Method for comparative performance analyze of encryption algorithms used in Public Key Infrastructure for secure transmitting of audio information

Snezhana Pleshkova, Dimitar Kinanev
Blvd. Kliment Ohridski 8
Department of Telecommunications, Technical University, Sofia, Bulgaria
dimitarkinanev@gmail.com

***Abstract**: In this article it will be analyzed the characteristics of the symmetric encryption algorithms Blowfish, Advanced Encryption Standard, Data Encryption Standard and Triple Data Encryption Standard for securing audio information using developed method for measuring their performance. The results will be compared with already examined ones based on the developed method for performance evaluation of the asymmetric encryption algorithm Rivest-Shamir-Adleman with which their advantages and disadvantages will be analyzed. For that purpose the resources provided by the Java programming language will be used.*

1. INTRODUCTION

The primary advantage of public-key cryptography is increased security and convenience: private keys never need to be transmitted or revealed to anyone. In a secret-key system for protecting audio information, by contrast, the secret keys must be transmitted (either manually or through a communication channel) since the same key is used for encryption and decryption. A serious concern is that there may be a chance that an enemy can discover the secret key during transmission of the audio information. Another major advantage of public-key systems is that they can provide digital signatures that cannot be repudiated. Authentication via secret-key systems requires the sharing of some secret and sometimes requires trust of a third party as well. As a result, a sender can repudiate a previously authenticated message by claiming the shared secret was somehow compromised by one of the parties sharing the secret.

A disadvantage of using public-key cryptography for encryption of audio information is the speed. There are many secret-key encryption methods that are significantly faster than any currently available public-key encryption method.

Based on this and on the fact that there are no detailed researches which analyze what would be the effect if encryption/decryption is applied when transmitting audio information in order to ensure its security, a method for performance evaluation of the symmetric algorithms will be developed.

2. BRIEF OVERVIEW OF METHODS FOR SYMMETRIC ENCRYPTION BLOWFISH, AES, DES AN 3DES

Blowfish [1] is designed in 1993 by Bruce Schneier. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. Blowfish is a fast block cipher, except when changing keys. Each new key requires pre-processing equivalent to encrypting about 4 kilobytes of text, which is very slow compared to other block ciphers.

The Advanced Encryption Standard (AES) [2], also known as Rijndael (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

The symmetric-key algorithm Data Encryption Standard (DES) [3] is developed in the early 1970s. DES is now considered to be insecure for many applications. This is mainly due to the 56-bit key size being too small. DES is the archetypal block cipher—an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length.

Triple DES (3DES) [4] applies the DES cipher algorithm three times to each data block. Triple DES provides a relatively simple method of increasing the key size of DES to protect against attacks, without the need to design a completely new block cipher algorithm.

3. Practical analyzes of Blowfish, AES, DES and 3DES encryption algorithms applied for security of audio information.

Figure 1 illustrates the workflow of the developed method for analyze of the symmetric algorithms performance used for encryption/decryption of audio information:

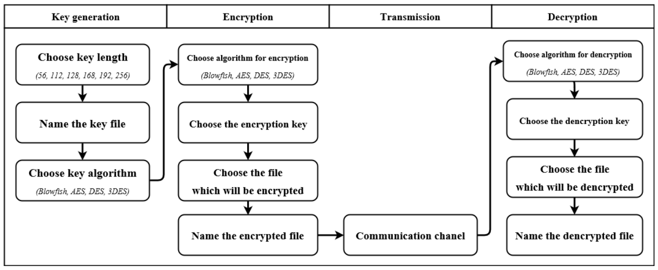
Key generation
Encryption
Transmission
Decryption
Choose key length
(56, 112, 128, 168, 192, 256)
Name the key file
Choose key algorithm
(Blowfish, AES, DES, 3DES)
Choose algorithm for encryption
(Blowfish, AES, DES, 3DES)
Choose the encryption key
Choose the file which will be encrypted
Name the encrypted file
Communication chanel
Choose algorithm for dencryption
(Blowfish, AES, DES, 3DES)
Choose the dencryption key
Choose the file which will be dencrypted
Name the dencrypted file

Fig. 1. Workflow of the developed method for analyze of the symmetric algorithms performance used for encryption/decryption of audio information

3.1. Key generation

During the key generation process with the command >java -cp . keyGen “key size” “file name” “algorithm” the following parameters are set:

Choose key length – They could be 56, 112, 128, 168, 192, 256 bits

Name the key file – provide a name of the file where the key will be stored

Choose key algorithm – provide which algorithm will be used for the key generation

AES key generation could be described in four steps:

• KeyExpansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

• InitialRound

AddRoundKey—each byte of the state is combined with a block of the round key using bitwise XOR.

• Rounds

SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

Each byte $a_{i,j}$ in the matrix is replaced by Sub byte $S(a_{i,j})$. The below two conditions should be met:

$$S(a_{i,j}) \neq a_{i,j} \quad (1)$$

$$S(a_{i,j}) \otimes a_{i,j} \neq 0xFF \quad (2)$$

ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

AddRoundKey

• Final Round (no MixColumns)

SubBytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.

ShiftRows - a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

AddRoundKey - each byte of the state is combined with a block of the round key using bitwise XOR

Table 1 defines the supported key lengths from the examined symmetric algorithms. It is visible that Blowfish is the most flexible algorithm in this aspect since it supports various key lengths unlikely the other algorithms.

Table 1. Symmetric algorithm supported key lengths

Key length (bits)	Blowfish	AES	DES	3DES
56	+	-	+	-
112	+	-	-	+
128	+	+	-	-
168	+	-	-	+
192	+	+	-	-
256	+	+	-	-

3.2. Encryption

During the key generation process with the command >java -cp . keyChiper “algorithm” “action” “key file” “file to be encrypted” “name of the encrypted file” the following parameters are set:

Choose algorithm for encryption – Choose the algorithm which will be used to encrypt the file.

Choose the encryption key – Point from where the software to take the encryption key which will be used to encrypt the file

Choose the file which will be encrypted – Point the file which will be encrypted.

Name the encrypted file – Point what will be the name of the newly produced encrypted file.

For each round in Blowfish $i = 0,1,...,n$ compute

$$L_{i+1} = R_i \, , \tag{3}$$

$$R_{i+1} = L_i \oplus F(R_i, K_i) \, . \tag{4}$$

Then the cipher text is

$$(R_{n+1}, L_{n+1}) \tag{5}$$

3.3. Decryption

During the key generation process with the command >java -cp . keyChiper “algorithm” “action” “key file” “file to be decrypted” “name of the decrypted file” the following parameters are set:

Choose algorithm for decryption – Choose the algorithm which will be used to decrypt the file.

Choose the decryption key – Point from where the software to take the decryption key which will be used to decrypt the file

Choose the file which will be decrypted – Point the file which will be decrypted.

Name the decrypted file – Point what will be the name of the newly produced decrypted file.

The decryption of a chipper text (5) is accomplished by computing for $i = n, n-1,...,0$

$$R_i = L_{i+1} \tag{6}$$

$$L_i = R_{i+1} \oplus F(L_{i+1}, K_i) \tag{7}$$

4. EXPERIMENTAL RESULTS FROM TESTING SYMMETRIC ENCRYPTION ALGORITHMS BLOWFISH, AES AND DES. COMPARISON BETWEEN THE RESULTS WITH THE ASYMMETRIC ENCRYPTION ALGORITHM RSA

The tests have been completed on computer with the following parameters:

Processor: Intel(R) Core(TM) i5-4300U CPU @ 1.90 Ghz 2.50Ghz; Installed memory (RAM): 8 GB; System type: 64-bit; Operating System: Windows 7

Java library: JDK 1.8.0_71

Table 2 illustrates the results from the conducted tests of encrypting the test audio file.

Table 2. Experimental results of encryption

	Time (ms)			
Key length (bits)	Blowfish	AES	DES	3DES
56	440	-	48	-
112	306	-	-	28
128	305	306	-	-
168	295	-	-	21
192	294	314	-	-
256	293	315	-	-

From the results it is visible that Blowfish`s performance is getting better with the key length growth. However, DES and 3DES provides the best speed performance while encrypting the audio information.

Table 3 illustrates the results from the conducted tests of decrypting the encrypted test audio file:

Table 3. Experimental results of decryption

	Time (ms)			
Key length (bits)	**Blowfish**	**AES**	**DES**	**3DES**
56	294	-	21	-
112	295	-	-	23
128	297	296	-	-
168	298	-	-	21
192	299	300	-	-
256	300	303	-	-

Considering the characteristic of the encryption and decryption process, normally the decryption takes less time as visible also from the results. It is visible that again DES and 3DES provides best times for encryption and decryption compared with Blowfish and AES.

In comparison Table 4 illustrates the performance results for the asymmetric RAS algorithm [5]:

Table 4. Experimental results for RSA algorithm

	RSA	
Key length (bits)	**Time for encryption (ms)**	**Time for decryption (ms)**
56	294	-
112	295	-
128	297	296
168	298	-
192	299	300
256	300	303

5. Conclusions

During the test it has been seen that there is no limitation of the audio file size which could be encrypted at a time unlikely the RAS algorithm where larger files should be divided into blocks 53 bytes long each.

From the carried out tests [Table 2, Table 3] it is visible that at one hand the symmetric algorithms are faster than the asymmetric RSA [Table 4] which is caused by the smaller keys they use but at the other it illustrates their weakness in comparison with the RSA asymmetric algorithm since the smaller key used is less secure and easy predictable. Based on these results in encryption systems for securing audio information the best solution is to combine the symmetric and asymmetric algorithms in order to get both the security advantages of public-key systems and the speed advantages of secret-key systems.

The obtained results from these tests could be used for further analyze of the influence on transmitting audio information if encryption and decryption is applied, for example in VoIP systems where the audio information is transmitted live and there are defined expectations about the acceptable delay.

Acknowledgment

This work was supported by Technical University – Sofia inner program to research projects under 172PD0032-07: “Algorithms for the study of methods for improving the security of information through audio infrastructure for encryption with public key in multimedia communications computer systems and networks”.

References

[1] Bruce S. "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)". Fast Software Encryption, Cambridge Security Workshop Proceedings. Springer-Verlag. 1993, pp. 191–204.

[2] Daemen, J., R. "AES Proposal: Rijndael". National Institute of Standards and Technology. 2003 p. 11-126.

[3] Biham E. "Differential Cryptanalysis of DES-like Cryptosystems". Journal of Cryptology, 1991

[4] Barker W. "NIST Special Publication 800-67 Version 1: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher", 2004

[5] Pleshkova Sn., D. Kinanev. “Method for security enhancement of audio information in communication multimedia systems and networks applying encryption algorithm with public key”.CEMA’2016, Athens, pp. 77-81