Available Online at www.ijcsmc.com/journal

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 11, Issue. 11, November 2022, pg.13 – 30

Improving Standard Methods of Message Cryptography

Prof. Ziad Alqadi
Albalqa Applied University, Faculty of Engineering Technology, Jordan Amman
DOI: https://doi.org/10.47760/ijcsmc.2022.v11i11.003

Abstract: Protecting secret messages from being hacked is a vital issue. In this paper research some standard symmetric and asymmetric methods of data cryptography will be studied and a comparative analysis of these methods will be provided. A simple, highly secure and efficient method of secret messages cryptography will be introduced; the method will use a character private key with variable length. Increasing the PK length will increase the key space making the method capable to resist any attack, the produced decrypted message will be very sensitive to the PK, any changes in the PK during the decryption phase will be considered as a hacking attempt by producing a damaged decrypted message. The proposed method will be implemented using various messages; the obtained results will be analyzed to prove the quality, security and efficiency achievements provided by the proposed method.

Keywords: Cryptography, PK, TP, MSE, PSNR, CC, NSCR.

Abbreviations

The following abbreviations will be used in this research paper:

PK: private key
ET: encryption time
DT: decryption time
TP: throughput
SM: secret message
MSE: mean square error
PSNR: peak signal to noise ratio
CC: correlation coefficient
NSCR: number of samples change ratio

Introduction

Messages may be private or secret, thus they require a high level of protection when using unsecure communication environment [22-26]. One of the most popular techniques to protect the secret messages is data cryptography, which means encrypting the message before sending it and decrypting the message after receiving it. Cryptography may be symmetric or asymmetric. Symmetric encryption involves the use of one secret private key (as shown in figure 1) for both encryption and decryption phases. The plaintext is read into an encryption algorithm along with a PK. The key works with the algorithm to turn the plaintext into ciphertext, thus encrypting the original sensitive data. This works well for data that is being stored and needs to be decrypted at a later date. The use of just one key for both encryption and decryption reveals an issue, as the compromise of the key would lead to a compromise of any data the key has encrypted [27-32]. This also does not work for data-in-motion, which is where asymmetric encryption comes in.

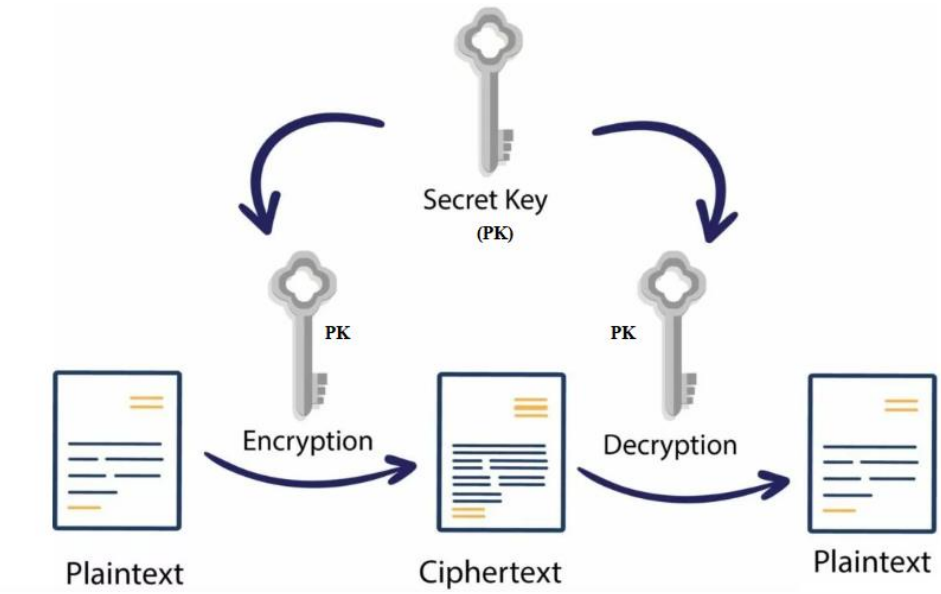

Figure 1: Symmetric data cryptography

Asymmetric encryption works with a pair of keys. The beginning of asymmetric encryption involves the creation of a pair of keys, one of which is a public key, and the other which is a private key (see figure 2). The public key is accessible by anyone, while the private key must be kept a secret from everyone but the creator of the key. This is because encryption occurs with the public key, while decryption occurs with the private key [11-20]. The recipient of the sensitive data will provide the sender with their public key, which will be used to encrypt the data. This ensures that only the recipient can decrypt the data, with their own private key [1-10].

To secure and protect the secret message, key size is the most important parameter in symmetric and asymmetric cryptography. The key size of symmetric cryptography is less than the asymmetric cryptography which make symmetric cryptography less secure for more sensitive data [33-39].

The encryption/decryption time of asymmetric cryptography is greater than the symmetric cryptography which makes encryption/decryption more complex for a large amount of data [3], [4]. Due to larger key size and greater key generation time of asymmetric cryptography, public key cryptography is used once for key exchange only and further encryption/ decryption is done by symmetric key cryptography [5], [6].

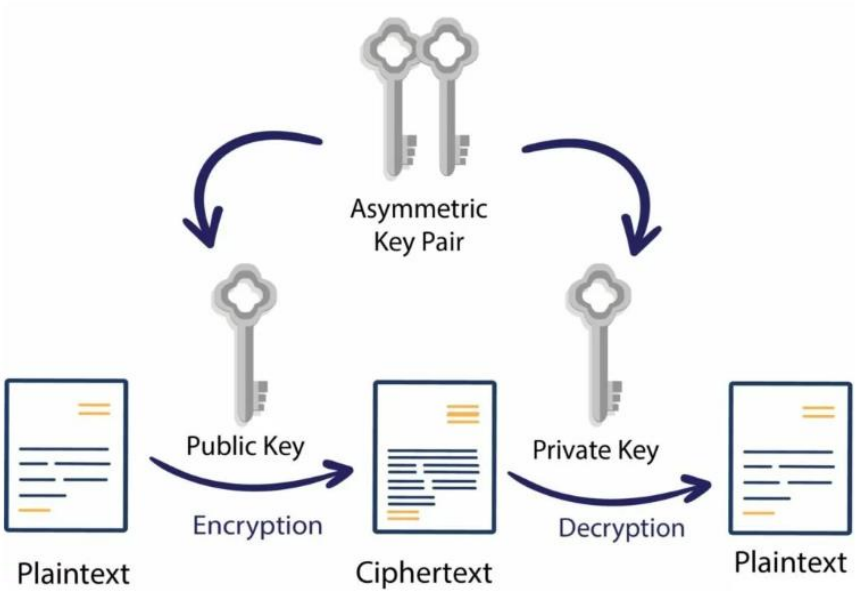

Figure 2: Asymmetric data cryptography

Many standards for message cryptography were introduced, here in this research paper we will focus on the most popular standard, the proposed method will be compared with these standard, below a brief description of these standards will be given:

- DES:

a symmetric cryptographic algorithm used for encryption and decryption of data [10]. In DES, only one secret private key is used for both encryption and decryption. The key size of DES is 56-bit (see figure 3). To encrypt-decrypt the data, the data must be divided into blocks with equal size (64 bits blocks), the encryption/decryption process is to be repeated in 16 rounds, each round performs specific logical and arithmetic operations, the key space provided by DES is small and it cannot resist hacking attacks. Another version of DES is 3DES (see figure 4), which increases the PK length to 168 bits making the process of cryptography more secure, but slowly.

- AES:

AES is the advancement of 3DES algorithm [11]. Basically, AES is based on the Rijndael cipher developed by two cryptographers, Joan Daemon and Vincent Rijmen. AES is different from DES and 3DES due to variables key sizes such as 128,192, and 256 bits [12] (see figure 5). Same like DES and 3DES, AES also performs encryption on blocks which are 128-bit [7]. AES algorithm is used in small devices for encrypting a message to send over a network. Some other applications are monetary transaction [12] and security applications [8] [13].

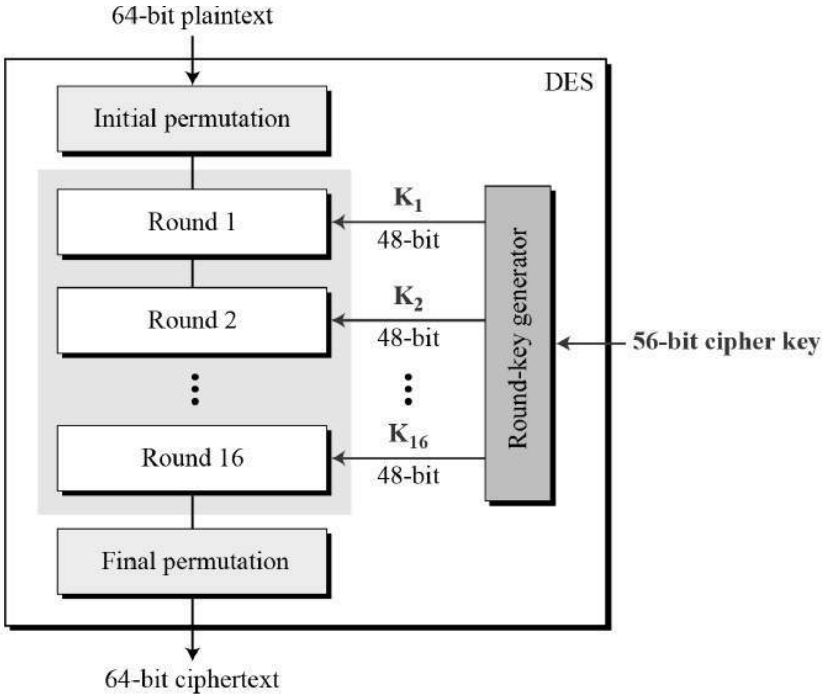

Figure 3: DES procedures

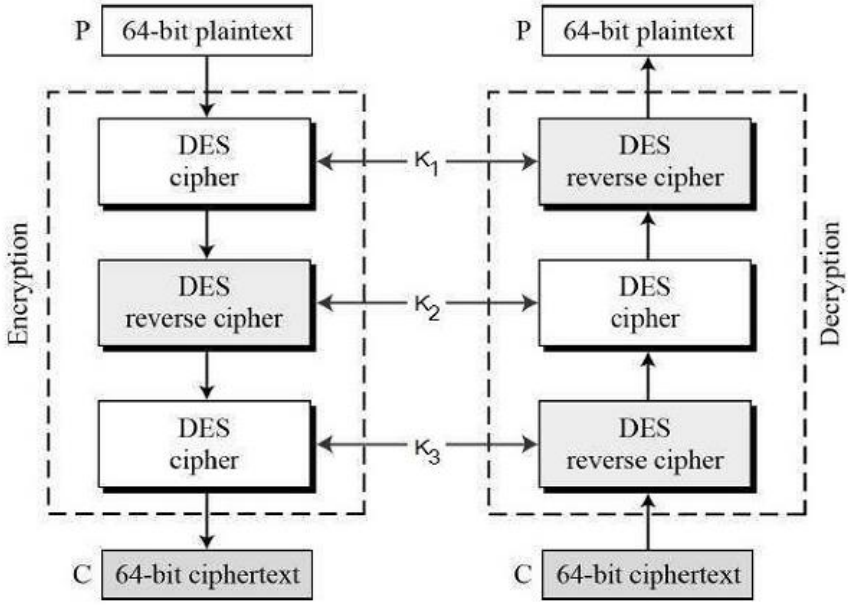

Figure 4: 3DES procedures

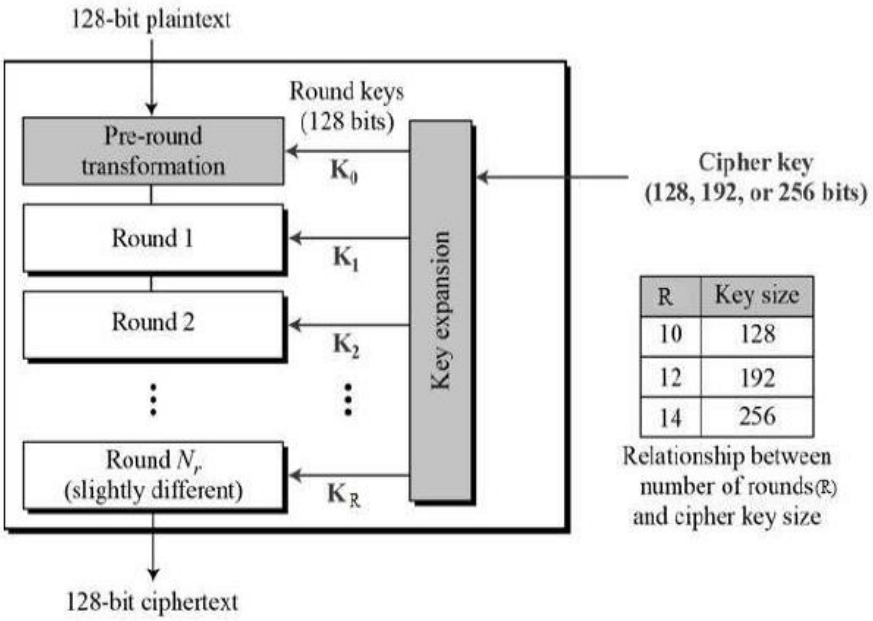

Figure 5: AES procedures

- RSA:

RSA (Rivest, Shamir and Adleman): RSA stands for Rivest, Shamir and Adleman who introduced the RSA algorithm in 1977 [14]. RSA is an asymmetric cryptographic algorithm [1] which is also used for encryption and decryption of the message. RSA (see figure 6) is widely used in transferring of keys over an in secure channel. Due to asymmetric nature, there are two keys used in the algorithm. One is public key and second is a private key. The public key is openly accessible to everyone in the cryptosystem and the private key is kept secret by authorized person. RSA provides confidentiality, integrity, authenticity, and non-repudiation of data [15] [11]. RSA is more commonly used in electronic industry for online money transfer [9]. In future, RSA can be used in Java cards [16]
- ElGamal:

ElGamal algorithm was introduced in 1985by Taher ElGamal [16]. ElGamal is an asymmetric key encryption algorithm that is based on the Diffie-Helmankey exchange as an alternative to RSA for public key encryption. ElGamal is also used in digital signature generation algorithm called ElGamal signature scheme [10] [17]. A homomorphic algorithm named paillier used for its semantic security [2].

- Blowfish:

Designed by Bruce Schneider in 1933, this algorithm uses keys ranging from 32 to 448 bits. Its main purpose was to serve as an alternative to DES [21]. It has the well-known 16 round Feistel Structure (see figure 7), and operates on S-boxes which depend on large keys. It's large key size and range makes the cipher increase its strength and opportunities of use [21].

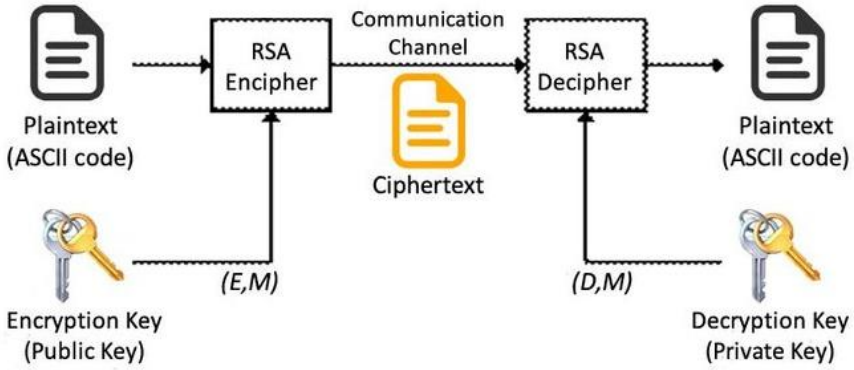

Figure 6: RSA procedures

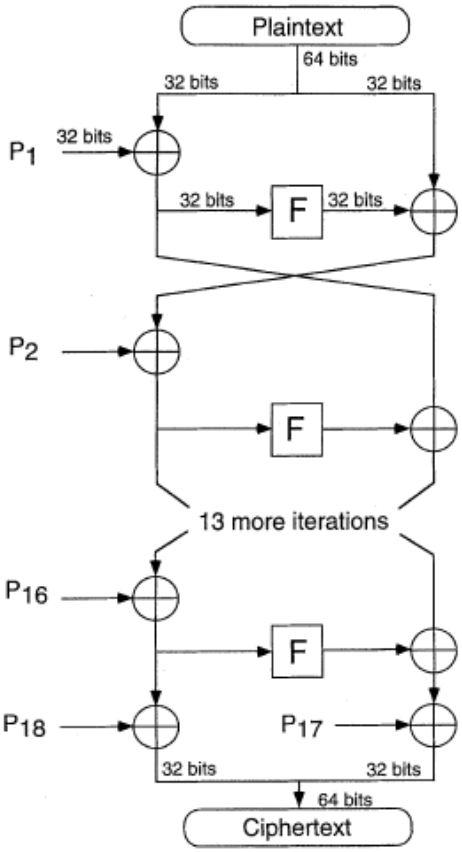

Figure 7: BF procedures

In this paper research a simple and highly secure method of message cryptography will be introduced, the method will use a variable length character PK, the objectives of the proposed method are to satisfy the following [40-45]:

- Provide a low quality encrypted message, and a high quality decrypted message, the proposed method will satisfy the quality requirement shown in table 1.

Table 1: Cryptography quality requirements

Quality parameter	Measured between encrypted and source messages	Measured between decrypted and source messages
MSE	High	0
PSNR	Low	infinite
CC	Low	1
NSCR	High	0

- Increasing the level of security by using a variable long length PK.
- Minimizing the ET/DT and maximizing the throughput of message cryptography.

The Proposed Method

The proposed method uses a PK which contains characters (upper and lower cases characters, numbers and special characters), the key length is variable, this key can suit any SM with any size, the encryption phase can be implemented applying the following steps:

Step 1: Get the SM, and retrieve its length (L)

Step 2: Convert the character SM to decimal

Step 3: Get the PK

Step 4: Convert the PK to decimal

Step 5: Resize the PK length to L

Step 6: Apply XORing the resized key with the SM to get the encrypted SM

Step 7: Convert the encrypted SM to characters.

Figure 8 illustrates an example of message encryption

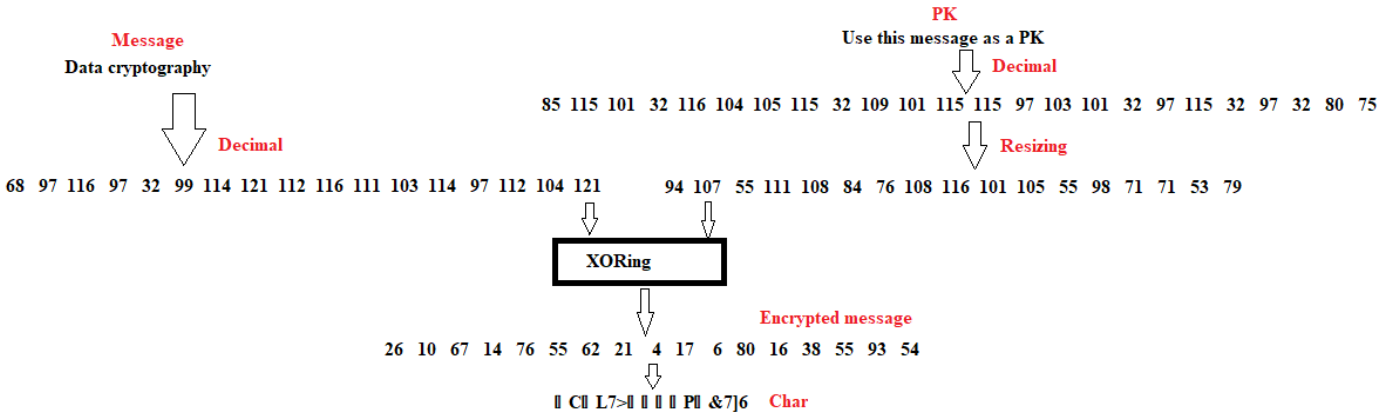

Figure 8: SM encryption example

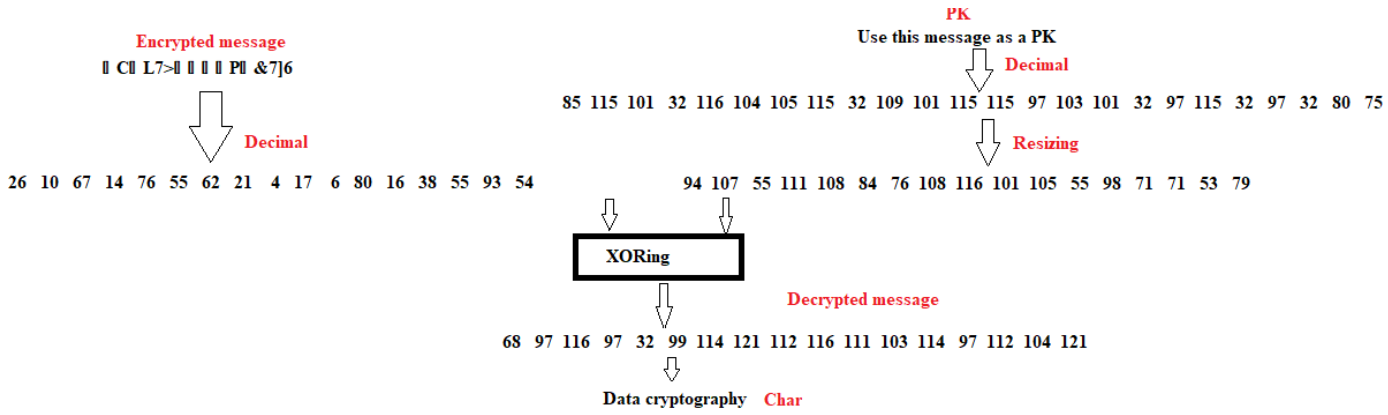

Figure 9: SM decryption example

The decryption phase can be implemented using the same steps using the encrypted SM as source input.

Implementation and Results Analysis

Several messages were implemented using the proposed method, the obtained results were analyzed using various approaches of data analysis methods to prove the enhancement provided by the proposed method, below these approached will be discussed.

Sensitivity Analysis

The generated encrypted and decrypted messages are very sensitive to the selected PK, any changes in the PK in the decryption phase will be considered as a hacking attempt by producing a damaged corrupted decrypted SM, to show this several SMs were encrypted using PK1, the encrypted SMs were decrypted using PK2, table 2 shows the obtained damaged decrypted SMs:

PK1:

'Use this message as a PK'

PK2:

'You cannot crack me!!'

Table 2: Sensitivity analysis

Source SM	Decrypted SM
Secret message cryptography	_}u%□T"cz<~ m0□rtz3M_t Ai&□
Message protection	Lc□]l`=>M\yq2XqRk>
Low quality encrypted message	@gs□w8oewN1!{^6Lwf|65%' Y-b)□
Character private key	CsS□sju!q>%v~t*u□r6□□

Increasing throughput	IuQ□whr-myup p$t□:-□□
Decreasing encryption time	H}v□□qvpV"?z&#zmx$@G wM□#□
Decreasing decryption time	H}v□□qvpV"?{-#zmx$@G wM□#□

From table it was shown that any changes in the PK during the decryption phase will produce a damaged decrypted message, which means that the process of cryptography is very sensitive to the values of the selected PK.

Visual Analysis

Visually we can prove the quality of the proposed method, the encrypted SM must be a damaged and unreadable message, while the decrypted SM must be identical to source SM, to show this the previous messages were encrypted and decrypted using the same PK (PK1), table 3 shows the obtained results, here the encrypted SMs are a corrupted damaged SMs, while the decrypted SMs are identical to the source SMs.

Table 3: Visual analysis

Encrypted SM	Decrypted SM
□□ @#□G□□P□ □L□□□Q#□]M-W:2	Secret message cryptography
□□@□ □SK □□□T□M#Y!	Message protection
□□□f[□□!_N□□□□□□□W\M D+KQ5.	Low quality encrypted message
□□&4□□□O□J□□□□I□6□S&4	Character private key
□□$4□ □C□ U□ □G□4WH69	Increasing throughput
□□□[=□□□9LP□□□□□□E+□!□"J?.	Decreasing encryption time
□□□[=□□□9LP□□□□□□E+□!□"J?.	Decreasing decryption time

Quality Parameters Analysis

The quality between two SMs [39-46] can be measured by the quality parameters MSE, PSNR, CC and NSCR, The MSE and NSCR between the source message and the encrypted one must be high, while the PSNR and CC between them must be low. The MSE and NSCR between the source message and the decrypted one must be zero, while the PSNR must be infinite, and CC must be equal 1.

MSE and PSNR can be calculated using equations 1 and 2:

$$PSNR - 10\ \log_{10}\ \frac{MAX^2}{MSE}\text{dB}, \quad \textbf{(1)}$$

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2, \quad \textbf{(2)}$$

Where: MAX is the maximum possible value of samples values, N is the total number of samples, xi and yi are the corresponding sample values of the source and encrypted/decrypted messages.

The value of CC between two SMs expresses the dependency between their corresponding sample values. This is another statistical evaluation for testing the quality of the algorithm of data cryptography. Calculating correlation coefficient determines the level of correlation between two SMs and the correlation coefficient is always in range [−1, 1]. Values between |1–0.7| is considered as strong correlation (samples from the source files are similar to samples from the encrypted file), correlation between |0.7–0.3| is considered as medium correlation and values between |0.3–0| is considered as weak correlation. Correlation coefficient can be calculated using equation 3:

$$\mathbf{CC}_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad \textbf{(3)}$$

where

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2,$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2,$$

$$cov(x,y) = \sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}),$$

N is the total number of samples, xi and yi are the sample values of two SMs, $\bar{x}$ and $\bar{y}$ are the mean values of samples, and finally cov (x, y) is covariance between both SMs.

Number of sample change rate (NSCR) is robustness test for establishing the quality of data cryptography algorithms. The purpose of the test is to compare the corresponding sample values of two SMs to show the difference in percent. NSCR can be calculated using equation 4.

$$NSCR = \frac{\sum_{i=1}^{N} D_i}{N} \times 100\%, \quad \textbf{(4)}$$

where

$$D_i = \begin{cases} 1, x_i \neq y_i \\ 0, Otherwise \end{cases}$$

The proposed method was implemented using various SMs, the calculated values of MSE between the source SM and the encrypted one was always equal zero, the PSNR was always equal infinite, the CC value was always equal 1, while the NSCR was always equal zero, this prove that the proposed method provided a high quality in the decryption phase, table 4 shows the quality parameters measured between the source SMs and the encrypted ones, the results shown in table 4 prove that the encryption phase provided a low quality SM, thus the provided method satisfied the quality requirements of good cryptography:

The following PK, with length=60 characters where used:

PK: 'Use this message as a PK, this key will protect your message'

Table 4: Quality parameters values between source and encrypted SMs

Message number	Message size (byte)	MSE	PSNR	CC	NSCR
1	10	5761.2	24.1577	0.4475	100
2	50	5051.6	25.1546	0.6577	100
3	100	5142.8	24.5716	0.5068	100
4	200	5706	22.2689	0.5023	100
5	500	6251.6	23.3408	0.8148	100
6	1000	5399.6	22.5582	0.5192	100
7	2500	2350.8	31.0493	0.8074	100
8	5000	5299.6	24.5147	0.8133	100
9	7500	4038	27.7116	0.6637	100
10	10000	5492.4	23.7500	0.5390	100
Remarks		High	Low	Low	High
		Low quality			

Efficiency Analysis

Various in lengths SMs were implemented using the proposed method, ETs/DTs were measured and TPs were calculated, table 5 shows the obtained results:

Table 5: Efficiency results

Message number	Message size (byte)	ET/DT(second)	TP(K bytes per second)
1	10	0.0420	0.2325
2	50	0.0430	1.1355
3	100	0.0420	2.3251
4	200	0.0420	4.6503
5	500	0.0430	11.3554
6	1000	0.0440	22.1946
7	2500	0.0420	58.1287
8	5000	0.0420	116.2574
9	7500	0.0430	170.3307
10	10000	0.0440	221.9460

From the obtained results shown in table 5 it is seen that the proposed method is efficient by providing a good ET/DT and TP. Bigger messages were selected and treated using the proposed method and the standard methods; table 6 shows the obtained ET, while table 7 shows the obtained DT.
Long lengths messages were selected and encrypted-decrypted using the proposed method and the standard methods, table 6 shows the measured ETs, while table 7 shows the measured DTs

Table 6: Obtained ETs

Method	Message size (K bytes)				
	32	126	200	246	280
	Encryption time (seconds)				
DES	0.27	0.83	1.19	1.44	1.67
3DES	0.4644	1.4276	2.0468	2.4768	2.8724
AES	0.15	0.46	0.72	0.95	1.12
BF	0.1091	0.3353	0.4808	0.5818	0.6747

RSA	0.13	0.52	0.74	1.11	1.39
ElGamal	0.45	1.03	1.41	1.75	1.83
Proposed method	0.0584	0.1421	0.1659	0.2108	0.2696

Table 7: Obtained DTs

Method	Message size (K bytes)				
	32	126	200	246	280
	Decryption time (seconds)				
DES	0.44	0.65	0.85	1.23	1.45
3DES	0.7568	1.1180	1.4620	2.1156	2.4940
AES	0.15	0.44	0.63	0.83	1.10
BF	0.1778	0.2626	0.3434	0.4969	0.5858
RSA	0.15	0.43	0.66	0.93	1.23
ElGamal	0.43	0.85	1.13	1.30	1.64
Proposed method	0.0584	0.1421	0.1659	0.2108	0.2696

From tables 6 and 7 it is seen that the proposed method decreased both the ET and DT, this is also clear shown in figures 10 and 11.

The proposed method provided a better throughput (message length/ET) as shown in table 8.

The proposed method is more efficient and it provides a significant speedup comparing with the standard method of message cryptography:

Speedup_12=ET_2/ET_1

TP_1/TP_2

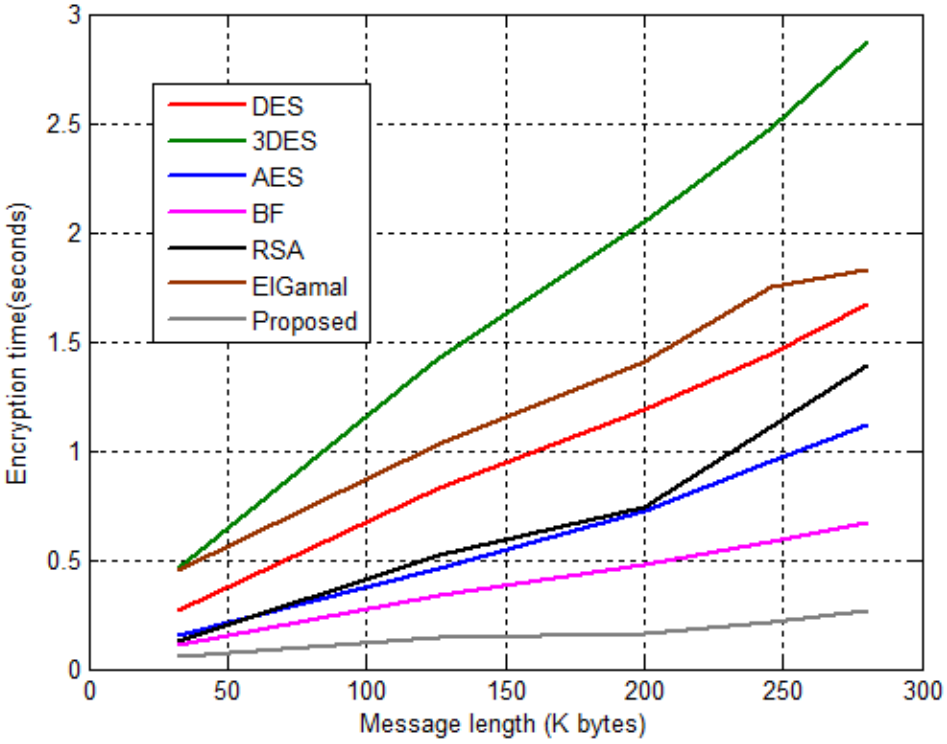

Figure 10: ETs comparisons

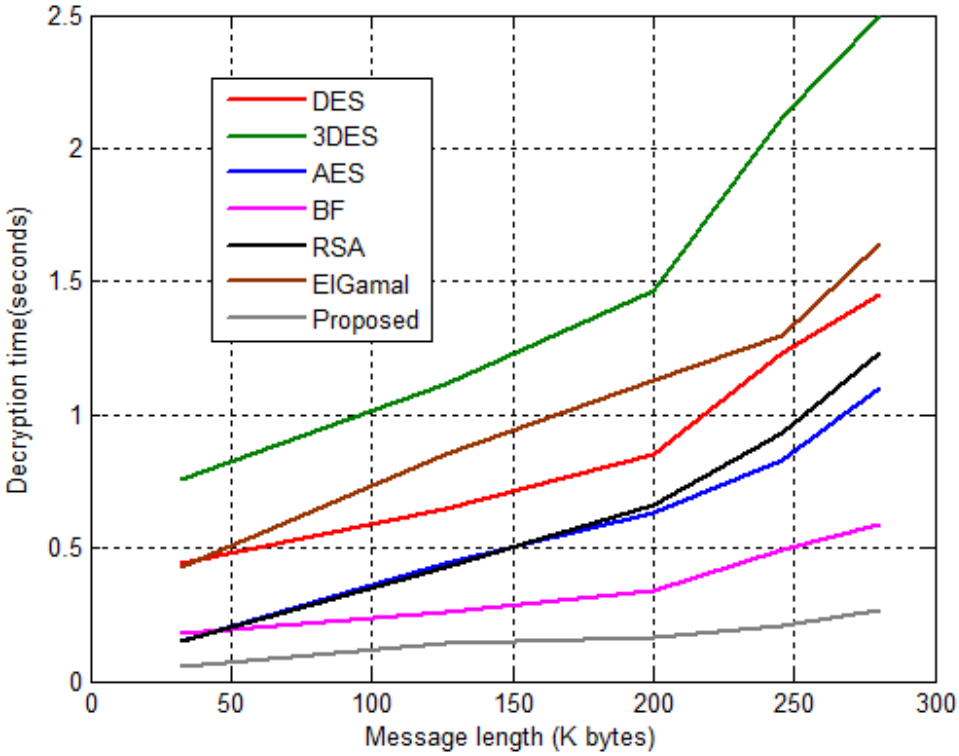

Figure 11: DTs comparisons

Table 8: Speedup of the proposed method

Method	Average encryption TP(K byte per second)	Speedup of proposed method	Average decryption TP(K byte per second)	Speedup of proposed method
DES	148.8889	8.3465	174.0260	7.1409
3DES	86.5633	14.3560	101.1779	12.2823
AES	236.4706	5.2552	255.2381	4.8688
BF	368.5200	3.3721	430.7527	2.8849
RSA	206.6838	6.0126	236.4706	5.2552
ElGamal	124.2658	10.0003	150.2804	8.2692
Proposed method	1242.7	1.0000	1242.7	1.0000

Security Analysis

The proposed method uses a character PK, the length of the PK is variable, and it may contain upper and lower case characters, numbers and special characters, thus the key space can be calculated using equation 5:

Possible combinations = possible number of characters ^{L}

$$\textbf{Key space} = 94^{L} \qquad (5)$$

L: PK length in characters
This key space will capable to resist any hacking attack, and it will rapidly increase when increasing the PK length.
A PK of 20-character length will take the following time:
P=500,000 PKs per second

$$\textbf{Combinations: } 94^{20}$$

$$\textbf{Combination:=2.90106241131461823373062754674 14e+39}$$

$$\textbf{Time to crack:=1838582408874323924335581 63.27866 years}$$

Conclusion

A simple, highly secure and efficient method of SM cryptography was introduced, the method can be used to encrypt-decrypt any message with any length without the need to modify the algorithm or the PK. The PK contains a character values and it has a variable length, from short to long, the selected PK length can suit any message with any length.

The proposed method was implemented using various SMs; the obtained results were analyzed using various approaches of data analysis.

The sensitivity analysis showed that the decrypted message was very sensitive to the selected PK, any changes in this key during the decryption phase was considered as a hacking attempt by producing a damaged decrypted message.

The quality analysis showed that the proposed method gave a low quality message in the encryption phase and a high quality message in the decryption phase based on the calculated quality parameters MSE, PSNR, CC and NSCR.

The efficiency of the proposed method was tested, ET, DT and TP were calculated and compared with standard methods efficiencies and it was shown that the proposed method provided a significant speedup.

References

[1] A. Al Hasib and A. A. M. M. Haque, "A comparative study of the performance and security issues of AES and RSA cryptography," Proc. -3rd Int. Conf. Converg. Hybrid Inf. Technol. ICCIT 2008, vol. 2, no. November 2001, pp. 505–510, 2008.

[2] S. Farah, M. Y. Javed, A. Shamim, and T. Nawaz, "An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms," Recent advances Inf. Sci., vol. 8, pp. 121–124, 2012.

[3] G. Singh, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," Int. J. Comput. Appl., vol. 67, no. 19, pp. 975–8887, 2013.

[4] A. Patil and R. Goudar, "A Comparative Survey of Symmetric Encryption Techniques for Wireless Devices," Int. J. Sci. Technol. Res., vol. 2, no. 8, pp. 61–65, 2013.

[5] C. Science and M. Studies, "An Efficient Password Security Mechanism Using Two Server Authentication and Key Exchange," pp. 50–53, 2015.

[6] A. Levi and E. Sava's, "Performance evaluation of public-key cryptosystem operations in WTLS protocol," Proc. - IEEE Symp. Comput. Common., pp. 1245–1250, 2003.

[7] S. S. and K. Annapurna Shetty, "A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm," Int. J. Innov. Res.Comput. Commun. Eng., vol. 2, no. Special issue 5, p. 98, 2014

[8] D. Elminaam, "Performance evaluation of symmetric encryption algorithms," Int. J. Comput. Networks, vol. 8, no. 12, pp. 280–286, 2008.

[9] H. Mathur and P. Z. Alam, "Cryptology Algorithm," Int. J. Emerging Trends Technol. Comput. Sci., vol. 4, no. 1, pp. 4–6, 2015.

[10] D. Sukhija, "Performance Evaluation of Cryptographic Algorithms: AES and DES," vol. 3, no. 9, pp. 582–585, 2014.

[11] M. Panda, "Performance Analysis of Encryption Algorithms for Security," pp. 840–844, 2016.

[12] E. Barker, A. Roginsky, G. Locke, and P. Gallagher, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths," NIST Spec. Publ., no. January, pp. 800–131, 2011.

[13] H. O. Alanazi, B. B. Zaidan, a. a. Zaidan, H. a. Jalab, M. Shabbir, and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors," J. Comput., vol. 2, no. 3, pp. 2151–9617,2010.

[14] A. K. Mandal and C. Parakash, "Performance Evaluation of Cryptographic Algorithms: DES and AES," 2012.

[15] A. Sterbenz and P. Lipp, "Performance of the {AES} Candidate Algorithms in {Java}," Third {Advanced Encryption Stand. Candidate Conf. April 13--14, 2000, New York, NY, USA, pp. 161–168, 2000.

[16] R. L. Rivest, A. Shamir, and L. Adleman "A Method for Obtaining Digital Signatures and Public- Key Cryptosystems." Communications of the ACM, vol. 26, no. 1, pp. 96–99, 1983.

[17] M. E. Student, "Algorithms for Secure Cloud," vol. 3, no. 6, pp. 1–9,2014.

[18] G. Bernabé and N. Clarke "Study of RSA Performance in Java Cards,"2013.

[19] P. Nalwaya, V. P. Saxena, and P. Nalwaya, "A cryptographic approach based on integrating running key in feedback mode of ElGamal system," Proc. - 2014 6th Int. Conf. Comput. Intel. Commun. Networks, CICN2014, pp. 719–724, 2014.

[20] X. Li, X. Shen, and H. Chen, "ElGamal digital signature algorithm of adding a random number," J. Networks, vol. 6, no. 5, pp. 774–782, 2011.

[21] S. Sahu, A. Kushwaha, M. Scholar, Performance Analysis of Symmetric Encryption Algorithms for Mobile Ad hoc Network, Published 2014, Computer Science, Corpus ID: 13907600.

[22] Abdullah N. Olimat, Ali F. Al-Shawabkeh, Ziad A. Al-Qadi, Nijad A. Al-Najdawi, Forecasting the influence of the guided flame on the combustibility of timber species using artificial intelligence, Case Studies in Thermal Engineering, Volume 38, 2022, 102379, ISSN 2214-157X, https://doi.org/10.1016/j.csite.2022.102379.

[23] M. Abu-Faraj, and Z. Alqadi, "Image Encryption using Variable Length Blocks and Variable Length Private Key," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 11, Iss. 3, pp. 138-151, 2022.

[24] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Dual Approach for Audio Cryptography," Journal of Southwest Jiaotong University, vol. 57, no. 1, pp. 24-33, 2022.

[25] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," Symmetry, vol. 14, Iss. 4, pp. 664-678, 2022.

[26] M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Purr- posed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022.

[27] M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi, "Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study," Journal of Southwest Jiaotong University, vol. 56, no. 6 , pp. 685-694, 2021.

[28] M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Meth- odds for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12 , pp. 451-458, 2021.

[29] J. Vilkamo and T. Bäckström, "Time-Frequency Processing: Methods and Tools," in Parametric Time-Frequency Domain Spatial Audio, V. Pulkki, S. Delikaris-Manias, and A. Politis, Eds. Wiley, 2017, pp. 3–24.

[30] K Matrouk, A Al-Hasanat, H Alasha'ary, Ziad Al-Qadi, H Al-Shalabi, Speech fingerprint to identify isolated word person, World Applied Sciences Journal, 31 (10), 1767-1771, 2014.

[31] Ziad alqadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, vol. 2, issue 4, pp. 288-298, 2007.

[32] Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh, A Novel Based On Image Blocking Method to Encrypt-Decrypt Color, International Journal on Informatics Visualization, vol. 3, issue 1, pp. 86-93, 2019.

[33] Musbah J Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering and Technology, vol. 7. Issue 3.13, pp. 104-107. 2018.

[34] Jihad Nadir, Ashraf Abu Ein, Ziad Alqadi, A Technique to Encrypt-decrypt Stereo Wave File, International Journal of Computer and Information Technology, vol. 5, issue 5, pp. 465-470, 2016.

[35] Saleh Khawatreh, Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi, A Novel Methodology to Extract Voice Signal Features, International Journal of Computer Applications, vol. 975, pp. 8887, 2018.

[36] Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9. Issue 9, pp. 4092-4098, 2019.

[37] Aws Al-Qaisi, Saleh A Khawatreh, Ahmad A Sharadqah, Ziad A Alqadi, Wave File Features Extraction Using Reduced LBP, International Journal of Electrical and Computer Engineering, vol. 8. Issue 5, pp. 2780-2787, 2018.

[38] Ayman Al-Rawashdeh, Ziad Al-Qadi, using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research, vol. 8, issue 4, pp. 1356-1359, 2018.

[39] Ashraf Abu-Ein, Ziad AA Alqadi, Jihad Nader, A TECHNIQUE OF HIDING SECRETE TEXT IN WAVE FILE, International Journal of Computer Applications, 2016.

[40] Ismail Shayeb, Ziad Alqadi, Jihad Nader, Analysis of digital voice features extraction methods, International Journal of Educational Research and Development, vol. 1, issue 4, pp. 49-55, 2019.

[41] Jihad Nader Ahmad Sharadqh, Ziad Al-Qadi, Bilal Zahran, Experimental Investigation of Wave File Compression-Decompression, International Journal of Computer Science and Information Security, vol. 14m issue 10, pp. 774-780, 2016.

[42] Ziad A AlQadi Amjad Y Hindi, O Dwairi Majed, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management, vol. 4, issue 2, pp. 48-55, 2020.

[43] Majed O Al-Dwairi, A Hendi, Z AlQadi, an efficient and highly secure technique to encrypt-decrypt color images, Engineering, Technology &Applied Science Research, vol. 9, issue 3, pp. 4165-4168, 2019.

[44] Amjad Y Hendi, Majed O Dwairi, Ziad A Al-Qadi, Mohamed S Soliman, a novel simple and highly secure method for data encryption-decryption, International Journal of Communication Networks and Information Security, vol. 11, issue 1, pp, 232-238, 2019.

[45] Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, USING SPEECH SIGNAL HISTOGRAM TOCREATE SIGNAL FEATURES, International Journal of Engineering Technology Research & Management, vol. 4, issue 3, pp. 144-153, 2020.

[46] M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Ex- Traction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.

