It used 16 rounds of transposition and substitution to encrypt each group of 8 (64 bit) plaintext letters and produced output from each round is one by one. The number of rounds is exponentially proportional to the amount of time. Therefore, the number of rounds increases then the security of the algorithm increases exponentially [16].

In general, DES was proved insecure for large corporations or governments and it is simpler not to use DES algorithm. However, for backward compatibility and cost of upgrading, DES should still be preferred, outweighing the risk of exposure [8]. DES is highly vulnerable to linear cryptanalysis attacks. Weak keys are also a great issue. DES is also exposed to brute force attack [7].

2.2. Triple DES (3DES)

Triple DES is an enhanced version of DES in November 1998 [8]. It uses three 64-bit keys and overall key length of 192 bits. It is based on the concept of feistel structure and also contains 8 S-boxes. The procedure for encryption is exactly the same as DES but this process is repeated three times without changing the original structure of DES algorithm. It operates as encrypt, decrypt, encrypt. This procedure for decrypting is the same as the procedure for encryption, except it is accepted same as reverse process [16].

3DES is exposed to differential and related-key attacks. It is also susceptible to certain variation of meet-in-the-middle attack [7]. 3DES offers high level of security in comparison with DES and is still used by the US government.

2.3. Blow Fish Algorithm

Blow Fish algorithm is the important type of the symmetric key encryption. It has a 64 bit block size and a variable key length from 32 bits to 448 bits in general [3]. It is based on 16 round feistel cipher network that uses the large key size. The key size is larger as it is difficult to break the code in the blowfish algorithm. Blow Fish has some classes of weak keys. 4 rounds of blowfish are exposed to 2nd order differential attacks. So, reliability of Blowfish is questionable due to the large number of weak keys [7].

Blowfish's security lies in its variable key size (128-448 bits) providing high level of security. Blowfish is invulnerable against differential related-key attacks, since every bit of the master key involves many round keys that are very much independent, making such attacks very complicated or infeasible. Such autonomy is highly enviable.

2.4. IDEA

International Data Encryption Algorithm (IDEA) was developed by James L. Massey and Xuejia Lai (Zurich, Switzerland) in 1990 [8]. It is a symmetric key algorithm based on the concept of substitution-permutation structure. It is fairly fast, considered secure, and is also resistant to both linear and differential analysis. It is a block cipher that uses a 64 bit plain text with 8 rounds and a key length of 128-bit permuted into 52 sub- keys each of 128- bits. It does not contain S- boxes and same algorithm is used in reversed for decryption [15]. IDEA has a strong resistance against differential cryptanalysis under certain hypothesis. IDEA makes use of multiple group operations [7] to increase its strength against most familiar attacks. It consists of 128 bit key size making it as a strong security algorithm [8]. No weaknesses relating linear or algebraic attacks have yet been reported. The best attack which applies to all keys can break IDEA reduced to 6 rounds.

2.5. TEA

Tiny Encryption Algorithm (TEA) was designed by David Wheeler and Roger Needham of the Cambridge Computer Laboratory in 1994 [8]. It is known for its simple structure and easy implementation, typically a few lines of code [8]. It is also a feistel structured symmetric key algorithm. It is a block cipher that uses a 64 bit plain text with 64 rounds and a key length of 128-bit with variable rounds having 32 cycles. It does not contain S- boxes and same algorithm is used in reversed for decryption. TEA algorithm offers the same security level as that of IDEA. TEA is also susceptible to a related-key attack. Because of these weaknesses, the XTEA cipher was designed.

2.6. CAST 5

CAST 5 was produced by Carlisle Adams and Stafford Tavares in 1996. CAST-128 (CAST 5) is a block cipher used for different applications, particularly as an evasion cipher in various editions of GPG and PGP. It is also used by the Canadian Communications Security Establishment permitted by

Canadian government [8]. It is symmetric key algorithm based on the backbone concept of feistel structure. It is a block cipher with a 64 bit plain text with 12 or 16 rounds and a variable key length of 40 to128-bit. It also contains 4 S- boxes and same algorithm is used in reversed for decryption [4]. It makes the use of variable key size operation to increase its security strength. The security of CAST 5 is a great level and it resistant against both linear & differential attacks [8].

2.7. AES (Rijndael)

Rijndael was developed by Joan Daemen and Vincent Rijmen in October 2000 declared by the National Institute of Standards and Technology. Rijndael using variable key size is extremely fast and compact cipher. The AES is a block cipher that uses a 128 bit plain text with variable 10, 12, or 14 rounds and a variable key length of 128, 192, 256 bit permuted into 10 sub- keys each of 128, 192, 256 bit length respectively. It only contains a single S- box and same algorithm is used in reversed for decryption.

AES is also a symmetric key algorithm based on the feistel structure. Security of Rijndael depends on its variable nature key size allowing up to a key size of 256-bit, to provide resistance against certain future attacks (collision attacks and potential quantum computing algorithms) [8]. General attacks of Irondale [7] are Square Attack, Improved Square Attack, Impossible Differential Attack and Reversed Key Schedule Attack, but none of the attacks were practically possible.

2.8. AES (RC6)

RC6, a derivative of RC5, designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin [8] is a symmetric key algorithm. It is patented by RSA Security. RC6 offers good performance in terms of security and compatibility. RC6 is a feistel structured private key algorithm that makes use a 128 bit plain text with 20 rounds and a variable key length of 128, 192, and 256 bit. It does not contain S- boxes and same algorithm is used in reversed for decryption.

Its security lies in the completely random series of its output bits with 15 rounds or less, running on input blocks of 128 bits[7]. A linear cryptanalysis attack can be launched for 16 rounds RC6. The RC6 algorithm is also strong against differential cryptanalysis, which worked with more than 12 rounds [8].

2.9. AES (Serpent)

Serpent is a symmetric key block cipher that was a finalist in the Advanced Encryption Standard (AES) contest. Serpent was designed by Ross Anderson, Eli Biham, and Lars Knudsen. Security presented by Serpent was based on more conventional approaches than the other AES finalists. It is open in the public sphere and not yet patented. Serpent is based on substitution-permutation network structure. It consists of a 128 bit plain text with 32 rounds and a variable key length of 128, 192, and 256 bit. It also contains 8 S- boxes and same algorithm is used in reversed for decryption.

In order to avoid the collision attack, serpent usually discreet to modify keys well before 264 blocks has been encrypted. Serpent with its minimum potential (only half number of rounds) is still as secure as that of three-key triple DES [8].

2.10. AES (Two Fish)

Two Fish is a symmetric key algorithm that was one of the five finalists of the Advanced Encryption Standard contest. Two Fish was designed by Bruce Schneier along with John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. It is also based on the feistel structure. The AES is a block cipher that uses a 128 bit plain text with 16 rounds and a variable Key Length of 128, 192, 256 bit. It makes use of 4 S-boxes (depending on Key) and same algorithm is used in reversed for decryption. It is an open to public sphere and not yet patented [8]. It is possibly susceptible to chosen-key attacks that may reduce the security of algorithm when applied to certain implementations, such as a hash function [7].

2.11. AES (MARS)

MARS base on layered, compartmentalized approach included Don Coppersmith (DES team member) [8]. It is based on heterogeneous structure. It makes use of a 128 bit plain text with 32 rounds and a variable key length from 128 to 448 bits (multiple of 32-bit). It only contains a single S- box the same algorithm is used in reversed for decryption.

MARS offers enhanced security and speed than triple DES and DES. It is an iterated cipher with unusually 32 rounds of different types. The middle rounds of MARS are the considered as its strong part. The security of MARS is dependent on data rotations. So, visual Cryptanalysis is not successful against MARS. It is highly resistant to against all kind of

Relative key attacks, differential attacks and timing attacks [8].

2.12. Advantages

Symmetric algorithms have some various advantages. Symmetric-key ciphers can be designed to have high rates of data [12]. Key lengths are relatively short. It can be employed as primitives to construct various cryptographic mechanisms. It can be composed to produce stronger ciphers and works with high speed in encryption. It does not consume too much of computing power [11].

2.13. Disadvantages

Symmetric algorithms have some various disadvantages. In a two-party communication system, the key must be shared by the sender and the receiver. Effective key management requires the use of an unconditionally trusted TTP [12]. Sound cryptographic practice dictates that the key be kept changing frequently for each communication session.

3. Asymmetric Encryption

The asymmetric key cryptographic algorithms involve large mathematical calculations and therefore, the time complexities are quite high [11]. Public key methods are important because they can be used for transmitting encryption keys. It is used to securely distribute the session key. It is better (more secure) than symmetric encryption. The following asymmetric algorithms such as RSA, DH, ECC and DSA are described in details according to their overview of architecture and security [8].

3.1. RSA

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. It is the most commonly used public key encryption algorithm. It is based on the presumed difficulty of factoring large integers, the factoring problem [3]. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key [8]. The prime factors must be kept secret. It involves three steps: key generation, encryption and decryption. The key size should be greater than 1024 bits for a reasonable level of security. It provides key size of 2048 bits. RSA can be used in mobile nodes, because they are vulnerable to many attacks due to their broadcast nature [10].

3.2. DH

The Diffie–Hellman key exchange method (DH) is a widely used key exchange algorithm. It is a public key encryption algorithm using discrete logarithms in a finite field. Two parties allow to exchange a secret key over an insecure medium without any prior secrets [13]. This key can then be used to encrypt subsequent communications using a symmetric key cipher. The method was followed shortly afterwards by RSA, an implementation of public key cryptography using asymmetric algorithms. Here, keys are exchanged between two users; unknown to each other [2].

3.3. ECC

ECC stands for Elliptical curve cryptography. It is a public key encryption technique based on elliptic curve theory. It can be used to create faster, smaller, and more efficient cryptographic keys. Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They are also used in several integer factorization algorithms such as Lenstra elliptic curve factorization. The attraction is the same level of security provided by keys of smaller size. Its key size (160 bits) is small and considered as much secure as RSA with 1024 bits key. It uses small length key pairs (Public and Private) to make robust with memory requirement and processing time. It is better decision for small devices with limited computational power and memory chip [5].

3.4. DSA

DSA stands for Digital Signature Algorithm. A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. It is a type of asymmetric cryptography. They are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. They are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type hash function. DSA is used to generate dynamic and smaller size of bits which depends on each byte of data [2].

3.5. Advantages

Asymmetric algorithms have some various advantages. Only the private key must be kept secret. Depending on the mode of usage, a private key/public key pair may remain unchanged for considerable

periods of time [12]. Many public-key schemes yield relatively efficient digital signature mechanisms. In a large network, the number of keys necessarily may be smaller than in the symmetric-key scenario.

3.6. Disadvantages

Asymmetric algorithms have some various disadvantages. The public-key encryption methods are several orders of magnitude slower than the best known symmetric-key schemes. Key sizes are typically much larger than symmetric key encryption and the size of public-key signatures is larger than providing data origin authentication from symmetric-key techniques [12].

Table 1. Symmetric & Asymmetric Algorithms Categories

Symmetric & Asymmetric Algorithms	Algorithm Structure	Plain Text / Cipher Text Length	Key Size (bits)	# of S boxes	# of Rounds	Flexible, Speed	Modification, Encryption ratio	Country (s)	Security Analysis (Attacks)
DES	Feistel Structure	64 bits	56	8	16	Yes, Fast	None, High	US (IBM)	Brute force
3DES	Feistel Structure	64 bits	112 to 168	8	48	Yes, Fast	168, Moderate	US (IBM)	Brute force , Chosen-plaintext, Known plaintext, Meet in the Middle
Blowfish	Feistel Structure	64 bits	32-448	4	16	Yes, Fast	64-448, High	US (Counterpane)	Dictionary attacks
IDEA	Substitution-Permutation Structure	64 bits	128	N/A	8	No	None	Switzerland	Bicliques attack
TEA	Feistel	64 bits	128	N/A	64 (32 cycles)	No	None	UK (Cambridge)	Chosen-plaintext, Related key
CAST 5	Feistel	64 bits	40-128	4	12-16	Yes	64,128,256	Canada	Linear & differential attacks
Rijndael	Feistel	128 bits	128,192,256	1	10, 12, 14	Yes, Fast	128,192,256 High	Belgium	Chosen-plain, Known plain text
RC6	Feistel	128 bits	128,192,256	N/A	20	Yes	128-2048	US (RSA)	Linear cryptanalysis , Known plain text
Serpent	Substitution-Permutatio	128 bits	128,192,256	8	32	Yes	256	UK, Israel, Norway	Collision attack

	n								
Two Fish	Feistel	128 bits	128,192,256	4	16	Yes	256	US (Counterpane)	Chosen Key Attack
MARS	Heterogeneous	128 bits	128-448	1	32	Yes	128-448	US (IBM)	Related key, Timing, Differential, Meet in the middle
RSA	N/A	N/A	>1024 bits	N/A	N/A	N/A, Fast	N/A, High	US (RSA)	Timing Attacks
DH	N/A	N/A	Key Exchange management	N/A	N/A	N/A, Slow	N/A, High	US (RSA)	Eavesdropping
ECC	N/A	N/A	160,224,256	N/A	N/A	N/A	N/A	US	Weil descent, Side-channel attacks
DSA	N/A	N/A	1024	N/A	N/A	N/A	N/A	US	Key-only known message

4. Conclusion

In this paper, the existing symmetric and asymmetric encryption algorithms are studied. In the symmetric encryption algorithms, the most popular symmetric key algorithms are studied. During this study, it was observed that AES (Rijndael) was the best among all symmetric encryption algorithms. And, in the asymmetric encryption algorithms, the most popular asymmetric key algorithms are studied. It is analyzed that Diffie-Hellman cryptography algorithm secret keys are exchanged between two users. Whereas a digital signature is used by receiver in DSA to confirm that the signal received is unaltered. It is also concluded that all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security.

References

[1] Bruce Schneier, Doug Whiting "A Performance Comparison of the Five AES Finalists", third AES Candidate Conference, 2000, to appear.

[2] Dimple, "Encryption Using Different Techniques: A Review", International Journal in Multidisciplinary and Academic Research (SSIJMAR), Vol. 2, No. 1, January-February-2013(ISSN 2278 – 5973).

[3] E .Thambiraja , G. Ramesh ,Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X.

[4] Heys, H.M.; Tavares, E.,"On the Security of the CAST Encryption Algorithm", Electrical & Computer Engg.

[5] Ijaz Ali Shoukat, Kamalrulnizam Abu Bakar, Mohsin Iftikhar," A Survey about the Latest Trends and Research Issues of Cryptographic Elements", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011,ISSN (Online): 1694-0814.

[6] John Justin M, Manimurugan S, "A Survey on Various Encryption Techniques", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[7] LimorElbaz&Hagai Bar-El, "Strength Assessment of Encryption Algorithms", October 2000,

[8] MansoorEbrahim, Shujaat Khan , Umer Bin Khalid "Symmetric Algorithm Survey: A Comparative Analysis", International Journal of Computer Applications (0975 – 887) Volume 61– No.20, January 2013.

[9] Mohit Mittal, "Performance Evaluation of Cryptographic Algorithms", International Journal of Computer Applications, ISSN 0975-8887.

[10] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tenjinder Singh "Comparative Analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology, ISSN 0976-3945.

[11] RituTripathi, Sanjay Agrawal. “Comparative Study of Symmetric and Asymmetric Cryptography Techniques” International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853.

[12] Santosh Kumar Yadav, “Some Problems in Symmetric and Asymmetric Cryptography”, DEPARTMENT OF MATHEMATICS, 2010.

[13] Simon Blake Wilson et al., “Key agreement protocols and their security analysis,”9-sep-1997.

[14] William Stalling,-Cryptography and network security: Principles and practices, fifth Edition.

[15] X. Lai and J. Massey. A proposal for a new block encryption standard. In Proceedings of the EUROCRYPT 90 Conference, pp. 3 89-404, 1990.

[16] Yogesh Kumar, Rajiv Munjal, Harsh Sharma, “Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures”, International Journal of Computer Science and Management Studies, ISSN: 2231-5268.