International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2000-000X
Vol. 2 Issue 11, November – 2018, Pages: 32-38

Enhancing Performance of Advanced Encryption Standard for Data Security

Omar G. Abood[1], Shawkat K. Guirguis[2]

Department of Information Technology, Institute of Graduate Studies and Researches,
Alexandria University, Egypt
e-mail:omar.ghazi88@yahoo.com[1], shawkat_g@yahoo.com[2]

Abstract:: *Information technology has been part and parcel of the contemporary world. Data transmission is considered to be a significant pillar for it. In processing the data, data transmission has improved dramatically. It improved to complex system, where one can find advantages and disadvantages. In fact, these disadvantages are concerning the confidentiality of the data. It became a subject of debate recently. The matter that argued for a several encryption algorithms to secure crucial data against hacking. The target of this research is to tackle Advanced Encryption Standard (AES), comparing and contrasting it with prominent valid algorithms to enhance security range. With the aim to minimize processing time, it takes five rounds instead of ten, concurrently, preserving the maximum security. The comparison is in terms of efficiency, key size, complexity and time consumed. The performance evaluation is by MATLAB R2016b.*

Index Terms— *Cryptography, Encryption, Decryption, Key Size, AES, DES, RSA.*

1. Introduction

Encryption changes the database into a cipher text. The opposite is decryption, it converts a cipher text to an ordinary and readable text. A cipher is a double algorithm, which invents the encoding and decoding processes. The extensive process of a cipher is dominated by an algorithm and a key. The key is secret, it is a brief group of symbols, that would encode and decode the plain and cipher texts respectively, in the case, the key is single. It is called a symmetric algorithm [1]. Data encoding is the process of changing data into certain symbols using secret codes. The process of encoding and decoding, depending on a solo single key, is known as an identical key cryptography. In this process, the same key is used for enciphering and deciphering. A safe channel is also needed between the sender and the receiver to commute the secret key. Symmetric algorithm is vital for both, block and streams ciphers. Stable shape is handled by a bunch of block cipher. It contains many similar rounds for processing. In each round, a substitution is done on one half of the information tackled, followed by a permutation that intermingles with the 2 halves. The basic key becomes larger, so the multiple keys are used for every round. A symmetric key cryptography refers to a cryptographic algorithm that need 2 different keys. The first is invisible while the other is public. The public key is used to encode a plain text, while the private key is used to decode cipher text. Symmetric enciphering strategies are approximately slower than symmetric encoding thousand times, which makes it unfeasible in encoding much of information [2]. Therefore, plenty of researches were introduced to enhance the cryptography process. The category of main encoding techniques is illustrated in Fig. 1. The most used techniques are AES and DES [3][4].

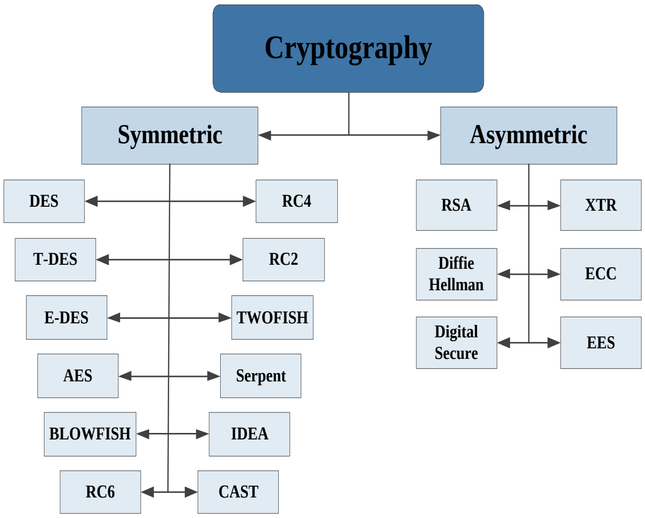

Fig. 1 Classification of Cryptography Algorithms

2. Cryptographic Algorithms encoding

Decrypting is one of two types either symmetrical or asymmetrical. The necessary algorithms are clarified with steps. They include AES and DES. They have to do with bilateral algorithms. In contrast to RSA that is relevant to unilateral algorithm.

A. DES

DES was established at IBM in 1972 by Horst Fiestel. The DES algorithm goal is to offer a strategy to secure crucial financial database [3]. The encoding instructions are as follows:

- DES receives data of 64-bit long ordinary message and 56 bits key and comes up with 64-bit block.
- The ordinary text block needs to modulate the bits.
- The 8 similar bits are eliminated from the key by exposing it to its permutation.
- Both of the visible message and the key will go through these two changes:

1. .The key has 2 sets; each has twenty-eight halves.
2. The half is spun by one or two bits.
3. The two parts reunite and go to the permutation's round to decrease the key from 56 bits to 48 bits. These pressed keys are used to encode the round's plaintext block.
4. The key parts from step 2 are used in the coming round.
5. The database block is divided into two 32-bit parts.
6. A part will be expanded in terms of permutation to raise the size to 48 bits.
7. The result of the sixth step is for OR'ed only, with 48-bit key from the third instruction.
8. The outcome of 7th instruction is a set-box, which replace key bits and decrease the 48-bit block to 32 bits.
9. The consequence of the 8th step, will be permuted by P-box.
10. The result of the OR'ed solely, will be the next part for the format block. The bipartite format parts are exchanged and form reservoir of the coming stage [3]. These steps are clarified in the Fig.2.

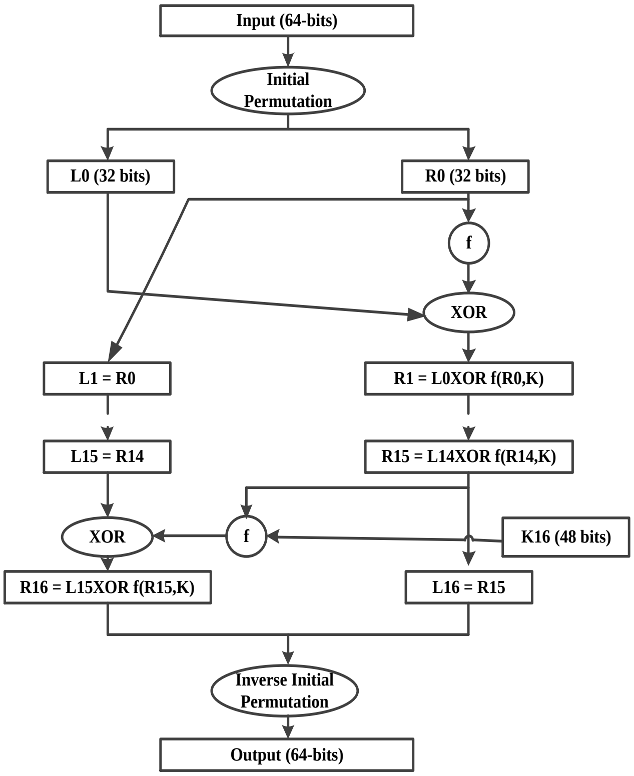

Fig.2 DES Algorithm Flowchart [5]

B. AES

AES is an enciphering strategy, suggested by the National Institute of Standards and Technology (NIST) in 2001 to substitute DES. AES could provide any group of databases [6]. During encryption-decryption, AES process encodes 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds to 256-bit keys to come out with the last encoded-message [7]. AES keeps in 128-bit information length that can be split into 4 fundamental active blocks. Those parts are dealt with as a line of bytes and combine a matrix of 4*4 named “The State”. For encryption and decryption, the cipher starts with an “Add round key stage”. However, and shortly before the eventual round, the output encounters 9 basic rounds, through each, 4 transformations take place; I. Sub-Bytes, II. Shift-Rows. III. Mix-Columns and IV. Add Round Key. In the last tenth round, mix columns transformation is unavailable [8] [9]. The entire operation is figured out in Fig. 3. Decryption is the reverse process. It uses opposite steps [10]:

1. *Sub-byte*

A 128-bit data block is the key for AES, that is to say every database item has 16-bytes. In the transformation of sub-byte, each data byte item is changed by implementing 8-bit substitution box known as Rijndael S-box.

2. *Shift Rows*

This transposition is easy, the bytes in the rest 3 lines of the state, that depend on a row position, are changed into a circle way.

3. *Mix Columns*

This step is a counterpart of duplicated set for every column of the states, whereas a single stable matrix is added to every state column. The bytes in that process are dealt with as multiple names.

4. *Add round key transformation*

A bit-like XOR is between the current state 128-bits and the round key 128-bits, whereas the transmutation is to be reversed.

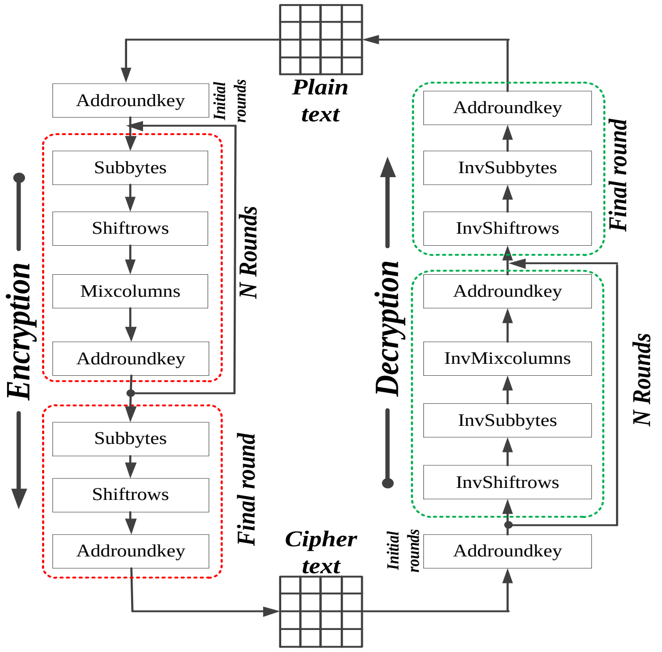

Fig.3 AES algorithm processing [5]

C. RSA

Dated back to 1978, The RSA stands for the first letters of its inventors' names. It is a prominent public key for system encipherment. For key exchange, digital signatures or database block encryptions are required. The algorithm implements different size encoding block and a key size which is variable. It presents an asymmetric encoding system that rely on numeral synthesis. It uses 2 basic numbers to come up with public and private keys. On the other hand, RSA has many faults, that is why it is not feasible for commerce. [13]. Fig. 4 depicts the steps order, following RSA for the cryptography of multiple blocks.

1. The process of Key Generating [14]
   a. Choose two different large random prime numbers such as p ≠ q.
   b. Calculate n = p × q.
   c. Compute phi (n) = (p-1) (q-1).
   d. Pick an integer e where 1<e<phi (n)
   e. Compute d to fulfill the relation d × e = 1 mod phi (n); d is kept as private key exponent.
   f. The public key is (n, e) whereas the private key is (n, d), keeping all the values d, p, q and phi secret.
2. Encipherment

   Original text P < n

   Encrypted text C= Pe mod n.
3. Decipherment

Encrypted text C
Original text P=Cd mod n.

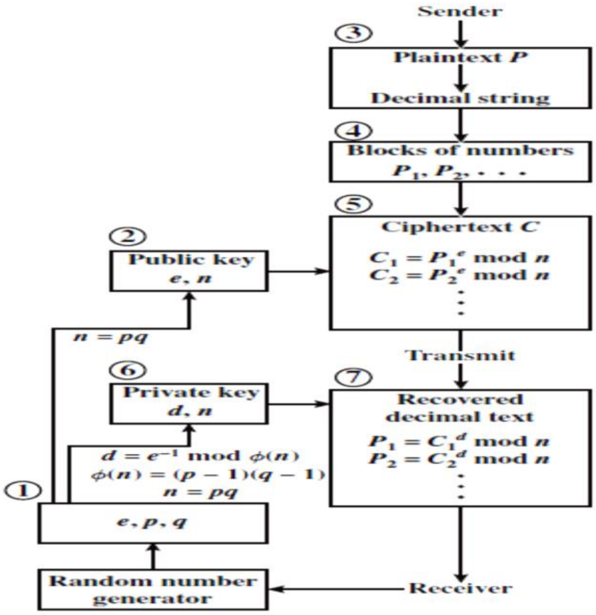

Fig. 4 RSA algorithm processing [5]

3. PROPOSED WORK

The defect in the implementation of the data cryptography algorithms is the encryption and decryption time, because data has a huge amount of information. Besides, vulnerability is another issue for cryptography algorithms to be considered. Thus, cryptography systems must be changed carefully to boost their inaccessibility for strangers. The AES is a block encryption scheme, which has a set of transformations; executed several times (It has been mentioned previously).

AES-128, AES-192, and AES- 256 are the main genres. These keys are exemplified in arrays with sizes 4×4, 4×6, and 4×8, however, 128-bit block data is arranged in the 4×4 array named state. In this paper, the modification was conducted in 5 rounds instead of 10 rounds in the original AES-128, to lower the encrypting and decrypting executing time. Fig. 5 shows the AES encryption algorithm using 5 rounds instead of 10 rounds.

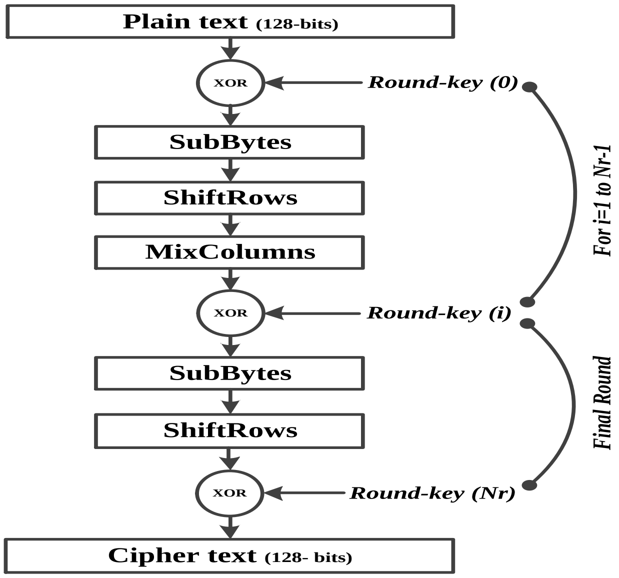

Fig. 5 128-bits AES encryption algorithm.

The pseudo-code for the proposed method:

```
Require: Plain-text [M x N], and key [$N_r$] [4 x 4],
Ensure: Cipher-text [M x N] bytes.
Suppose that the plain-text size is M x N pixels and the state size is [4 x 4] bytes.
for i = 1 step 1 to M / 4 do
    for j = 1 step 1 to N / 4 do
        Add-Round-Key (state [i, j], key [0] [4 x 4]);
        for r = 1 step 1 to $N_r$ - 1 do
            Sub-Bytes (state [i, j]);
            Shift-Rows (state [i, j]);
            Mix-Columns (state [i, j]);
            Add-Round-Key (state [i, j], key [r] [4 x 4]);
        end for
        Sub-Bytes (state [i, j]);
        Shift-Rows (state [i, j]);
        Add-Round-Key (state [i, j], key [r] [4 x 4]);
    end for
end for
for i = 1 step 1 to n=4 do
end for
```

4. COMPARISON OF CRYPTOGRAPHIC ALGORITHMS

Table I offers the comparison between all algorithms previously discussed in this paper with respect to key size, block size, round, structure, flexibility, and features.

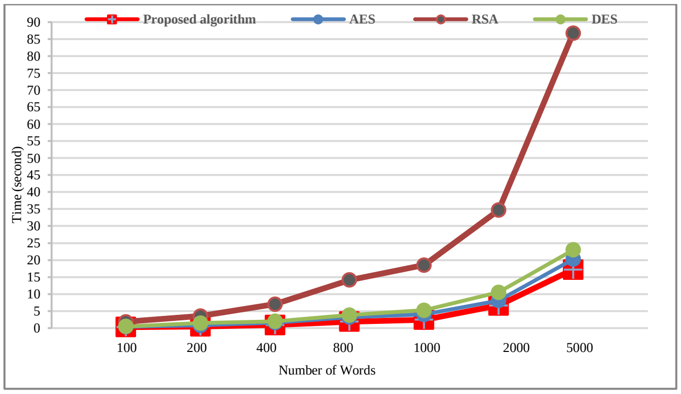

Fig. 6 Encryption execution time of different number of words.

TABLE I: Comparison between all algorithms previously discussed.

Items	Created By	Year	Key Size (bits)	Block Size	Round	Structure	Flexible	Features
DES [15]	IBM	1972	64	64 bits	16	Festial	No	Not Strong Enough
RSA [16]	Rivest Shamir Adlema	1978	1024, 4096	128 bits	1	Public Key Algorithm	No	Excellent Security and Low Speed
AES [7]	Joan Daeman & Incent Rijmen	2001	128,192, 256	128 bits	10, 12, 14	Substitution Permutation	Yes	Security is excellent. It is best in security and Encryption performance

5. RESULT AND DISCUSSION

In this section, selected algorithms are tested via comparison of different cryptographic algorithms such as DES, AES, and RSA, based on throughput for various numbers of words. The tests are conducted using Intel-R, Core-TM i5, CPU 2.40-GHz,128-bit processor with 8 GB of RAM. They could examine security analysis as the following:

A- *Encryption and Decryption Time*

The encrypted time can be defined as, the time consumed by the algorithm for the transformation of plaintext to cipher text. It's time to decrypt. The time can be utilized to compute the encryption throughput of the algorithms.

B- *Time Required for Breakage*

The following amount of time consumed, if a hacker or unauthorized person invents one million secret keys in a second [4]. It could be calculated as follows:

- The length of the master key = Key length.
- Total number of possible keys = Key space (2^n).
- Number of keys generated/second = 10^6.
- Total number of days per year = 365.
- Total number of seconds per day = 86400.

$$Amount\ of\ time\ required\ for\ breakage = \frac{Key\ space(2^n)}{10^6 * 365 * 86400}$$

Table II, and III display the time consumed for encryption and decryption. It is calculated for a message (plaintext) with different numbers of words (100, 200, 400, 800, 1000, 2000, 5000). It is efficient at [17]. The time required for breakage is shown in Table IV.

Figures 6 and 7 illustrate how encryption and decryption execution time depends on the number of words. Finally, a comparison and contrast of different algorithms with the proposed method concluded.

TABLE II: Encryption execution time for different file sizes.

Number of Words	DES	AES	RSA	Proposed algorithm
100	0.4752	0.41271	1.8438	0.28679
200	1.4533	0.81641	3.5367	0.46499
400	1.9881	1.5961	7.0457	0.90507
800	3.8236	3.2224	14.1674	1.8873
1000	5.25435	4.037	18.5096	2.4473
2000	10.50869	8.0976	34.7036	6.6568
5000	22.987143	20.282	86.7242	17.2075

TABLE III: Decryption execution time for different file sizes.

Number of Words	DES	AES	RSA	Proposed algorithm
100	0.471922	0.408306	1.7743	0.360888
200	1.957011	1.16398	3.453	0.689796
400	1.887155	2.33085	7.1067	1.35599
800	3.759431	4.6168	13.8771	2.66754
1000	6.831234	5.0771	18.4126	3.13447
2000	11.0625	10.3325	33.9662	7.36361
5000	29.917032	29.1165	84.3077	23.0176

TABLE IV: Time required to break the symmetric (private key) algorithms.

Algorithm	Key Size (bits)	Average number of years required
DES	64	~ 584942.42
AES	128	~ 1.08 * 10^{25}
	192	~ 1.9905 * 10^{44}
	256	~ 1.87993 * 10^{66}

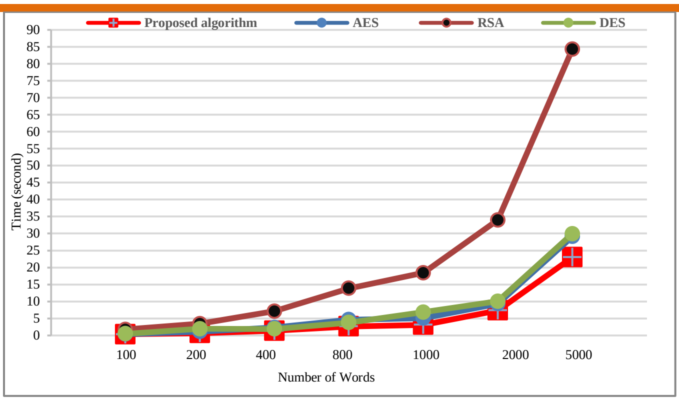

Fig. 7 Decryption execution time of different number of words.

As shown in Tables II, and III, the execution time of the proposed method is decreased to (25-40%).

6. Conclusion and Future Works

This paper has been proposed to modify the AES algorithm. It concentrates on the consumed time for both of encryption and decryption processes, summing up the rounds from 10 to 5 only (10 rounds in old AES). In addition, a comparison of the proposed method with the most well-known cryptography algorithms such as (AES, DES, and RSA) has been done. It is proved that the proposed method is faster in execution time for encryption and decryption, and the symmetric algorithms have the best overall performance than their asymmetric counterparts. Upon the obtained results, it is shown that DES is more competitive than the original AES in encryption and decryption times. Whereas, it requires higher security level. The overall results have proved that the original AES algorithm is the fastest, followed by the DES algorithm, and after that, with big gab comes RSA. In brief, the proposed method is the ultimate one as it managed to guarantee wide scope of security with minimal time consumed, as well as rapid application.

And with an eye on the future, if the previous method works side by side with DNA computing, it would be of great advantage for bunch of reasons in the technological arena.

Reference

[1] Wang, C. Huang, K. Yang, J. Wang, X. Wang, and X. Chen, “MAVP-FE: Multi-authority vector policy functional encryption with efficient encryption and decryption,” China Communications, vol. 12, no. 6, pp. 126–140, Jun. 2015.

[2] S. Kansal and M. Mittal, “Performance evaluation of various symmetric encryption algorithms,” 2014 International Conference on Parallel, Distributed and Grid Computing, Dec. 2014.

[3] R. Yegireddi and R. K. Kumar, “A survey on conventional encryption algorithms of Cryptography,” 2016 International Conference on ICT in Business Industry & Government (ICTBIG), 2016.

[4] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, “CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method,” Multimedia Tools and Applications, vol. 76, no. 6, pp. 8597–8626, Apr. 2016.

[5] Omar G. Abood and Shawkat K. Guirguis, “A Survey on Cryptography Algorithms”, International Journal of Scientific and Research Publications, Vol 7, No 8, pp. 495-516, July 2018.

[6] G. Singh and S. Supriya, “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security,” International Journal of Computer Applications, vol. 67, no. 19, pp. 33–38, Apr. 2013.

[7] FIPS, PUB. “197, Advanced Encryption Standard (AES),” National Institute of Standards and Technology, U.S. Department of Commerce, November 2001.

[8] Stallings, William. “Cryptography and network security: principles and practice,” Upper Saddle River, NJ: Pearson, 2017.

[9] Zilhaz Jalal Chowdhury, Davar Pishva and G. G. D. Nishantha, "AES and Confidentiality from the inside out," 2010 The 12th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, pp. 1587-1591, Apr. 2010.

[10] Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, “Performance Evaluation of Cryptographic Algorithms: DES and AES”, IEEE Students’ Conference on Electrical, Electronics and Computer Science, pp. 1-5, Apr. 2012.

[11] Xin Zhou and Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", the 6th International Forum on Strategic Technology, pp. 1118 – 1121, Sep. 2011.

[12] U. Somani, K. Lakhani, and M. Mundra, “Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing,” 2010 First International Conference on Parallel, Distributed and Grid Computing (PDGC 2010), Oct. 2010.

[13] Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma, “Secure and robust digital image watermarking scheme using logistic and RSA encryption,” Expert Systems with Applications, vol. 97, pp. 95–105, May 2018.

[14] S. N. Gowda, “Using Blowfish encryption to enhance security feature of an image,” 2016 6th International Conference on Information Communication and Management (ICICM), Oct. 2016.

[15] W. Diffie and M. E. Hellman, “Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard,” in Computer, vol. 10, no. 6, pp. 74-84, June 1977.

[16] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120-126, Feb. 1978.

https://www.sample-videos.com/sample-text.php. (Last accessed: 2/7/2018