Research Journal of Information Technology, 2011
ISSN 1815-7432 / DOI: 10.3923/rjit.2011.

A Review on Multimedia Communications Cryptography

[1]Yasser Salem, [2]Mohamed Abomhara, [3]Othman O. Khalifa, [4,5]A.A. Zaidan and [4,5]B.B. Zaidan

[1]Department of Computer Science, Faculty of Science, University of Sabah, Sabah, Libya
[2]Faculty of Computer Science and Information Technology, University of Malaysia, 50603, Kuala Lumpur, Malaysia
[3]Department of Electrical and Computer Engineering, Faculty of Engineering, International Islamic University Malaysia, 53100 Gombak, Kuala Lumpur, Malaysia
[4]Faculty of Engineering Multimedia University, 63100, Cyber Jaya, Malaysia
[5]Predictive Intelligence Research Cluster, Sunway University, No 5, Jalan Universiti, Bandar Sunway, 46150 Petaling Jaya, Selangor, Malaysia

Corresponding Author: Yasser Salem, Department of Computer Science, Faculty of Science, University of Sabah, Sabah, Libya

ABSTRACT

Now-a-days, Due to the repaid increasing and continuous use of multimedia communications on the internet, Security is becoming more and more relevant and important. However, special and reliable security is required for the many multimedia 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 will presents the currently algorithm of multimedia encryption schemes that have been proposed in the literature and description the effectiveness of the 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: Cryptography, multimedia security, symmetric key encryption, asymmetric key encryption, data encryption standard, triple data encryption standard, advance encryption standard

INTRODUCTION

Internet and multimedia have widespread application in areas such as digital television, mobile TV and video-conferencing. Once multimedia goes beyond simple public communications, then various factors have to be considered. One important factor to consider is that data security. Information sent or transmitted over the public networks must have reliable protection. The protection for multimedia applications can be achieved by using cryptography (Zaidan *et al*., 2010b, c).

Cryptography can protect multimedia applications in different ways. The multimedia applications are subjected to encryption and decryption so that it can be read only by authorized receivers (Ahmed *et al*., 2010). The use of cryptography also ensures that the data reaches its destination without change (not tempered with). It verifies the identity of the communicating parties and ensures that none of them can deny that he/she has sent or received a specific video (non-repudiation) (Al-Frajat *et al*., 2010).

Today, the use of multimedia data and contents are very widespread and is becoming a part of our daily life. In the absence of a reliable security system to protect multimedia data, multimedia users on the public networks like the Internet face risk of their sensitive information being compromised (Zaidan *et al*., 2010a). It is necessary, therefore, to provide adequate security for such information so that the service provided is reliable for conducting various types of business transactions. There is a need for end-to-end encryption for multimedia data. Due to the fact that, while communication between users can be made secure using encryption, multimedia transmitted between them through a public network is not encrypted.

The results from a number of researches indicate that multimedia data can be encrypted using symmetric key algorithm. Thus, the use of the symmetric key algorithm is a solution to provide end-to-end security for multimedia data (Zaidan *et al*., 2010d, e).

CRYPTOGRAPHY BASICS

Cryptography is based on hard mathematical problems like prime number factorization. It is not difficult to find the result of multiplying two numbers but it is extremely challenging to find prime factors of a number. Thus, cryptography is concerned with the design and the analysis of mathematical techniques which can offer secure communications in the presence of malicious adversaries. It is an area which is concerned with the transformation of data for security reasons. Cryptography first known usage was in ancient Egypt (Hmood *et al*., 2010a) and it has passed through different stages and had been affected by many events but had always been concerned about the way people handle information. In World War II, for instance, cryptography played an important role and was a key element that gave the allied forces the upper hand and enabled them to win the war (Hmood *et al*., 2010b). Using cryptographic methods, the allied forces were able to dissolve the Enigma cipher machine which the Germans used to encrypt their secret military communications (Hmood *et al*., 2010c).

Today, the use of cryptography is no longer limited to protect sensitive military information. It is now recognized as one of the major issues of the security policy of any organization and is indispensable to provide information security, trust, controlled access to resources and ensure secure electronic financial transactions. Before moving further, these are a number of terms which are commonly associated with cryptography (Zaidan *et al*., 2010f):

- **Plaintext** : The message which is transmitted to the recipient
- **Encryption** : The procedure of changing the content of a message in a way that it conceals the real message
- **Ciphertext** : The output which is produced after encrypting the plaintext
- **Decryption** : The reverse function of encryption. It is the process of retrieving the plaintext from the ciphertext

Security requirements: There must be some security services to secure the communications, to prevent some security issues such as eavesdropping. Cryptography provides the following security services (Abomhara *et al*., 2010a):

- **Confidentiality** : A service which keeps information accessible only to those who are authorized to access this information. The service contains both protection of all user data which are being transmitted between points and likewise, the protection of the traffic flow analysis

- **Integrity** : A service which ensures that only authorized users who are capable of writing, deleting of the transmitted information
- **Authentication** : A service which a receiver determines its source to confirm the sender's identity by using something that you have or you know. Normally, it is done by using the sender public key. It is the same integrity provided by digital signature
- **Non-repudiation** : It ensures the sender and receiver from denying the sending or receiving of a message and the authenticity of their signature. Typically, it is provided by digital signature

TYPES OF CRYPTOGRAPHY

Cryptographic systems can be divided into two types, namely Symmetric and Asymmetric cryptography. Both are used to protect the communication privacy between the entities to avoid eavesdropping and alteration. The next section provides a discussion on both types of cryptography and discuses their advantages and disadvantages (Alanazi *et al*., 2010a, b).

Symmetric cryptography: Symmetric cryptography (shared key) is a cryptosystem which provides the ability to secure exchange of messages between two ends. At the initial stage, the entities intend to communicate agree on a key. Integrity can be resolved using a suitable mode of operation with a symmetric cipher. Authentication in the symmetric cryptography can be achieved only if there are two entities sharing the same key. Authentication is to verify the identity of an individual, such as a person at a remote terminal or the sender of a message and ensuring that a message is genuine, has arrived exactly as it was sent and came from the stated source.

In spite of the fact that the symmetric cryptography provides all the security services, it still has some drawbacks. A scenario where we have communicating n entities and each two entities have their own shared key, the drawbacks will be as listed below (Abomhara *et al*., 2010a):

- It requires a secure transmission of the secret key before exchanging messages
- Each pair of users needs a different key. Assuming that a network has n users, this result in N (n-1)/2 key pairs
- Having this much of keys introduces the need for a secure storage of the secret key pairs. Where if one entity hacked, the whole network would be in danger

To clarify this scheme, a scenario can be assumed by two entities, namely A (Alice) and B (Bob) who are communicating over an insecure channel. Assuming that all communications take place in the presence of an enemy E (Eve) whose objective is to overcome any security services used by A and B. Assume that A and B are using the Internet as their communications channel as it is depicted in Fig. 1. EVE could try to read the traffic from A to B; therefore, learning A's credit card information or could attempt to masquerade as either A or B in the transaction. Another example, consider a situation where Alice is sending an e-mail message to Bob over the same medium (Internet). Eve could attempt to read the message or even modify it or send a message to Bob as if it was sent from Alice.

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

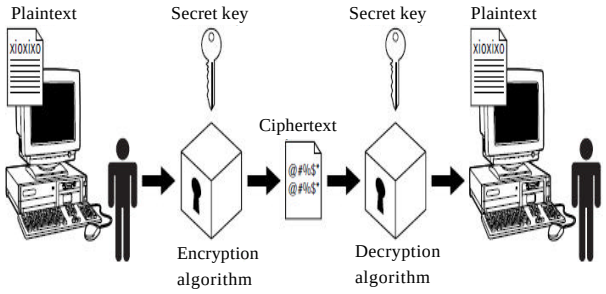

Fig. 1: Communication over insecure line

Data Encryption Standard (DES): DES was the result of a contest set by the US 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. 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 (Abomhara *et al*., 2010a).

Triple DES: was developed based on the DES algorithm to address the obvious flaws in DES. 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 aroused 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 (Abomhara *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*., 2009). 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 (Alam *et al*., 2010).

Asymmetric-key cryptography: Asymmetric-key cryptography, known as the Public-Key Cryptography (PKC), was proposed by Diffie and Hellman (1976) who introduced the concept of public-key cryptography. The idea of public-key cryptography is defining two different keys; one key (private key) is used to encrypt the plaintext and the other key (public key) to decrypt it. To send a message to a node, e.g., Bob; Bob's public key is used by Alice to encrypt the message. The cipher can only be decrypted using Bob's private key. The basic protocol between the two parties, i.e., Alice and Bob, is depicted in Fig. 2, in which EKpup is Bob's public key and Kpr is Bob's private key (Abomhara *et al*., 2010b).

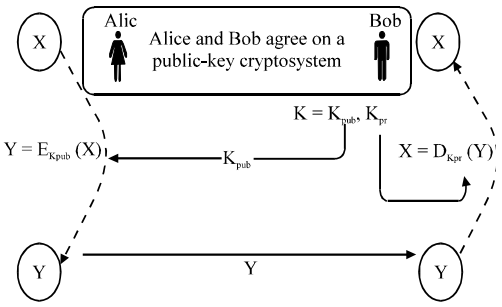

Fig. 2: Public key encryption protocol

Public-key schemes require the communicating parties to exchange keying material in an authenticated way. Despite the fact that the PKC has achieved all the security services, it still has some disadvantages as compared to the symmetric cryptography (Nabi *et al.*, 2010):

- Asymmetric encryption process uses a complicated mathematics compared to symmetric cryptography
- The asymmetric cryptography algorithms are much computationally demanding than the symmetric key algorithms

Even when the Public Key (PK) is properly implemented, it is still very slow as compared to the best known private key schemes. A hybrid cryptography scheme was introduced; it is a mixture of the PK and the symmetric cryptography and is used in some applications. The hybrid cryptosystem uses the PKC to agree on the shared key and then it uses the symmetric cryptography to encrypt and decrypt the messages. The public key cryptosystem algorithms can be categorized into three different groups, such as:

Algorithms based on the Discrete Logarithm Problem (DLP): The method to solve a given instance of the DLP is dependent on the size of the parameters and each time, the parameter size increases the difficulty of solving the problem. Given positive numbers a and b, find positive integer k such that b = a.k mod p, i.e., Diffie and Hellman and Digital Signature Algorithm (DSA).

Algorithms based on the Integer Factorization Problem (IFP): As for the integer factorization problem, its hardness is important for the security of the RSA public-key encryption and signature schemes. The problem of hardness resulted from the difficulty of finding the prime factorization of a given positive integer n, i.e., RSA.

Algorithms based on Elliptic Curve Discrete Logarithm Problem (ECDLP): The challenging part of this problem is to find the positive integer k given two points P and Q on an elliptic curve over a finite field, such that Q = k * P, i.e., the Elliptic Curve Digital Signature Algorithm (ECDSA) (NIST, 2000).

The most computationally intensive operation for Discrete Logarithm and RSA is based on the modular exponentiation. These operations are performed using very long operands to meet the required key size. The operands in the ECDLP algorithms are smaller than that in the Discrete Logarithm (DL) systems.

Table 1: Symmetric encryption VS asymmetric encryption

	Symmetric encryption	Asymmetric 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 efficiently.	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 sizes of at least 1000 bits to achieve sufficient, lasting security.
Hardware	Performs simple algorithms, requiring relatively inexpensive hardware.	Implements complex and time-consuming algorithms 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	

THE SUITABILITY OF USING SYMMETRIC KEY TO SECURE MULTIMEDIA DATA

Although asymmetric encryption provides far more functionalities, there are still many applications in which symmetric encryption is the best solution and does the job as securely and more efficiently. Because of its nature, symmetric technology is far less expensive to implement. The principal aspects of the two encryption methods are compared in Table 1.

CONCLUSION

In this study, a comparative study between symmetric and asymmetric key encryption was presented A brief discussion about the popular cryptography algorithms was made. A general survey about the use of cryptography and how it started was highlighted. The current known methods of cryptography (Symmetric key encryption and Asymmetric key encryption) were discussed 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

I would like to express our appreciation to all who have helped us understand the importance of knowledge and showed us the best ways to gain it.

REFERENCES

Abomhara, M., O. Zakaria, O.O. Khalifa, A.A. Zaidan, B.B. Zaidan and O.A. Hamdan, 2010a. Overview: Suitability of using symmetric key to secure multimedia data. J. Applied Sci., 10: 1656-1661.

Abomhara, M., O.O. Khalifa, O. Zakaria, A.A. Zaidan, B.B. Zaidan and A. Rame, 2010b. Video compression techniques: An overview. J. Applied Sci., 10: 1834-1840.

Ahmed, M.A., M.L.M. Kiah, B.B. Zaidan and A.A. Zaidan, 2010. A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. J. Applied Sci., 10: 59-64.

Al-Frajat, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010. Hiding data in video file: An overview. J. Applied Sci., 10: 1644-1649.

Alam, G.M., M.L.M. Kiah, B.B. Zaidan, A.A. Zaidan and H.O. Alanazi, 2010. Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study. Sci. Res. Essays, 5: 3254-3260.

Alanazi, H.O., H.A. Jalab, G.M. Alam, B.B. Zaidan and A.A. Zaidan, 2010a. Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. J. Med. Plants Res., 4: 2059-2074.

Alanazi, H.O., M.L.M. Kiah, A.A. Zaidan, B.B. Zaidan and G.M. Alam, 2010b. Secure topology for electronic medical record transmissions. Int. J. Pharmacol., 6: 954-958.

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

Hmood, A.K., B.B. Zaidan, A.A. Zaidan and H.A. Jalab, 2010a. An overview on hiding information technique in images. J. Applied Sci., 10: 2094-2100.

Hmood, A.K., H.A. Jalab, Z.M. Kasirun, B.B. Zaidan and A.A. Zaidan, 2010b. On the Capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Hmood, A.K., Z.M. Kasirun, H.A. Jalab, G.M. Alam, A.A. Zaidan and B.B. Zaidan, 2010c. On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates. Int. J. Phys. Sci., 5: 1054-1062.

NIST, 2000. Digital signature standard (DSS). FIPS PUB 186-2, National Institute for Standards and Technology, http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2.pdf.

Nabi, M.S.A., M.L.M. Kiah, B.B. Zaidan, A.A. Zaidan and G.M. Alam, 2010. Suitability of SOAP protocol in securing transmissions of EMR database. Int. J. Pharmacol., 6: 959-964.

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

Zaidan, A.A., B.B. Zaidan, A.K. Al-Fraja and H.A. Jalab, 2010a. Investigate the capability of applying hidden data in text file: An overview. J. Applied Sci., 10: 1916-1922.

Zaidan, A.A., B.B. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010b. An overview: Theoretical and mathematical perspectives for advance encryption standard/rijndael. J. Applied Sci., 10: 2161-2167.

Zaidan, A.A., B.B. Zaidan, A.Y. Taqa, K.M.S. Mustafa, G.M. Alam and H.A. Jalab, 2010c. Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem. Int. J. Phys. Sci., 5: 1992-2000.

Zaidan, A.A., B.B. Zaidan, H.O. Alanazi, A. Gani, O. Zakaria and G.M. Alam, 2010d. Novel approach for high (Secure and rate) data hidden within triplex space for non multimedia file. Sci. Res. Essays, 5: 1965-1977.

Zaidan, B.B., A.A. Zaidan, A. Taqa, G.M. Alam, M.L.M. Kiah and H.A. Jalab, 2010e. StegoMos: A secure novel approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem. Int. J. Phys. Sci., 5: 1796-1806.

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010f. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.