Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 10 (15): 1656-1661, 2010
ISSN 1812-5654

Suitability of Using Symmetric Key to Secure Multimedia Data: An Overview

[1]Mohamed Abomhara, [2] Othman O. Khalifa, [1]Omar Zakaria, [3]A.A. Zaidan,
[3]B.B. Zaidan and [1]Hamdan O. Alanazi
[1]Faculty of Computer Science and Information Technology, University of Malaysia,
50603, Kuala Lumpur, Malaysia
[2]Department of Electrical and Computer Engineering, Faculty of Engineering,
International Islamic University Malaysia, 53100 Gombak, Kuala Lumpur, Malaysia
[3]Faculty of Engineering, Multimedia University, 63100 Cyberjaya, Selangor Darul Ehsan, Malaysia

Abstract: With the increasing and continuous use of digital communications on the internet in recent times, security is becoming more and more relevant and important. However, special and reliable security is required for the many digital applications available such as video conferencing, digital television and mobile TV. The classical techniques of data security are not appropriate for the current multimedia usage. This study addresses the current algorithm of multimedia encryption schemes that have been proposed in the literature and description of multimedia security. It is a comparative study between symmetric key encryption and asymmetric key encryption in achieving an efficient, flexible and secure video data.

Key words: Multimedia security, data encryption standard, triple data encryption standard, advance encryption standard, symmetric key encryption, asymmetric key encryption

INTRODUCTION

An internet video streaming provides different features such as digital television, mobile TV, video conferencing and video in demand. Once the video stream goes beyond simple public communications and we start thinking about the possibilities, we realize that a lot of applications are not possible without some kind of data security (Abomhara *et al*., 2010a). We should not send information over public networks without some kind of reliable protection. The answer to cover this need in video streaming is no different than the answer anywhere else and it is cryptography (Naji *et al*., 2009a, b).

Cryptography can protect video streaming in different ways. It can provide encryption and decryption so that the video can be read only by authorized receivers. It provides a means to ensure that video reach their destinations without being tempered with. It provides ways to ensure the identity of communicating parties, making sure that none of them can deny that he/she had sent or received a specific video (Khalifa *et al*., 2004; Alaa *et al*., 2009).

AN OVERVIEW OF CRYPTOGRAPHY

Secured transmission/storage media against eavesdroppers is a very important task in applications such as commercial TV broadcast and video conferencing. However, cryptography (encryption and decryption) is being the science of protecting data. It can be applied to video streams at the transmitters and receivers (Rabah, 2006). Cryptanalysis is when hackers break the cryptography algorithms and decipher the encoded data (Naji *et al*., 2009a). It is a very sophisticated science to break the secrecy of encryption algorithms and reveal the encoded data. Thus, the main goal of cryptography is to keep the data secure from unauthorized individuals. Since cryptography's first known usage in ancient Egypt (Kessler, 1998), it has passed through various stages and has been affected by the ways in which people handled information. In the World War II, for instance, Cryptography played an important role and was a key element that gave the allied forces the upper hand, enabling them to win the war sooner, as they were able to dissolve the Enigma cipher machine, which the Germans used to encrypt their military secret communications (Kahn, 1980).

In modern days, cryptography is no longer limited to secure sensitive military information (Abomhara *et al*., 2010a). It was recognized as one of the major components of the security policy of any organization and considered industry standard for providing information security, trust, controlling access to resources and electronic financial transactions. The original data which is to be

Corresponding Author: Mohamed Abomhara, Faculty of Computer Science and Information Technology, University of Malaysia, 50603, Kuala Lumpur, Malaysia

transmitted or stored is called plaintext and this can be read and understood by either a person (a document) or by a computer. The disguised data, meanwhile, is called ciphertext and neither a human nor a machine can read it or properly process it until it is decrypted. A system or product that provides encryption and decryption is called cryptosystem (Zaidan *et al*., 2009a). Cryptosystem uses encryption algorithms to determine how simple or complex the encryption process will be, the necessary software component and the key (usually a long string of bits), which work with the algorithm to encrypt and decrypt the data (White, 2003; Harris, 2007).

In encryption, the key is a piece of information which specifies the particular transformation of plaintext to ciphertext, or vice versa during decryption. Encryption key is based on the keyspace, which is the range of the values that can be used to assemble a key. The larger the keyspace, the more possible keys can be constructed (e.g., today we commonly use key sizes of 128, 192,or 256 bit , so the key size of 256 would provide a 2^{256} keyspace) (Abomhara *et al*., 2010a). Moreover, the strength of the encryption algorithm relies on the secrecy of the key, the length of the key, the initialization vector and how they all work together. Depending on the algorithm and the length of the key, the strength of encryption can be considered (Zaidan *et al*., 2009b, 2010).

THE BASIC CONCEPTS OF VIDEO ENCRYPTION

The encryption and decryption of a plain text or a video stream can be done in two ways. In some of the encryption technologies, when two end points need to communicate with one another via encryption, they must use the same algorithm and most of the time, the same key. In other encryption technologies, they must use different but related keys for encryption and decryption purposes. Cryptography algorithms are either symmetric algorithms, which use symmetric keys (also called secret keys), or asymmetric algorithms, which use asymmetric keys (also called public and private keys).

Symmetric key algorithms: As shown in Fig. 1, in symmetric key encryption, the sender and receiver use the same key for encryption and decryption. Symmetric key encryption is also called secret key because both the sender and receiver have to keep the key secret and properly protected. If two users want to exchange data using secret key encryption, both of them must obtain a copy of the same key (Khalifa *et al*., 2004).

If one wants to communicate with the other person, then he needs to have three separate keys, one for each one. It sounds like is not a big deal, but if one wants to communicate with hundreds of people, keeping track and

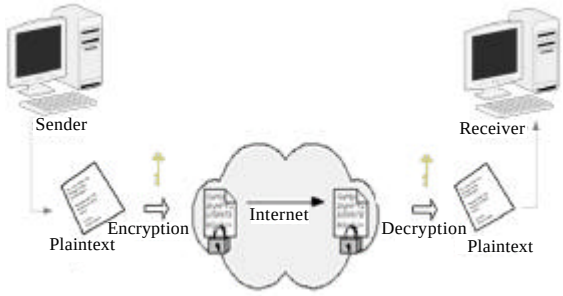

Fig. 1: Symmetric key algorithm

using the correct key that corresponds to each specific receiver can be a daunting task. The more people he wants to communicate with, the more number of keys he needs to keep. The equation used to calculate the number of symmetric keys needed is N (N-1)/2 = number of keys, where, N represents the number of users (Harris, 2007) (Abomhara *et al*., 2010a). Basically, the security level of the symmetric keys encryption method is totally dependent on how well the users keep the keys protected. If the key is known by an intruder, then all the data encrypted using that key can be decrypted. This is what makes it more complicated how symmetric keys are practically shared and updated when necessary. If one wants to communicate with another for the first time, he has to figure out how to send the right key to the second person securely. It is not safe to send the key by an e-mail or have it delivered by courier to get it to the user as the key will not be protected and can be easily intercepted and used by attackers.

Symmetric keys can provide confidentiality but they cannot provide authentication because there is no way one can prove, through cryptography, who actually sent a massage if two people are using the same key. Despite all the problems and defects that symmetric keys have, they are still used in many applications as they are fast and can be hard to break if using a large key size. Symmetric keys can handle a large amount of data that would take an unacceptable amount of time with an asymmetric key to encrypt and decrypt (Kessler, 1998).

The following are the advantages and disadvantages of the symmetric key systems:

Advantages:

- It is much faster than asymmetric systems
- Its security is dependent on the length of the key. If using a large key size, the algorithm will be hard to break because symmetric algorithms carry out relatively simplistic mathematical functions on the bits during the encryption and decryption processes

- It doesn't consume too much computing power

Disadvantages:

- It requires a secure mechanism to deliver keys properly
- Each pair of users needs a unique key; if a user has N trading partners, then N secret keys must be maintained so that as the number of individuals increases, so does the number of keys
- The management of the symmetric keys becomes problematic
- Provides confidentiality but not authenticity because the secret key is shared

According to the data on which they act, the secret key cryptography schemes are further divided into main type of subdivided. If an algorithm encrypts all the bits in a group of blocks at the same time, then the algorithm is called block encryption algorithm. However, if the algorithm is applied to each bit individually, it is called stream encryption algorithm. Stream encryption dose treats the input data as a stream of bits. The bits are then subjected to mathematical functions individually. A key generator is needed to provide a bit key to be XORed with the data bits and produce the encrypted stream. In block encryption algorithms, meanwhile, the data are divided into a group of blocks of bits and each block is encrypted one at a time (Harris, 2007).

The most popular secret key encryption algorithms are Data Encryption Standard (DES), Triple DES (Khalifa *et al*., 2004) and Advance Encryption Standard (AES).

Data Encryption Standard (DES): is one of the most important examples of a block cipher. DES was the result of a contest set by the U.S. National Bureau of Standards (now called the NIST) in 1973 and adopted as a standard application in 1977. The winning standard was developed at IBM as a modification of the previous system called LUCIFER (Alanazi *et al*., 2010a; Abomhara *et al*., 2010a). The DES is widely used for encryption of PIN numbers, bank transactions and the likes. The DES is an example of a block cipher, which operates on blocks of 64 bits at a time, with an input key of 64 bits. Every 8th bit in the input key is a parity check bit, which means that in fact the key size is effectively reduced to 56 bits (Rabah, 2005a).

Triple DES: was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56), beyond the reach of brute-force techniques, which are used by the EFF DES Cracker. Triple DES has always been regarded with some suspicion since the original algorithm was never designed to be used in this way, but no serious flaws have been uncovered in its design and today, it is used in a number of Internet protocols (Alanazi *et al*., 2010a).

Advanced Encryption Standard (AES): In 1997, the NIST called for the submission of a new standard to replace the aging DES. The contest terminated in November 2001 with the selection of the Rijndael cryptosystem as the Advanced Encryption Standard (AES) (Naji *et al*., 2009a). The Rijndael cryptosystem operates on 128-bit blocks, arranged as 4×4 matrices with 8-bit entries. The algorithm can use a variable block length and key length and the latest specification allows for the combination of any key lengths at 128, 192, or 256 bits and blocks of length at 128, 192, or 256 bits (Abomhara *et al*., 2010b; Alanazi *et al*., 2010a).

AES VS DES and 3DES: Advance Encryption Standard (AES) and DES (or 3DES) are commonly used block ciphers. Whether you choose AES or 3DES depends on your needs. In this section, we would like to highlight their differences in terms of security, performance and summaries, as shown in Table 1. Since 3DES is based on DES algorithm, it will talk first about DES (Alanazi *et al*., 2010b; Khalifa *et al*., 2004).

DES, which was developed in 1977, was carefully designed to work better in hardware than software. DES performs lots of bit manipulation in substitution and permutation boxes in each of the 16 rounds. For example, switching bit 30 with 16 is much simpler in hardware than software. DES encrypts data in 64 bit block size and uses a 56 bit key effectively. A 56 bit key space amounts to approximately 72 quadrillion possibilities (Xu and Dereje, 2004). Although, it seems large, according to today's computing power, it is still insufficient and vulnerable to brute force attack (Alanazi *et al*., 2010b). Thus, DES is not able to cope with the technological advancement and is no longer appropriate for security. Since DES was widely used at that time, a quick solution was to introduce 3DES, which was secure enough for most purposes today. 3DES is a construction of applying DES three times in sequence. 3DES, with three different keys (K1, K2 and K3), has effective key length of 168 bits (The use of three

Table 1: Comparative results of the symmetric encryption algorithm (Alanazi *et al*., 2010b)

Factor	AES	DES	3DES
Developed	2000	1977	1978
Key length	128, 192 or 256 bits	56, 48 bits sub-key	112, 186 bits
Key space size	2128, 2192 and 2256	256	2112, 2186
Memory requirement	Very low	N/A	A/A
Cipher type	Symmetric key	Symmetric key	Symmetric key
Block size	128, 192 or 256 bits	64 bits	64 bits
Security level	High	Low	Medium (one week which exit in DES)
Cryptanalysis resistance	Strong against differential, truncated differential linear, interpolation and square attack	Vulnerable to differential, brute force attacker could be analyzed with plaint text using differential cryptanalysis	Vulnerable to differential line cryptanalysis, wea substitution table
Time required to check all possible keys at 50 billion keys sec^{-1}	For a 128 bit key: 5*1021 years	For a 112 bit key: 800 days	For a 56 bit key: 400 days

distinct keys is recommended in 3DES). Another variation is called two-key (K1 and K3 are the same) 3DES, which reduces the effective key size to 112 bits, making it less secure. The two-key 3DES is widely used in electronic payments industry. 3DES takes three times as much CPU power compared to its predecessor, which is a significant performance hit.

The AES outperforms 3DES both in software and in hardware (Alanazi *et al*., 2010b).

The Rijndael algorithm has been selected as the Advance Encryption Standard (AES) to replace 3DES. The AES is a modified version of Rijndael algorithm. It was submitted by Joan Daemen and Vincent Rijmen. When considered together, Rijndael's combination of security, performance, efficiency, implement ability and flexibility made it an appropriate selection for the AES. By design, the AES is faster in software and works more efficiently in hardware. It also works fast in small devices such as smart phones, smart cards etc. The AES provides more security due to a larger block size and longer keys. It uses 128 bits fixed block size and works with 128, 192 and 256 bit keys. Generally, Rigndael algorithm is flexible enough to work with keys and block size of any multiple of 32 bits, with a minimum of 128 bits and maximum of 256 bits. Although the AES has abstract advantages over 3DES for speed and efficiency, in some hardware implementation, where support for 3DES is mature, 3DES may operate faster (Alanazi *et al*., 2010b).

Asymmetric key algorithm: is also called public key algorithm. Public Key Cryptography was first described publicly by Stanford University Professor Martin Hellman and graduate student Whitfield Diffie in 1976 (Diffie and Hellman, 1976). They described a two key crypto system, in which two parties could securely communicate over a non-secure communications channel without having to share a secret key and address the problem of secret key distribution by using two keys instead of a single key. In public key algorithm, two keys are used (Rabah, 2005b). A public key is a key which is known by everyone, while a

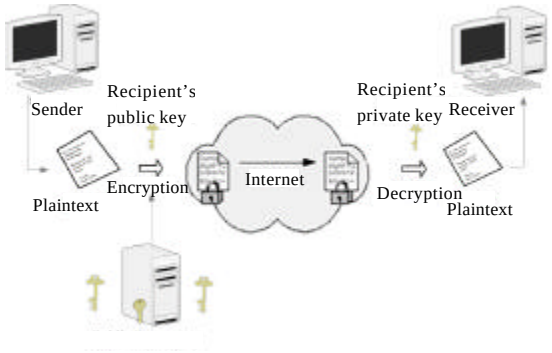

Fig. 2: Asymmetric key algorithm

private key should be kept secret and known only by the owner. This is shown in Fig. 2.

If the message is encrypted by one key, then the other key is required in order to decrypt the message. The public key and private key are mathematically related. However, it does not mean that if someone got the public key, he/she will be able to figure out the private key. But if someone obtains the private key, then there is big trouble as the private key should only be accessed by the owner and no one else (Harris, 2007; Abomhara *et al*., 2010b).

Each key in asymmetric key algorithm can be used to encrypt and decrypt as they both have the capability to do so. If a data is encrypted with a private key, it cannot be decrypted with a private key; it must be decrypted by the corresponding public key. Public key encryption provides both confidentiality and authentication. In the event that confidentiality is required, the sender would encrypt the data with the receiver's public key as in this matter, only the person who has the corresponding private key will be able to decrypt the data. This is called secure message format (Abomhara *et al*., 2010b). On the condition that authentication is required; the data would be encrypted with the sender's private key. Then each person who has the corresponding public key will be able

Table 2: Symmetric encryption vs. asymmetric encryption (Abomhara *et al.*, 2010b)

	Symmetic encryption	Asymmetic encryption
Functionality	Allows efficient communication between two parties in a closed environment	Enables security in settings in which symmetric encryption simply does not work or is more difficult to implement
Computational efficiency	Computes incredibly fast, since the relatively simple operations used are executed very efficiency	Computes slowly, using computationally heavy and complex operations, based on the difficulty of solving number-theoretic problems
Key size	Uses 128 bit symmetric keys, which are considered very secure	Employs key size of at least 1000 bits to achieve sufficient lasting security
Hardware	Performs simple algorithms, requiring relatively inexpensive hardware	Implements complex and time-consuming algoriths that need more powerful hardware
Security	No difference. Security is based on the strength of the algorithm and size of the key. Good algorithms exist for both encryption methods and key size effectiveness	

to decrypt the data. This allows the receiver to know that the data has been encrypted by the one who has the possession of that private key. Encrypting the data with a private key is called open message format, since confidentiality is not ensured. Anyone with a copy of the corresponding public key can decrypt the data.

Asymmetric algorithms work much slower than the symmetric algorithm because they use more complex mathematics to perform their functions, which require more processing time. With public key, you can just send out your public key to all of the people whom you need to communicate with, instead of keeping track of a unique key for each one of them.

The following are the advantages and disadvantages of the Asymmetric Key Systems:

Advantages:

- Better key distribution than symmetric systems
- Better scalability than the symmetric systems
- It provides authentication and confidentiality

Disadvantages:

- Works much more slower than symmetric systems
- It provides mathematically intensive tasks

One of the most used public key algorithms today is Rivest-Shamir Adelman (RSA). This algorithm was invented in 1977 by Ron Rivest, Adi Shamir and Len Adelman. The RSA is based on the idea of factorization of integers into their prime. Assuming that A and B want to communicate with one another and B chooses two distinct large primes p and q and multiplies them together to form N, N = p*q. He also chooses an encryption exponent e, such that the greatest common divisor of e and [(p-1)*(q-1)] is 1. That is gcd(e,[(p-1)*(q-1)])=1. He computes his decryption key d, d=1/e (mod [(p-1)*(q-1)]). Now he makes the pair (N,e) public and keeps p and q secret. This is how to generate keys and encryption and decryption are of the following forms. For some plain text block M and ciphertext block C: $C = M^e \bmod n$, $M = C^d \bmod n = (M^e) \bmod n = M^{ed} \bmod n$. Both the sender and receiver must know the values of n and e and only the receiver knows the value of d. This makes a public key encryption of KU = {e, n} and private of KR {d, n}.

THE SUITABILITY OF USING SYMMETRIC KEY TO SECURE MULTIMEDIA DATA

Although, asymmetric encryption provides far more functionality, there are still many applications in which symmetric encryption are the best solution, as it does the job securely and more efficiently. Due to its nature, symmetric technology is also far less expensive to implement. Public key cryptography is not applicable for securing real time video conferencing, as its operations require a large amount of time, which is unsuitable for video conferencing. The principal aspects of the two methods are compared in Table 2.

CONCLUSION

In this study, a comparative study between symmetric and asymmetric key encryption was presented. First of all, a brief discussion about the popular cryptography algorithms was made. A general survey about the use of cryptography and how it started was highlighted. Next, the current known methods of cryptography (Symmetric key encryption and Asymmetric key encryption) were discussed and evaluated in terms of their security level and encryption speed. Subsequently, the advantages and disadvantages of each type were presented, while illustrating their usage in different applications. Apart from this, brief synopses regarding the difference between block encryption and stream encryption was given. Last but not least, some examples of the encryption algorithms were provided, whereby the AES and DES were evaluated in terms of their speed and security level, as well as their suitability to secure video data.

ACKNOWLEDGMENTS

Authors would like to express our heartfelt appreciation to all those who have helped us understand the importance of knowledge and showed us the best way to attain it. We would also like to extend our gratitude to the Multimedia University, Malaysia for their ceaseless support in making our study successful.

REFERENCES

Abomhara, M., O. Zakaria and O.O. Khalifa, 2010a. An overview of video encryption techniques. Int. J. Comput. Theory Eng., 2: 103-110.

Abomhara, M., O. Zakaria, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2010b. Enhancing selective encryption for H.264/AVC using advance encryption standard. Int. J. Comput. Electr. Eng., 2: 223-229.

Alaa, T., A.A. Zaidan and B.B. Zaidan, 2009. New framework for high secure data hidden in the MPEG using AES encryption algorithm. Int. J. Comput. Electr. Eng., 1: 566-571.

Alanazi, H.O., A.H. Jalab, A.A. Zaidan and B.B. Zaidan, 2010a. New frame work of hidden data with in non multimedia file. Int. J. Comput. Network Security, 2: 46-54.

Alanazi, H.O., B.B Zaidan, A.A. Zaidan, A.H. Jalab, M. Shabbir and Y. Al-Nabhani, 2010b. New comparative study between DES, 3DES and AES within nine factors. J. Comput., 2: 152-157.

Diffie, W. and M. Hellman, 1976. New directions in cryptography. IEEE Trans. Inform. Theory, 22: 644-654.

Harris, S., 2007. CISSP® All-in-One Exam Guide. 4 Edn., McGraw-Hill, New York.

Kahn, D., 1980. Cryptology goes public. IEEE Commun. Magazine, 4: 19-28.

Kessler, G.C., 1998. An overview of cryptography. Retrieved from (accessed, 20 DES, 2009). http://www.garykessler.net/library/crypto.html#intro.

Khalifa, O.O., M.D. Rafiqul Islam, S. Khan and M.S. Shebani, 2004. Communications cryptography. Proceedings of the RF and Microwaves Conference RFM2004, Oct. 5-6, Subang, Selangor, Malaysia, pp: 220-223.

Naji, A.W., A.A. Zaidan and B.B. Zaidan, 2009a. Challenges of hidden data in the unused area two within executable files. J. Comput. Sci., 5: 890-897.

Naji, A.W., A.A. Zaidan, B.B. Zaidan, A. Shihab and O.O. Khalifa, 2009b. Novel approach of hidden data in the (unused area 2 within exe file) using computation between cryptography and steganography. Int. J. Comput. Sci. Network Security, 9: 294-300.

Rabah, K., 2005a. Theory and implementation of data encryption standard: A review. Inform. Technol. J., 4: 307-325.

Rabah, K., 2005b. Theory and implementation of elliptic curve cryptography. J. Applied Sci., 5: 604-633.

Rabah, K., 2006. Implementing secure RSA cryptosystems using your own cryptographic JCE provider. J. Applied Sci., 6: 482-510.

White, B.G., 2003. Cisco Security + Certification: Exam Guide. McGraw-Hill, New York.

Xu, Q.Z. and Y. Dereje, 2004. Theoretical Analysis of linear cryptanalysis against DES (Data Encryption Standared). Inform. Technol. J., 3: 49-56.

Zaidan, A.A., B.B. Zaidan and M. Anas, 2009a. High securing cover-file of hidden data using statistical technique and AES encryption algorithm. World Acad. Sci. Eng. Technol., 54: 468-479.

Zaidan, A.A., F. Othman, B.B. Zaidan, R.Z. Raji, H.K. Ahmed and A.W. Naji, 2009b. Securing cover-file without limitation of hidden data size using computation between cryptography and steganography. Proc. World Cong. Eng., 1: 259-265.

Zaidan, A.A., B.B. Zaidan, A.H. Jalab, 2010. A new system for hiding data within (Unused Area Two + Image Page) of portable executable file using statistical technique and advance encryption standard. Int. J. Comput. Theory Eng., 2: 220-227.