An Analysis and Comparison for Popular Video Encryption Algorithms

Mohammed A. Saleh, Nooritawati Md. Tahir, Ezril Hisham & Habibah Hashim
Faculty of Electrical Engineering, Universiti Teknologi MARA
Shah Alam, Selangor, Malaysia

Abstract_ The security of video in the communication field become the major concern, especially after the rapid development of multimedia technology (internet and mobile devices). Since the using of multimedia data transmission become more and more due to the wide internet using all around the world, the video protection techniques, is becoming necessary to keep that information not accessible by irrelevant public or malicious attackers. The researchers have designed different type of encryption algorithms to secure the multimedia data, that algorithms have their strength and weakness points. In this paper, we will focus on introducing and comparison between the three popular encryption algorithms, DES, RSA and AES, as well to choose which encryption algorithm can be used to exchange video safely, and maintain the balancing between the security and computational time.

Keywords: Asymmetric Encryption, Symmetric encryption, Data Encryption Standard (DES), Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES). Encryption algorithms comparison.

I. INTRODUCTION

According to the rapid growth of using mobile systems and the massive using of video through the internet networks. There is an imperative need to secure a sensitive multimedia data through the transmission processes, a popular way to do so is made by encrypting the video data stream using cryptography systems which is composed of one of the encryption algorithms for instance DES. One of the main challenges for securing video streaming is the amount of the data that should be encrypted, whereas the videos have large amount of data. Moreover, according to the resource, power and memory limitations in the mobile system, the video encryption algorithm should be selected carefully. For real-time video transmission, the selected encryption algorithm has to take into account various parameters like security, computational issues. The different types of encryption algorithms were designed to use in information security.

There are two main types of cryptographic system: symmetric key cryptography, and asymmetric key cryptography. The key in cryptographic systems means the value that used by an encryption algorithm to generate a ciphertext from the original data (plaintext) to making that data secured and visible only to individuals who have the corresponding key to recover it.

Symmetric Key Cryptography (private-key encryption)

With this type of cryptography, both the sender and the receiver know the same secret code, which called the key. In this encryption type the same secret key is used by the sender and the receiver, whereas the sender encrypts the plaintext data and the receiver decrypts the chipertex data with the same key. Fig. 1 shows the block diagram of the symmetric cryptography (private-key encryption).

Asymmetric Key Cryptography (public key encryption)

With this type, the cryptographic is unlike the symmetric encryption, where the two keys are used to encrypt the plaintext as well as decrypts the ciphertext data. Fig. 2 shows the block diagram of asymmetric cryptography, whereas one of these two keys is used as a public key and it's distributed publicly and the other is called private key which is kept secret by its owner. According to the highest computational processing power that requires in asymmetric key cryptography, they are slower than Symmetric key cryptography by hundreds of times.

The purpose of this paper is to analyze the three popular encryption algorithms and compare between them in terms of encryption and decryption methods, computational issues and security. In addition, to show the most suitable algorithm to secure a video transmission and compliance with the limitations in the mobile system. The rest of the paper is organized as follows: In section II, the encryption algorithms DES, RSA, AES are described briefly. Video encryption algorithms are briefly described in section III. Section IV, contains the comparison between the DES, RSA, AES algorithms according to their encryption and decryption processes, Computational issues, and security weakness and strength points, and finally the paper is ended with the conclusion in section V.

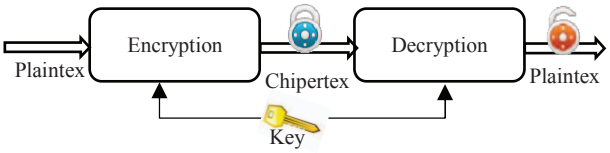

Fig. 1. Block diagram of asymmetric cryptography

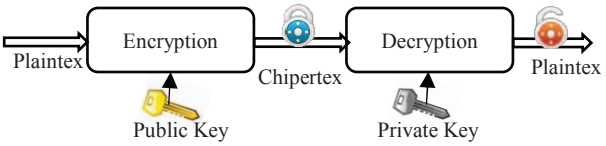

Fig. 2. Block diagram of symmetric cryptography

978-1-4799-8969-0/15/$31.00 ©2015 IEEE

II. ENCRYPTION ALGORITHMS

Encrypting algorithms are used to convert an original data (plain text message) to an encrypted data (ciphertext message) in a form that can retrieve the original data by decrypting process. That algorithm uses a key to encrypt and decrypt the intended data. Whereas the strength of the encryption algorithms depends on the type of that algorithm and length of the keys.

There are popular types of encryption algorithms that used to secure multimedia data. The classification of encryption techniques is shown in Fig. 3. Here, in this section the three important encryption algorithms are discussed:

A. DES

Data Encryption Standard (DES), it was developed by IBM in the 1970, and adopted by the US government as a national office of standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976 [1]. DES is a block cipher and based on symmetric key encryption with 64 bit block data size encrypting by a 56 bit key. Many attacks were registered on DES, so it was enhanced to become 3-DES with increasing the key bits into 168 bits to increase the encryption level, but it faced the problem is of slowness. The encryption method in the 3-DES algorithm is same as in the original DES, but with increasing the encryption level by applying DES three times. Thus, by applying the DES encryption algorithm three times on each data block, 3-DES become slower than AES encryption algorithm.

B. RSA

Ron Rivest, Adi Shamir and Leonard Adleman (RSA) is a public key encryption algorithm (Asymmetric Cryptography), it was described publicly in1977 [2] [3]. It can used to provide secrecy and digital signature, by utilizing the practical difficulty of factoring the product of two prime numbers and the factoring problem [3]. In RSA a public key and a private key are generated, whereas the public key is used to encrypt the desired block data (plaintext messages), where everyone can have the public key, while the private key is used to decrypt the encrypted block data (ciphertext messages). If the value of keys (public and privet) are small then the security become weak, so it can be decrypted by side channel attacks or random probability theory [1], but if the value of keys is large then more time will consume in the encryption and decryption process that causes a performance degradation compared to other algorithms.

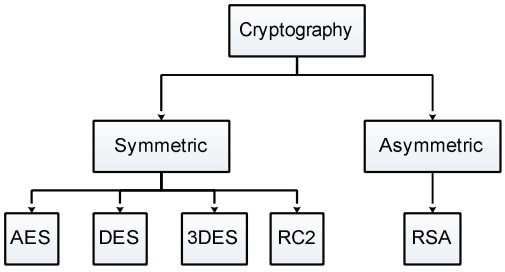

Fig. 3. The classification of encryption techniques

C. AES

In 2001, the US government adopted advanced encryption standard (AES) that was designed in 1998 by Vincent Rijmen and Joan Daemena. AES is a symmetric key encryption algorithm; it encrypts 128 bit block size by one of three types of key size, which are: 128, 192, or 256 bit. In AES the encryption and decryption is being by a same key (symmetric encryption). The numeral of iteration of transformation rounds are determined by the key length [4], therefore for the 128 bit key, the number of round are 10, also for 192 and 256 bit key size are 12 and 14 respectively. AES was classified by the National Security Agency (NSA) as the encryption standard for safe and transfer of top secret information [5].

III. VIDEO ENCRYPTION ALGORITHMS

A Multimedia communication is one of the dramatically growing of the information technology revolution nowadays, thus cause the increasing in remote video communication demand. To provide the secured way for the transmission of video information, the encryption techniques have been being developed. Though, the security aspects of video connections have yet to be fully addressed. The recently use standards of video coding do not include the encryption techniques.

In many cases of the encryption methods, the encryption of the compressed video data is secured as any other data types, that means the encryption process is performed after the completing of video encoding process, whereas the decryption in the receiver side is performed before all stages of video decoding process [6].

For instance the Naïve encryption algorithm is one of famous encryption methods, while its encryption process is simple and direct, thus the all data are encrypted. Nowadays, the researchers' focus include data Encryption for video streaming in securing the contents of translated media, which considered as a challenge due to video streaming requirements, data communications, data retrieval, video contents compression and resource of hardware requirements. To ensure the video transmission security and deal with the computational overhead that can be generated by applying the encryption algorithms in real time video transmission, the researcher have propose different types of encryption algorithm, here the encryption algorithms are classified into three main categories:

A. Fully Data Encryption

In this type of algorithms, the content of the video is completely encrypted after the compression process using any encryption standard algorithms such as DES, RSA, IDEA, AES. However, in real time video transmission, the fully data encryption technique is not appropriate due to computation overhead and slow speed that can be generated by that algorithm.

B. Permutation Data Encryption

In this type, the video encryption algorithms generally use some of the permutation algorithms that scrambles the contents of the video. The scrambling process of this algorithm can be applied on each or specific part of video data. Since in some algorithms the permutation list is used as the secret key to encrypt video data contents [7], Fig. 4 shows the Permutation Encryption Scheme.

C. Selective Data Encryption

In this type of algorithms, some parts of video contents are selected and encrypted using any encryption standard algorithms such as DES, RSA, IDEA, AES. Because each byte is not encrypted, and according to the size of the selective video data, the computational time and complexity are reduced. Fig. 5. Shows the logical steps of complete (Naïve) Encryption Scheme and Selective Encryption Scheme in the video system.

IV. COMPARISONS

Every encryption algorithm has its characteristic; the level of security, hardware cost, computational overhead, and resource consuming, so the security level depends on a some factors such as, number of bits key. Here, according to those characteristics we will compare between the most popular three algorithms DES, RSA and AES. Table I. show the comparison between the encryption algorithms.

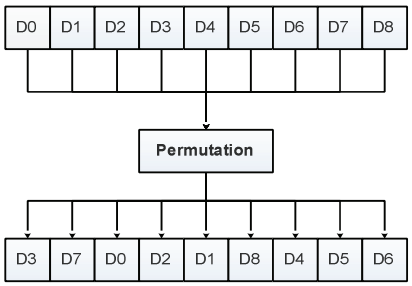

Fig. 4. Permutation Encryption Scheme

TABLE I. COMPARISON OF ENCRYPTION ALGORITHMS

FACTORS	DES	AES	RSA
DEVELOPED	1970	2000	1977
KEY LENGTH (BITS)	56, 168	128,192 or 256	Variable
BLOCK SIZE (BITS)	64	128	Less than or equal to log2(n)*
CIPHER TEXT	Symmetric block cipher	Symmetric block cipher	Asymmetric Block Cipher
SECURITY	Low	High	High
POSSIBLE KEYS	2^{56}	2^{128}, 2^{192} and 2^{256}	Variable
COMPLEXITY	Complex	Complex	Simple

* The block size must be less than or equal to log2(n); where $2k < n <= 2^{k+1}$.

A. Encryption and Decryption

Encryption and decryption process are responsible for making the data impossible to decode without knowing the encryption and decryption key by converting a plaintext (data) into ciphertext and retrieve the plaintext (data) from ciphertext. Every encryption algorithm has its way to encrypt and decrypt the data. In this section we will discuss those processes in the DES, RSA, and AES algorithms.

1) DES

a) Encryption: The encryption process of DES is based on substitution and transportation attributes, DES consists of

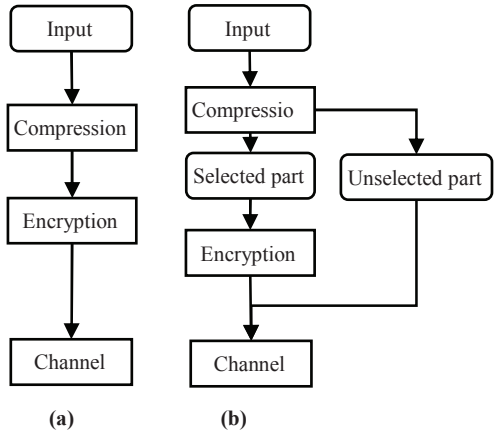

Fig. 5. (a) Naïve Encryption Scheme, (b) Selective Encryption Scheme [11].

16 rounds where every round performs substitution and transportation as:

- Handling over a plaintext block of 64 bits to Initial Permutation (IP) function.
- Two halves of permutated block are produced by Initial Permutation (Left Plaintext(LPT) and Right Plaintext(RPT) [2] [3] [4]).
- Each LPT and RPT go through 16 rounds for encryption process.
- Rejoined of each LPT and RPT, and performs the final permutation on the combined block.

b) Decryption: Same as the encryption process, with some of minor differences the decryption is performed in DES. The reversal of key portions in the decryption process differs from the encryption. Such as, if N is the original key and divided into N1, N2, N3,…. N16 rounds, the key in the decryption will be as N16, N15, N14,…. N1.

2) RSA

a) Key generation: Before performing the encryption and decryption process the RSA algorithm generate the public and private key. Let the public key is (N, E) And the private key is (N, D).

b) Encryption: The encryption process in RSA is performed as follow:

- The input binary text is divided into 8 bits separately.
- Convert the first 8 bits into an integer form M.
- Public key (N, E) will be taken from key generator.
- Perform the encryption process for that integer M.

- Generate the ciphertext C =M^E mod N.
- Send the ciphertext C to the receiver.

c) Decryption:

- The input binary text is divided into 8 bits separately.
- Convert the first 16 bits into an integer form.
- Privet key (N, D) will be taken from key generator.
- Perform the decryption process for that integer.

  $M = C^D$ mod N [8].

3) AES

a) Encryption: In AES Standard the encryption and decryption process are accomplished by performing some rounds, where the number of rounds depends on the key size (e.g. 128,192, and 256 key required 10, 12, and 14 rounds respectively), each round performs some specific functions [9]. AES starts by initializing first round following by a number of rounds and ended by the final round. The encryption steps are ordered as follow:

- Bytes Substitution: Every byte in an input state is replaced by the corresponding byte from the s-box (substation table).
- Rows Shifting
  1- Unchanged the 1st row.
  2- The bytes in the 2nd, 3rd and 4th rows are cyclically shifted by 1, 2 and 3 bytes to the left, respectively.
- Mixing Columns: The columns in the state array are considered as a polynomial over GF (28). Using multiplying a fixed polynomial M(x) with modulo x^4+1. Where $M(x)=03*x^3+ 01*x^2+ 01*x + 02$ [10].
- Add Round Key: Performs XOR between the state and 128-bits of the round key.

b) Decryption: The Decryption process of AES is same as the encryption process, but in the reverse order:

- Shift rows inversion
- Sub bytes transformation using S-Box Inversing
- Mix column inversion
- Sub key inversion

B. Computational issues

1) DES: The computational complexity in DES is caused by the large computations and complications of the encryption process of this algorithm. Furthermore the software implementation of DES is slow in processing the large amounts of multimedia data [11].

2) RSA: To secure a given message M by RSA, the system computes S = MEmod N, where N = L *Q is a result of two prime integers each N/2 bits long and E is a secret key of signer. However the main computational issue can caused by the modular exponentiation of a message M. The Chinese remainder theorem (CRT) was used to speed up the RSA encryption and decryption computation [12], so using CRT The RSA becomes four times faster than the direct exponentiation algorithm.

3) AES: Each byte in AES algorithm is considered as Galois field, GF(28), which is an element of a finite field of characteristic 28 terms. Whereas GF(28) is the field of 256 elements, and a polynomial of degree 7 with a coefficient {0, 1} represents each element of which [9]. The operations that generate the computational complexity are:

a) Addition and Subtraction: The addition and subtraction operations are performed on any elements by XORing the coefficients of the corresponding powers in the polynomials for those elements.

For example: $(x^6+ x^4+ x^2+x + 1) \oplus (x^5+ x^4 + x + 1) = (x^6+ x^5 + x^2)$.

b) Multiplication: The multiplication operation in AES is performed by ordinary polynomial multiplication and taking its reminder by an irreducible polynomial of degree 8 ($M(x) = (x^8+ x^4 + x^3 + x + 1)$).

Example: $(x^6+ x^4+ x^2+ x + 1)(x^7+ x + 1)$

$=(x^{13}+ x^{11}+ x^9+ x^8+ x^6 + x^5 + x^4 + x^3 +1)$

And modulo of $(x^{13}+ x^{11}+ x^9+ x^8+ x^6+ x^5+ x^4+ x^3 +1)$ with $M(x) =(x^7+ x^6+ 1)$.

C. Security

1) DES: The Brute Forced, Linear and differential cryptanalysis are the main attacks on DES that have been registered. In spite of the massive published information on the cryptanalysis of DES encryption standard, a brute force approach still the most practical attack until now [13].

2) RSA: The registered attacks on RSA algorithm are: Brute force, Oracle attacks, Mathematical attacks, Timing attacks and Chosen Ciphertext attacks. Whereas the attacker use different methods to attack the RSA encryption algorithm, thus the RSA cryptosystem security is imperfect [9].

3) AES: The security strength of all keys of AES algorithm (i.e., 128, 192 and 256) is sufficient to protect classified information up to the secret level [5]. Whereas the key lengths 192 and 256 provide top-secret information. Only the side channel attacks on some specific implementations have successfully published on AES algorithm. So there are no major security attack has been proven successful against the AES till now [9]. The AES algorithm has been reviewed by The National Security Agency (NSA) and stated that, the AES algorithm is enough secured for U.S. Government non classified data.

V. Conclusion

In this paper, we have studied symmetric and asymmetric encryption algorithm and presented a theoretical performance analysis and comparisons between the three commonly use encryption algorithms; DES, RSA and AES by highlighting some of the important characteristics as well as the computational and security issues of both algorithms. We conclude that, a symmetric key cryptographic system provides higher security and faster than asymmetric key cryptographic system. DES security has proven as an inadequate safe algorithm. Meanwhile AES algorithm

provides better security and has very low memory requirements , it become one of most efficient encryption algorithm, and emerged as one of the strongest encryption algorithm from the existed algorithms. In addition to that, AES has chosen as the appropriate encryption algorithm to secure the real-time video stream, whereas the plaintext of AES is derived by concatenation for encoded video data stream [15]. However, the critical issue of AES and DES encryption algorithms is the secret key distribution. As an asymmetric cryptosystem, RSA solves the problem inherent distributing the secret key. But the major drawback of RSA is its greater computational overhead due to its large key [9].

ACKNOWLEDGMENT

The authors would like to acknowledge the Ministry of Education (MOE) Malaysia for providing the grant 600-RMI/NRGS 5/3 (5/2013), and Research Management Institute of Universiti Teknologi MARA (UiTM) for supporting this research work.

REFERENCES

[1] A. Kakkar, M. L. Singh, and P. K. Bansal, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network," vol. 2, no. 1, pp. 87–92, 2012.

[2] A. K. Lenstra, J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter, "Ron was wrong, Whit is right.," IACR Cryptol. …, pp. 1–16, 2012.

[3] D. Brumley and D. Boneh, "Remote timing attacks are practical," Comput. Networks, vol. 48, pp. 701–716, 2005.

[4] P. S. Mukesh, M. S. Pandya, and S. Pathak, "Enhancing AES algorithm with arithmetic coding," 2013 Int. Conf. Green Comput. Commun. Conserv. Energy, pp. 83–86, Dec. 2013.

[5] J. Song, K. Lee, and H. Lee, "Biclique cryptanalysis on lightweight block cipher: HIGHT and Piccolo," Int. J. Comput. Math., pp. 1–16, 2013.

[6] A. Pande, P. Mohapatra, and J. Zambreno, "Securing Multimedia Content using Joint Compression and Encryption," IEEE Multimed., pp. 1–1, 2012.

[7] S. Gupta, "Comparative Analysis of Encrypted Video Streaming in Cloud Network," vol. 5, no. 4, pp. 5470–5476, 2014.

[8] Y. Kumar, R. Munjal, and H. Sharma, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures," vol. 11, no. 03, pp. 60–63, 2011.

[9] A. Al Hasib and A. A. M. M. Haque, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography," 2008 Third Int. Conf. Converg. Hybrid Inf. Technol., no. November 2001, pp. 505–510, Nov. 2008.

[10] B. Manoj and M. N. Harihar, "Image Encryption and Decryption using AES," no. 5, pp. 290–294, 2012.

[11] P. Kawle, A. Hiwase, G. Bagde, E. Tekam, and R. Kalbande, "Modified Advanced Encryption Standard," no. 1, pp. 21–23, 2014.

[12] C. Kim, J. Ha, S. Kim, S. Kim, S. Yen, and S. Moon, "A Secure and Practical CRT-Based RSA to Resist Side Channel Attacks," 2004.

[13] S. K. R and B. Gambhava, "New Approach of Data Encryption Standard Algorithm," no. 1, pp. 322–325, 2012.

[14] A. Kulkarni, "Proposed Video Encryption Algorithm v / s Other Existing Algorithms : A Comparative Study," vol. 65, no. 1, pp. 3–7, 2013.

[15] Z. Shahid, M. Chaumont, and W. Puech, "Fast Protection of H.264/AVC by Selective Encryption of CAVLC and CABAC for I and P Frames," vol. 5, pp. 565–576, 2011.