Text and Biomedical Images Disguising using Advanced Encryption Standard

Ali E. Taki El_Deen[1]
IEEE senior member,
Alexandria University, Egypt

Mohy E. Abo-Elsoud[2]
IEEE senior member,
Electronics and Communications Dept,
Mansoura Universit, Egypt

Salma M. Saif[3]
Electronics and Communications Dept, Mansoura University, Egypt

***Abstract*— Medical images security has become a pressing issue as communications of images increasingly extends over open networks, and hospitals are hard-pushed by government mandates, and security guidelines to ensure health data security. Hence, Data Security is widely used to ensure security in communication, data storage and transmission. This paper presents the application of the 128, 192, and 256-bits AES for text and biomedical images encryption and decryption. Also a comparison between AES, DES, RSA, and Blowfish encryption algorithms will be discussed**.

***Keywords*— AES, Medical image security, Encryption, Decryption, DES, RSA, Blowfish**

1. INTRODUCTION

The science of secrecy includes two different approaches: the design of proper tools to insure secrecy which is stricto sensu cryptography (cryptographie) and the attacks of these tools to find out their weaknesses, called cryptanalysis (cryptanalyse). Thus the science that covers these two parts is nowadays called cryptology (cryptologie) [1].

Providing confidentiality is not the only objective of cryptography. Cryptography is also used to provide solutions for other problems:

1. Data integrity. The receiver of a message should be able to check whether the message was modified during transmission, either accidentally or deliberately. No one should be able to substitute a false message for the original message, or for parts of it.

2. Authentication. The receiver of a message should be able to verify its origin. No one should be able to send a message to Bob and pretend to be Alice (data origin authentication). When initiating a communication, Alice and Bob should be able to identify each other (entity authentication).

3. Non-repudiation. The sender should not be able to later deny that she sent a message [2].

Cryptography is the study of methods for sending messages in secret (namely, in enciphered or disguised form) so that only the intended recipient can remove the disguise and read the message (or decipher it) [3].

There are many applications for cryptography in many fields such as biomedical engineering, military applications, network communication security, space community, and mobile systems.

For an example, Encrypting data on mobile devices eliminates the dangers associated with loss or theft. The process makes data worthless to unauthorized users. Typically, by processing data through a mathematical formula called an algorithm, encryption software converts data into "ciphertext." Following this conversion, that data requires users to input their unique credentials to gain access to it. Provided those credentials stay private, they make it virtually impossible for others to access the data.

Another example is that, NASA, ESA, and the rest of the space community, including commercial companies, are increasingly reliant on terrestrial and space networking to return critical data. With that comes a requirement for strong security for data that can range from an astronaut's personal information to valuable commercial satellite imagery.

So, Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to. Businesses use it to protect corporate secrets, governments use it to secure classified information, and many individuals use it to protect personal information to guard against things like identity theft.

Cryptography is divided into several branches as shown in figure 1.

Symmetric ciphers: Both the sender and the receiver agree on a single key for their communication, the key is used to encrypt and to decrypt the data [4].

Asymmetric ciphers: Also called public-key cryptography. In this case two different keys are involved, they are related by some mathematical property. Everybody who is in possession of the public key can encrypt data, but cannot decrypt it, just the person holding the secret key can decrypt this data [4].

Block ciphers: A Block Cipher is a cryptosystem that separates the plaintext message into strings, called blocks, of fixed length k ∈ N, called the block length, and enciphers one block at a time [3].

Stream ciphers: Stream ciphers are a very important group of ciphers. A stream cipher is a cryptosystem that transforms (encrypts or decrypts) individual symbols of the alphabet, which are usually simply binary digits, one at a time [5].

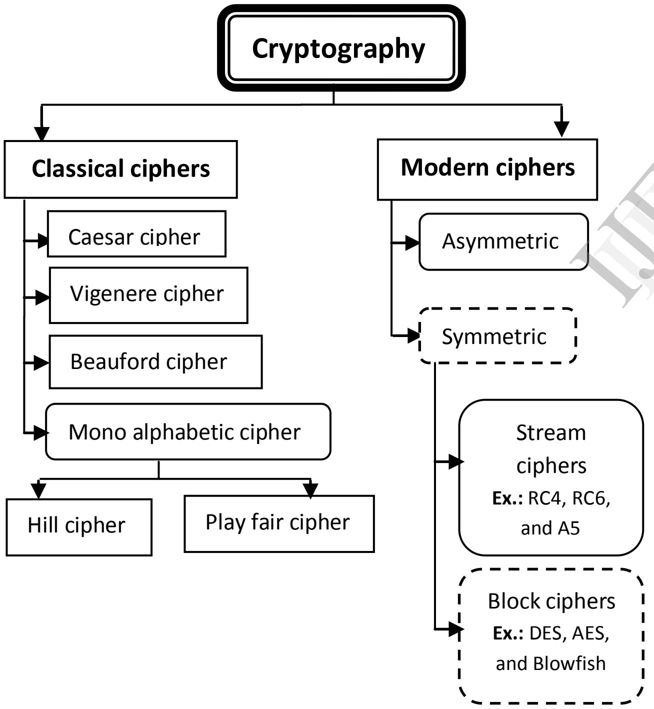

Fig 1: Cryptography branches

AES has been designed to be resistant to well-known attacks and exhibits simplicity of design.

The remainder of this paper is organized as follow: Section (2) covers an overview of the AES algorithm. Multimedia elements are presented in Section (3), while, section (4) provides the discussion of the experimental results. Finally the paper is concluded in Section (5).

2. Overview of the AES Algorithm

The AES cipher is almost identical to the block cipher Rijndael. The Rijndael block and key size vary between 128, 192 and 256 bits. However, the AES standard only calls for a block size of 128 bits. Hence, only Rijndael with a block length of 128 bits is known as the AES algorithm. The number of internal rounds of the cipher is a function of the key length according to table 1.

Key lengths	*# rounds = n_r*
128 bit	10
192 bit	12
256 bit	14

Table 1: Number of internal rounds

AES consists of so-called layers. Each layer manipulates all 128 bits of the data path [6]. There are only three different types of layers. Each round, with the exception of the first, consists of all three layers. The last round nr does not make use of the MixColumn transformation, which makes the encryption and decryption scheme symmetric.

Key Addition layer: A 128-bit round key, or subkey, which has been derived from the main key in the key schedule, is XORed to the state.

Byte Substitution layer (S-Box): Each element of the state is nonlinearly transformed using lookup table with special mathematical properties.

Diffusion layer: It provides diffusion over all state bits. It consists of two sublayers, both of which perform linear operations:

- The ShiftRows layer permutes the data on a byte level.
- The MixColumn layer is a matrix operation which combines (mixes) blocks of four bytes [6].

The key schedule computes round keys, or subkeys, $(k_0,k_1, . . . ,k_{nr})$ from the original AES key [6].

The AES decryption process uses the following three transformations: InvShiftRows, InvSubBytes, and InvMixColums. As the name indicates, these are essentially inverse transformations of ShiftRows, SubBytes, and MixColumns used during the encryption process [5]. However, it turns out that the inverse layer operations are fairly similar to the layer operations used for encryption. In addition, the order of the subkeys is reversed, i.e., we need a reversed key schedule [6].

The Overall flow of the encryption and decryption algorithm of the 128 bits AES algorithm is show in Figure 2.

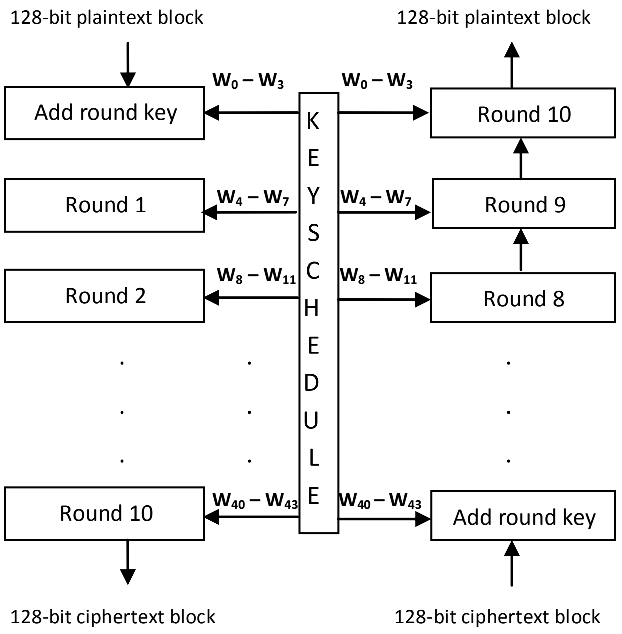

Fig 2: Design flow of 128 bits AES Algorithm [7]

If we compare AES as a symmetric key type with RSA as an asymmetric key type, it is obvious that 1024-bit RSA keys are equivalent in strength to 80-bit symmetric keys, 2048-bit RSA keys to 112-bit symmetric keys and 3072-bit RSA keys to 128-bit symmetric keys. RSA claims that 1024-bit keys are likely to become crackable sometime between 2006 and 2010 and that 2048-bit keys are sufficient until 2030. An RSA key length of 3072 bits should be used if security is required beyond 2030. NIST key management guidelines further suggest that 15360-bit RSA keys are equivalent in strength to 256-bit symmetric keys.

Blowfish has a 64-bit block size whereas AES has a 128-bit block size, so you are sort of comparing apples and oranges (there are some things you can do in AES which would be unwise in Blowfish, in particular Blowfish in CTR mode can be distinguished from a random stream after only a few dozen gigabytes of output, replacing 128 by 64 in the calculations).

As for strict brute force complexity, I think you've pretty much answered your own question, if we assume that 256-bit keys are sufficiently resistant to brute-forcing then using a longer key makes no sense. It's like trying to decide what's best between "infeasible" and "infeasible". But theoretically speaking, Blowfish uses all 448 bits of the key, so a brute-force attack would take on average 2447 guesses at the key.

DES is a block cipher, with a 64-bit block size and a 56- bit key whereas AES has a 128-bit block size and supports three key lengths 128- bit, 192- bit, and 256- bit. DES consists of a16-round series of substitution and permutation while AES consists of 10, 12, or 14 rounds depending on key length. DES uses a balanced Feistel structure while AES does not. DES is vulnerable to differential and linear cryptanalysis; weak substitution tables while AES is Strong against differential, truncated differential, linear, interpolation and square attacks.

3. Multimedia Elements

i. Text

Inclusion of textual information in multimedia is the basic step towards development of multimedia software. Text can be of any type; may be a word, a single line, or a graph. The textual data for multimedia can be developed using any text editor.

However to give special effects, one needs graphics software which supports this kind of job.

Even one can use any of the most popular word processing software to create textual data for inclusion in multimedia. The text can have different type, size, color, and style to suit the professional requirement of the multimedia software [8].

ii. Image

Another interesting element in multimedia is graphics does not have a single agreed format. They have different format to suit different requirements. The size of a graphic depends on the resolution it is using. A computer image uses pixel or dots on the screen to form itself. And these dots or pixels, when combined with number of colors and aspects are called resolution.

Resolution of an image or graphics is basically the pixel density and number of colors it uses, and the size of image depends on its resolution [8].

The image may suffer from degradations which have occurred during the acquisition of the image. Such degradations may include noise, which are errors in the pixel values, or optical effects such as out of focus blurring, or blurring due to camera motion. Image restoration concerns the removal or reduction of these degradations [9].

4. Experimental Results

1-Text:

128-bits AES:

Plaintext:

Name: Salma Mohamed Seif El-eslam saad El-dein Ibrahim El-mansy.

Ciphertext:

\Ë 8Î !ñÝd° sªn {iëºsëu"Ð ÒgúÿUÝí¨ OstK&I Z*rÁ5ó Ë!¨B ñ

192-bits AES:

Plaintext:

Name: Salma Mohamed Seif El-eslam saad El-dein Ibrahim El-mansy.

Ciphertext:
ZB Äªpj}Ü!&-±UyÈë7Ò89 /zãvä*1®2²3qÌ)l?,É_F¤º &2ö z@Z • ®îÚ

256-bits AES:

Plaintext:
Name: Salma Mohamed Seif El-eslam saad El-dein Ibrahim El-mansy.

Ciphertext:
z[úê3d ø&Óß •ïÕB Þ/|DÌ ¡ þ ÿþ-F»x\) èû}Ììµ@Öò A°w4nBû |"è~

Let s = s_0; s_1; s_2; ….. ; s_{n-1} be a binary sequence of length n. This subsection presents four statistical tests that are commonly used for determining whether the binary sequence s possesses some specific characteristics that a truly random sequence would be likely to exhibit. It is emphasized that the outcome of each test is not definite, but rather probabilistic. If a sequence passes all four tests, there is no guarantee that it was indeed produced by a random bit generator [10]. These tests are:

- Frequency test (Monobit test).
- Serial test.
- Poker test.
- Run test.

For a significance level of α = 0.05, the threshold values for freq., serial, poker, and run tests are 3.8415, 5.9915, 14.0671, and 9.4877 respectively [10]. Our tests results are given in figure 3.

Statistical tests of Text Data:

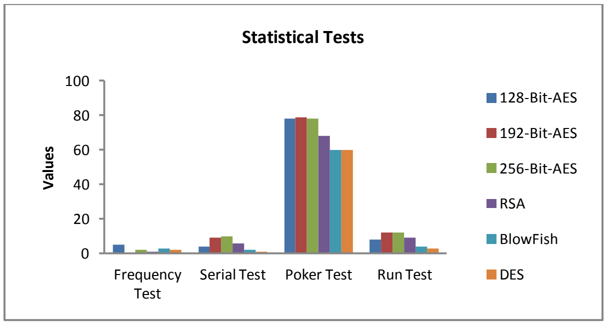

Fig 3: Tests values

Processing time of Text Data:

The processing time in seconds required to encrypt and decrypt text data using different encryption algorithms is given in figures 4, 5.

Text Data encryption time:

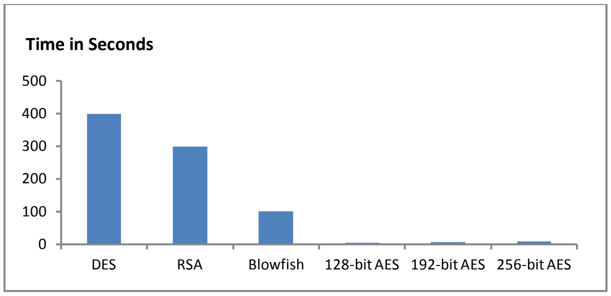

Fig 4: The encryption time for text in seconds

Text Data decryption time:

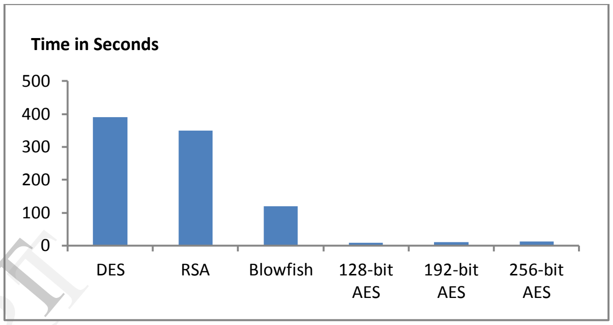

Fig 5: The decryption time for text in seconds

2-Image:

First, when the image is corrupted with noise, we must decrease this noise before the encryption process. This is an example showing the cameraman image corrupted with salt & pepper noise which we first process to decrease this noise and then perform encryption. Figure 6 shows the corrupted image and figure 7 shows the image after noise decrement and encryption then decryption processes.

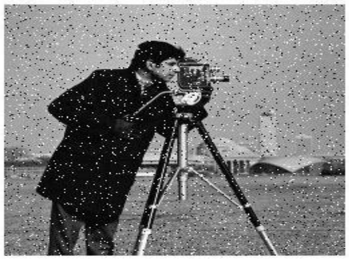

Fig 6: The corrupted image

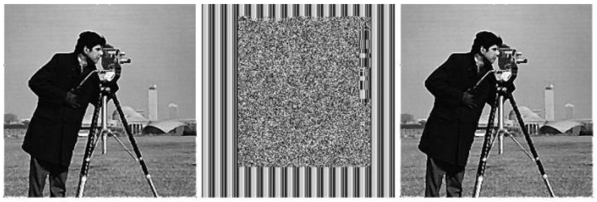

Fig 7: The processed, encrypted, and decrypted image respectively

The biomedical image must be clear from any noise, this is because the doctor depend on it to make the diagnose, figures 8, 9, and 10 are examples on applying AES encryption algorithms on an X-ray. The resulted encrypted and decrypted images are shown in figures 8, 9, and 10.

128-bits AES:

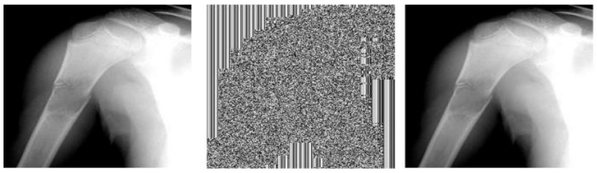

Fig 8: Original, encrypted, and decrypted image respectively

192-bits AES:

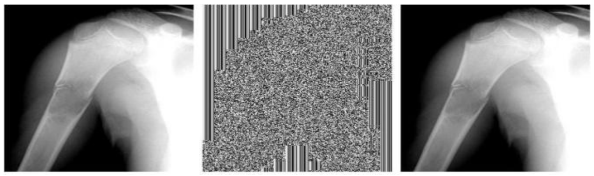

Fig 9: Original, encrypted, and decrypted image respectively

256-bits AES:

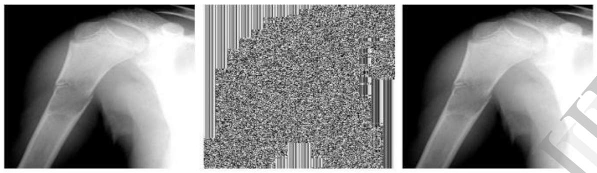

Fig 10: Original, encrypted, and decrypted image respectively

Processing time of Image:

The image size is often larger than text. As in text, the results show the superiority of 128-bits AES over the 192-bits AES and 256-bits AES in terms of the encryption time.

For text and image, when we are talking about data security, the 256-bits AES algorithm is more secure than the 128 and 192-bits AES, RSA, Blowfish, and DES algorithms. So when our consideration is in a more secure data no matter how much time does it take, we then use the 256-bits AES algorithm.

5. CONCLUSION

In this paper, AES algorithm for disguising has been introduced. Such algorithm is a powerful and provides a good security. In addition, the encryption of text and biomedical images using 128, 192, and 256-bits AES algorithms has been presented. Security levels of AES, DES, RSA, and Blowfish algorithms have been examined. We have noted that AES more security and fast compared to the other algorithms. Moreover, the results proved that the 256-bits AES algorithm is highly secure but the 128-bits AES algorithm is faster so depending on applications.

REFERENCES

[1] Christophe RITZENTHALER, "Cryptology course", 2nd Semester 2006.

[2] Hans Delfs, Helmut Knebl, "Introduction to Cryptography: Principles and Applications", Second Edition, ISBN: 9783540492436, 2007.

[3] Richard A. Mollin, "An Introduction to Cryptography", Second Edition, ISBN: 1584886188 / 9781584886181, 2005.

[4] Andreas Uhl, Andreas Pommer, "Image and Video Encryption from Digital Rights Management to Secured Personal Communication", ISBN: 0387234039 / 0387234020, 2005.

[5] Borko Furht, Edin Muharemagic, Daniel Socek, "Multimedia Encryption and Watermarking", ISBN: 0387244255 / 9780387244259, 2005.

[6] Christof Paar, Jan Pelzl, "Understanding Cryptography", ISBN: 9783642041006, 2010.

[7] Avi Kak, "AES: The Advanced Encryption Standard, Lecture Notes on "Computer and Network Security"", February, 2013.

[8] T. Vaughan, "Multimedia Making it work", 8th Edition, ISBN: 9780071748469 / 0071748466, 2011.

[9] Alasdair McAndrew, "An Introduction to Digital Image Processing with Matlab", 2004.

[10] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Hand Book of Applied Cryptography", 1997.

Biography

Ali Taki El-Deen *received the PhD degree in Electronics and Communications Engineering in "Encryption and Data Security in Digital Communication Systems". He has a lot of publications in various international journals and conferences. His current research interests are in multimedia processing, wireless communication systems, and Field Programmable Gate Array (FPGA) applications.*

Salma M. Seif *received BSc in Electronics and Communications, Master student.*