TIME EVALUATION OF DIFFERENT CRYPTOGRAPHY ALGORITHMS USING LABVIEW

Israa Hashim Latif

Department of Laser and Optoelectronics Engineering, AL-Nahrain University, Baghdad, Iraq

Abstract A new LabVIEW simulation design was applied to provide a comparison study among several types of the most common symmetric and asymmetric encryption algorithms. Also, the comparison with advanced encryption package program was made. The results showed that the new LabVIEW simulation design had advantages in several points, where the evaluated time required for the encryption and decryption processes will be lesser than it values using advanced encryption package program.

In this work, the symmetric encryption algorithms were used: AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard) and RC2 (Rivest Cipher) algorithms, while the asymmetric encryption algorithm used was the RSA (Rivest-Shamir-Aldeman) algorithm. The comparison had been achieved using different sizes of text files with different key sizes. The final results proved that the LabVIEW simulation design is better than the Advanced Encryption Package because it increased the algorithm’s performance by 65% in terms of speed and throughput, and for the algorithms’ comparison, the final results showed the effectiveness of AES algorithm over the other algorithms in terms of speed and throughput for the encryption and decryption processes.

Keywords:

Encryption process, Decryption process, AES, DES, 3DES, RC2, RSA, LabVIEW.

1. INTRODUCTION

Cryptography is known as the combination of mathematics with security engineering, it is the way to transfer special information with communication paths in the presence of adversary outsider attackers. It gives us the tools that are behind the most protocols of modern security. It is the most suitable technique of key enabling for protecting different systems [1], which converts the original plain text to a cipher text (the encryption operation) and restoring the main text from cipher text (the decryption operation) [2]. Consequently, the original form of files will be difficult to be unless knowing the key that is used in the process of encryption. Various kinds of encryption algorithms can be found with various properties [4].

Cryptography relies on two keynote components: an algorithm (the technique of cryptographic) and an algorithm’s key. The algorithm is a numerical sequence, and the key is a factor that used for transformation of data [3]. The main aim of cryptography is to provide different concepts of security such as confidentiality, data integrity, authentication, authorization and non-repudiation [2].

In Cryptography, there are two types of encryption algorithms: symmetric (secret) key algorithms and asymmetric (public) key algorithms. In the symmetric algorithms, only one key is used for both encryption and decryption operations, such as DES, 3DES, CAST-128, BLOWFISH, IDEA, AES, RC2 and RC6. And for asymmetric algorithms (public-key algorithms) we use two keys because the encryption process has its own key (public key), and the decryption process has also its own key (private key), such as DH, SSL, DSA, SSH, and RSA. For both types, the keys can be generated from indiscriminate number generators. The cryptographic keys must be found between the sender and the receiver either manually or using entrusted third limb key administers [3]. In earlier works, the calculation of execution time for the different encryption algorithms for a text's encryption and decryption operations, many comparisons were made. In [10], a theoretical comparison of symmetric and asymmetric cryptography algorithms (DES, 3DES, BLOWFISH, AES and RSA) were made in terms of performances, weaknesses and strengths, this comparison proved that AES is the fastest than
DES, 3DES and RSA in terms of speed in processing text files. In [11], a comparative analysis was performed of three algorithms; DES, AES and RSA considering certain parameters such as computation time, memory usages and output byte, this theoretical comparison approach proved that DES algorithm needed a lowest encryption time while AES algorithm required a lowest memory usage. In [12], a comparison in performance of six useful symmetric algorithms: DES, 3DES, AES, RC2, RC6 and BLOWFISH were applied and the performance of different algorithms was different according to data loads, and the theoretical comparison proved that the AES algorithm had the better performance over DES and 3DES algorithms in terms of speed and throughput.

Figure 1 shows the Classification of Cryptography.

The Cryptography algorithms which used in this work are:

1.1. Data Encryption Standard (DES)

DES is a symmetric key algorithm, block cipher type. It has a key length of 56 bits and block size of a 64 bit. It is poor and weak to the key attack if it is used a feeble key. DES was established in 1972 by IBM as a data encryption algorithm. The government of USA depended on DES as the criterion of the encryption algorithms. Firstly it had a 64 bit key size, after that, the NSA laid a limitation for using the DES algorithm with a 56-bit key length, for this, DES abjures 8 bits of the 64 bit key and then uses the compacted 56 bit key, which derived from 64 bit key can encrypt data of 64-bit block size. DES can operate in various modes; CBC, CFB, OFB and ECB, which making it so flexible [5].

1.2. Triple Data Encryption Standard (3DES)

3DES is a symmetric key algorithm, block cipher type. It firstly found in 1998 and named 3DES because it achieves DES cipher three times to every data block in encryption – decryption – encryption operations using DES. The key length is either 112 bits or 168 bits, while the block size is 64 bit. The reason of the increasing computational power available now days make a weakness to the original DES cipher, in order to avoid force attacks and various cryptanalytic attacks; 3DES was designed to provide a comparatively simple process of increasing the key size of DES to be safe against like these attacks, without designing a completely new block cipher algorithm [5].

1.3. Rivest Cipher (RC2)

RC2 is a symmetric key algorithm, block cipher type. It firstly developed by Ron Rivest in 1987, has a data block of 64-bit block and a key size from 40 bits to 128-bits (an increment step of 8 bits). The 40-bit key a small key size and very weak but is favored by the governments for export purposes. With this state, the key is created from a Key and an IV (Initialization Vector). The Key has 12 characters (96 bits), and the IV has 8 characters (64 bits), which create the synoptic key [6].

1.4. Rivest, Shamir &Adelman (RSA)

RSA is an asymmetric key algorithm, block cipher type. It was published in 1977 and named according to its founders Rivest, Shamir &Adelman. It had two keys: a public key for encryption process and a private key to decryption operation. The RSA algorithm includes three steps; first step is the key
generation, which is the key that used to encrypt and decrypt messages and data. The second step is the encryption step, which is a conversion process from plain text to a cipher text. And the third step is decryption step, where the encrypted text is converted into plain text at another side. RSA has a key size is from 1024 to 4096 bits, which is created by a product of two large prime numbers. [7].

1.5. Advanced Encryption Standard (AES)

AES is a symmetric key algorithm, block cipher type. It developed in 1998 by Joan Daemen and Vincent Rijmen. AES algorithm can apply any blend of data, and it has key length of 128, 192, and 256 bits. AES can encrypt a data block of 128 bit length which can be split into four main operational blocks. These blocks are deemed as array of bytes and indited as a matrix of the order of 4×4 (also called as state and subject to rounds where different transformations are applied). For full encryption operation, the number of rounds used is changed depending on key length, i.e., the number (N)=10, 12, 14 for key length of 128,192 and 256 respectively. Every round of AES uses permutation and substitution network, which is appropriate for both hardware and software applications [8].

2. RESEARCH METHODS

Many different text files in size were applied to the symmetric and asymmetric cryptography algorithms (DES, 3DES, RC2, AES and RSA) using LabVIEW 2016 toolkit and advanced encryption package 2017 programs. Each tool is applied to an algorithm to calculate the execution time, file memory size and the algorithm's throughput for different text files in size.

2.1 The Cryptography Algorithm’s Design in LabVIEW 2016

The LabVIEW (Laboratory Virtual Instrumentation Engineering Workbench) Simulation system is designed to calculate the execution time for each algorithm to encrypt many experimental text files. Each Simulation system design had two main windows: the front panel window and the block diagram window [9], as shown in figure 2 (a, b, c, d and e).

Figure 2a. The front panel and block diagram of LabVIEW 2016 simulation design for DES algorithm

Figure 2b. The front panel and block diagram of LabVIEW simulation design for 3DES algorithm
From figure 2, it is noticed in each front panel window, there are eight fields of data:

1) The Path field: This field was used to import a certain text file.
2) The Execution Time field: it is an unsigned long (32-bit integer) icon, which was used to display the total execution time of the encryption and decryption processes in milliseconds.
3) The File Size field: This field is a (64-bit integer) icon, which is used to display the size of file in Bytes.
4) The Imported Text File Field: it is a string icon, which is used to display the contents of the imported text file.
5) The Encrypted Text: it is a string icon, which is used to display the encrypted text file.
6) The Decrypted Text: it is a string icon, which is used to display the decrypted text file.
7) The Algorithm’s Password: it is a string icon, which is used to display the password (Key) for the algorithm.
8) The Key Size: it is an unsigned word (16-bit integer) icon, which was used to display the key size according to the algorithm’s type and mode.

While each block diagram window in figure 2 consists of five parts:
1) The first part is the execution time’s calculation part of each algorithm, which evaluated time value the encryption and decryption processes. This part consists of Starting Tick count (ms), Ending Tick count (ms) and the flat sequence structure.
2) The second part described the technique and steps to import, read and get size of the imported text file.
3) The third part showed the algorithm key and key size.
4) The fourth part included the two vi icons of an algorithm; first vi icon evaluated the encryption process and second one evaluated the decryption process.
5) The fifth part described the output decrypted text.

2.2 The Cryptography Algorithm’s Calculations using Advanced Encryption Package 2107

The AEP 2017 (Advanced Encryption Package) is the file encryption software Compatible with Windows 7/Vista/XP with the ability to encrypt file using 20 encryption algorithms. AEP Pro gave lots of options for the type of algorithm and keys. Figure 3 shows the Advanced Encryption Package 2017 program window, which consists of many fields, the important fields are:
1) A field to choose the file to be encrypted.
2) A field to choose the encryption algorithm type.
3) A field to enter and confirm a password for the encryption algorithm.
4) An ENCRYPT NOW field to run the encryption process.
5) A field to apply the speed of the encryption process.

Figure 3. Text files’ encryption using advanced encryption package 2107 program
2.3 RESULTS AND DISCUSSION

A. LabVIEW 2016 Simulation Design

The six text files (915kB, 5.384 MB, 11.804 MB, 35.350 MB, 59.809MB and 106 MB) were used to achieve six experimental results, in each experiment, five cryptography algorithms (AES-256, DES-56, 3DES-168, RC2-128 and RSA- 2048) were used.

The Performance of each algorithm was evaluated in terms of speed, memory file size and throughput using LabVIEW 2016 Simulation Program. The encryption time of any cryptography algorithm is the time for the encryption algorithm, which takes to convert a plain text to a cipher text. The encryption time is used to calculate the throughput of any process of encryption, which is calculated as the total encrypted plaintext (in bytes) divided by the encryption time (in ms). The LabVIEW 2016 simulation design results are shown in table 1 and figure 4.

Table 1. The Time Evaluation of different cryptography algorithms using different text files by LabVIEW

| The Text File Size in Bytes | AES (256-bit) | DES (56-bit) | 3DES (128-bit) | RC2 (128-bit) | RSA (2048-bit) |
|----------------------------|---------------|--------------|----------------|---------------|----------------|
| Text File1 (915 kB)        | 2050          | 2133         | 2235           | 2064          | 4915           |
| Text File2 (5.384 MB)      | 3606          | 3255         | 3094           | 3867          | 7805           |
| Text File3 (11.804 MB)     | 4882          | 6481         | 7062           | 7847          | 15440          |
| Text File4 (35.350 MB)     | 13371         | 16735        | 18337          | 21505         | 39107          |
| Text File5 (59.809 MB)     | 25038         | 32411        | 38483          | 39958         | 65527          |
| Text File6 (106 MB)        | 51249         | 65721        | 78041          | 83432         | 109237         |

Figure 4: Time evaluation of different cryptography algorithms by using LabVIEW 2016

Figure 4 and table 1, showed the superiority of AES over other algorithms in terms of processing time. DES is the better one after AES because it consumes less evaluated time than other algorithms. 3DES and RC2 approximately consume the same time values during the encryption and decryption processes while RSA is the slowest one. The throughput of any cryptographic algorithm indicates the algorithm’s speed during encryption and decryption processes,

\[
\text{Throughput} = \frac{\text{Total Text files size in (MB)}}{\text{Total Evaluation Time of Algorithm in (ms)}}
\]
As the cryptographic technique’s throughput value is increased, the power consumption of that technique will be decreased depending on the decreased time during encryption and decryption processes.

Figure 5 and table 2, showed the throughput of each algorithm evaluating same text files, AES had the larger throughput; it can encrypt more than 13 MB in one second, the second better algorithm is DES; it can encrypt more than 10 MB in one second, while 3DES and RC2 approximately encrypted the same range of data, about 8MB, in one second. Finally, RSA algorithm had the lowest performance among other algorithms; it encrypted about 5MB in one second.

Table 2. The total average time evaluation and throughput of different cryptography algorithms using different text files and LabVIEW 2016

| The Total Average Time and Throughput | The Algorithms |
|--------------------------------------|----------------|
| AES (256-bit) | DES (56-bit) | 3DES (168-bit) | RC2 (128-bit) | RSA (2048-bit) |
| Total Average Time | 16699.33 | 21122.67 | 24542 | 26445.5 | 40338.5 |
| Throughput (MByte/sec) | 13.12999 | 10.38041 | 8.934154 | 8.291089 | 5.435552 |

Figure 5. The throughput of the cryptographic algorithms by using LabVIEW 2016

B. Advanced Encryption Package 2107

The same six text files (915kB, 5.384 MB, 11.804 MB, 35.350 MB, 59.809MB and 106 MB) were used again to achieve six experimental results by using Advanced Encryption Package 2107, as shown in figure 6, in each experiment, also five cryptography algorithms (AES-256, DES-56, 3DES-168, RC2-128 and RSA- 2048) were used. The obtained results are shown in table 3.

Table 3. The time evaluation of different cryptography algorithms using different text files by using advanced encryption package 2017

| The Text File Size in Bytes | AES (256-bit) | DES (56-bit) | 3DES (168-bit) | RC2 (128-bit) | RSA (2048-bit) |
|----------------------------|---------------|--------------|----------------|---------------|----------------|
| Text File1 (915 kB)        | 2122          | 2355         | 2518           | 2593          | 5209           |
| Text File2 (5.384 MB)      | 3970          | 4832         | 5707           | 5738          | 7623           |
| Text File3 (11.804 MB)     | 7986          | 8394         | 8984           | 9426          | 17327          |
| Text File4 (35.350 MB)     | 24475         | 25179        | 29559          | 30689         | 42322          |
| Text File5 (59.809MB)      | 42014         | 45271        | 49049          | 49762         | 77320          |
| Text File6 (106 MB)        | 71864         | 80769        | 82677          | 84667         | 110177         |
From figure 7 and table 4, it is clear that the AES is the fastest algorithm in the encryption and decryption processes over other algorithms in terms of processing time. DES had the second level of performance after AES because it consumes less evaluated time than other algorithms. 3DES and RC2 approximately consumed the same time values during the encryption and decryption processes while RSA again the slowest one. As shown in figure 7 and table 4, AES had the better throughput than other algorithms.

**Table 4.** The Total Average Time Evaluation and Throughput of different Cryptography algorithms using different text files using advanced encryption package 2017

| The Total Average Time and Throughput | AES (256-bit) | DES (56-bit) | 3DES (168-bit) | RC2 (128-bit) | RSA (2048-bit) |
|---------------------------------------|---------------|--------------|----------------|---------------|----------------|
| Total Average Time                    | 152431        | 166800       | 178494         | 182875        | 259978         |
| Throughput(MByte/sec)                | 8.630882      | 7.887374     | 7.370634       | 7.194062      | 5.060482       |
2.4 CONCLUSION

This work presents a very good performance evaluation of using the LabVIEW 2016 program as a simulation design system to perform two effective comparison methods, as explained below:

The first comparison is made between the two evaluation methods: The LabVIEW 2016 simulation design program and advanced encryption package 2017 program. The LabVIEW 2016 simulation design provides a simple approach to calculate the values of encryption and decryption times for the chosen cryptographic algorithms (AES, DES, 3DES, RC2 and RSA). It had many advantages over the advanced encryption package 2017 program in both of the total time required to complete the encryption and decryption processes, and in calculating the evaluated time of a cryptographic algorithm during encryption and decryption processes, because it consumed lesser time, besides, the time of encryption and decryption processes can be achieved with an one run command, while in advanced encryption package 2017 program, it must apply two runs commands, one for encryption process and the other for decryption process.

In LabVIEW 2016 simulation design, the front panel window provided the full information about encryption and decryption processes including the value of execution time, original text file, the resulted encrypted text file, the resulted decrypted text file, the algorithm’s key and its size. This facility is not found in advanced encryption package 2017 program.

Finally, In LabVIEW 2016 simulation design, we get all the possible key’s values for any algorithm and this facility can achieve all the experimental statuses, while the advanced encryption package 2017 program gave only limited keys’ sizes for each algorithm.

The second compassion is among the five encryption algorithms. From the simulation results of LabVIEW 2016 program and the obtained results of advanced encryption package 2017 program, both, showed that the AES is the fastest encryption technique among the others in terms of speed and throughput and the lowest one in terms of power consumption, i.e. we can get a higher efficiency with lower time in spite of the design complexity of AES-256, because it can encrypt a 128-bit block cipher (which is the biggest block cipher for cryptographic algorithms) in 14 rounds only. DES had the second better performance during encryption and decryption processes, while 3DES and RC2 the same performance level. Finally, RSA had the lowest performance level in terms of speed and throughput.

REFERENCES

[1] Stallings W 2017 Cryptography and Network Security 7th Ed, (Prentice Hall) 58-309
[2] William S 2017 Cryptography and network security principles and practice 7th Ed (Prentice-Hall Inc) 23-50
[3] Hercigonja Z 2016 Comparative Analysis of Cryptographic Algorithms (Croatia: International Journal of Digital Technology & Economy 1 127-34
[4] Al-Nbhan W, A N A and Zahary A T 2016 A Comparative Study among Cryptographic Algorithms: Blowfish, AES and RSA (Morocco: International Arab Conference on Information Technology (ACIT2016) Beni Mellal)
[5] Tripathi R and Agrawal S 2014 “Comparative Study of Symmetric and Asymmetric Cryptography Techniques (International Journal of Advance Foundation and Research in Computer (IJAFRC)) 1 68-76
[6] William J and Buchanan 2011 Rc2 encryption in .net http://buchananweb.co.uk/
[7] Chalurkari S N, khochare N and Mashram B B 2011 Survey on Modular Attack on RSA Algorithm (International Journal of Computational Engineering & Management 14 106
[8] Pahal R and Kumar V 2013 Efficient Implementation of AES (International Journal of Advanced Research in Computer Science and Software Engineering 13 290-95
[9] Hans-Petter Halvorsen 2016 LabVIEW MathScript 2013 Lectures
[10] Wahid M N A et al 2018 A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention (Journal of Computer Science Applications and Information Technology 3 1-7)

[11] Seth S M Mishra R 2011 Comparative Analysis of Encryption Algorithms for Data Communication (International Journal of Computer Science and Technology 2 292-94)

[12] Mathur M. Kesarwani 2013 A Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES (Proceedings of National Conference on New Horizons in IT – NCNHIT) 143-47