Journal of Computer Science

Original Research Paper

Segmented Block Cipher Algorithm Based on ASCII-Codes Maneuver

[1]Shadi Rasheed Masadeh and [2]Hamza Abbass Al-Sewadi

[1]Faculty of Information Technology, Isra University, Amman, Jordan
[2]Faculty of Information Technology, Middle East University, Amman, Jordan

Article history
Received: 02-11-2017
Revised: 24-11-2017
Accepted: 14-12-2017

Corresponding Author:
Hamza Abbass Al-Sewadi
Faculty of Information Technology, Middle East University, Amman, Jordan
Email: alsewadi@hotmail.com

Abstract: Due to their complexity, computation time and power requirement, the secure and widely used cryptographic systems such as 3DES and AES may not be considered suitable for applications like mobile and remote sensing of sensitive data. Therefore, secure but less complicated algorithms for data encryption are still sought. This paper suggests a new Segmented Block Cipher Algorithm (SBCA) is a symmetric algorithm that relies on simple mathematical operations and permutation processes on segmented message blocks. The ASCII code representations of the message characters and the key contents are dealt with throughout the encryption and decryption phases. Obtained results manifested a reasonable computation time while the checked security strength looks.

Keywords: Information Security, Encryption/Decryption, Secret Key, Symmetric Cryptography, Block Cipher

Introduction

Data security has been the concern of people and authorities since the old Roman and Chinese empires. Cryptography is the term used for securing the data by converting it from clear and intelligible form into cipher or unintelligible form (encryption) and then the reverse process recovers the original data (decryption). So many methods have been developed and used over the years involving sequences of processes (called algorithms) and secret information (called key). Traditionally, the same key is used for encryption and decryption processes, hence, it is termed symmetric cryptography (Stallings, 2011). According to Kirchhoff's Principle, it is always assumed that the algorithm is known, therefore, any algorithm strength should be based on the secrecy of the key (Knudsen and Robshaw, 2011), which should be strong enough to stand attacks. Recently, after the advances in the computer systems, new and advanced cryptographic systems were developed that introduced lengthy and sophisticated processes cryptosystems, such as Data Encryption Standard (DES), Pretty Good Privacy (PGP), Blowfish, International Data Encryption Algorithm (IDEA), etc. (Schneier, 1996). Then with more advances in computation capabilities, other more powerful system were developed, such as triple DES (3DES), Advanced Encryption Standard (AES) (Yan, 2009, Verma *et al*., 2013), AES-GCM (Wilkinson, 2017), FAROQ (Dawood *et al*., 2017), etc. All these system are symmetric systems, as they use the same key for both encryption and decryption, which raised the problem of key distribution.

Another type of cryptosystems emerged after the genius discovery of Diffie and Hellman (1976), which introduced the possibility of using a pair of asymmetric keys; one is used for encryption and the other for decryption. They initiated what is known today as the public key cryptosystem. This new system proved useful for secrecy, authentication and key distribution. Many public key systems were developed afterword, the most widely used of them is RSA which is developed by Rivest *et al*. (1977).

Any cryptographic system is breakable, given the computation power and time, besides, with the dramatic advances in computation efficiency; the danger becomes drastic, leading for nonstop search seeking new sophisticated and efficient cryptographic algorithms. However, efforts are also spent on less sophisticated algorithms for speed purposes, such as new versions of playfair cipher (Goyal *et al*., 2015; Kumar *et al*., 2010).

This paper suggests a new block cipher algorithms that relies on ASCII code maneuver of segmented messages for the encryption/decryption processes and incorporating multi-section secret key.

After, the introduction of section 1, related work is shown in section 2. The proposed ciphering algorithm is outlined in section 3. Then section 4 includes the

experimentation investigation of the algorithm, presenting the results and discussing the consequences. Finally section 5 concludes the paper.

Related Work

The widely circulated symmetric cryptographic systems in use today are of block ciphers types. It can be said that modern block cipher have started as early as 1949 triggered by Shannon's seminal paper, which was based on the concept of iterated product using multiple sub-keys and incorporating the simple operations of substitution and permutation. This concept was implemented in the Feistel network at IBM in the late 1960s and was then adopted in the first block cipher system, known as Data Encryption Standard (DES) (van Tilborg and Jajodia, 2011).

DES was standardized as suitable security technique widely employed for commercial and governmental applications used for encrypting sensitive but unclassified data in 1977 by the FIBS standard. In the late 1980s, differential and linear cryptanalysis found good ground for attacking DES (Matsui and Yamagishi, 1992; Biham and Shamir, 1993). However, the linear attack on DES was not really practical as it requires 247 known plaintexts (Matsui, 2007). After the realization that DES is becoming vulnerable to be breached by Brute force attack due to increasing computation efficiency and cryptanalysis attacks, a triple Data Encryption Standard (3DES) was defined and standardized. It works by applying DES three times using either double or triple keys.

Due to the need for running DES three times, the application of resulting 3DES means very long operation time. The weakness of DES led to the development of the more advanced and highly secure block ciphers cryptosystems, namely the Advanced Encryption Standard (AES) that was referred to as Rijndael, which was announced in year 2000 winning an international competition for a system to replace DES. It was standardized by FIPS standard published in 2001. AES proved to be fairly strong and may survive both linear and differential attacks for years to come, however, it is complex and also time consuming which makes it un-attractive for certain applications that have limited power supply or does not tolerate lengthy encryption/decryption processes. Since about ten years, data security, researcher interests focused their attention towards hash functions; however, more interests were also growing for the development of lightweight block ciphers symmetric cryptosystem, such as; the ultra-light block cipher, PRESENT (Bogdanov *et al*., 2007), the lightweight block cipher for multiple platforms, TWINE (Suzaki *et al*., 2013), the lightweight block cipher, LBlock (Wu and Zhang, 2011), A family of lightweight block cipher, KLEIN, (Gong *et al*., 2012), the bit-slice ultra-lightweight block cipher suitable for multiple platforms, RECTANGLE (Zhang *et al*., 2014) and many more. The role of energy in the profile for many important application domains of lightweight cryptography is thoroughly investigated by Patrick and Schaumont (2016).

Moreover, a recent lengthy survey listed a comprehensive study of tens of the reported lightweight cryptosystem that were suggested, tested, standardized and implemented by academic community, government organizations and intelligent agencies (Biryukov and Perrin, 2017). They discussed their implementation constraints and what they are usually designed to satisfy, covering relevant national (e.g., NIST) and international (e.g., ISO/IEC) standards. They also discussed some identified trends in the design of lightweight algorithms, such as designers' preference for arx-based and bitsliced-S-Box-based designs and simple key schedules. They classified the field of lightweight cryptography into two related but distinct areas: Ultra-lightweight and IoT cryptography.

Materials and Methods

The proposed symmetric cryptographic algorithm is a segmented block cipher algorithm (referred to hereafter as SBCA) based on operating on ASCII codes. The message to be encrypted M is first segmented into blocks of 60 characters each (M1, M2, ..., Mi, etc.). Then each block Mi is encrypted by the algorithm using a key K that consists of 10 alphanumeric characters in addition to one integer as follows.

Encryption Key

The key is randomly selected and agreed upon by the communicated parties using the printable characters. Only these characters are used for both the message contents and the key (which are from number 32 to 122 in the ASCII code table for the Latin language). The message and the key components are replaced by their ASCII-code serial number values. Figure 1 shows the block diagram for the encryption/decryption processes of the SBCA algorithm. It summarizes the required steps used for both encryption and decryption processes, then these processes will be explained in details in the following.

Encryption Algorithm

Encrypting each message segment block Mi is achieved by the following steps.

Read text file Mi as input plaintext blocks of 60 characters each.

Replace this text file components by the serial number of their ASCII code.

DOI: 10.3844/jcssp.2017.748.755

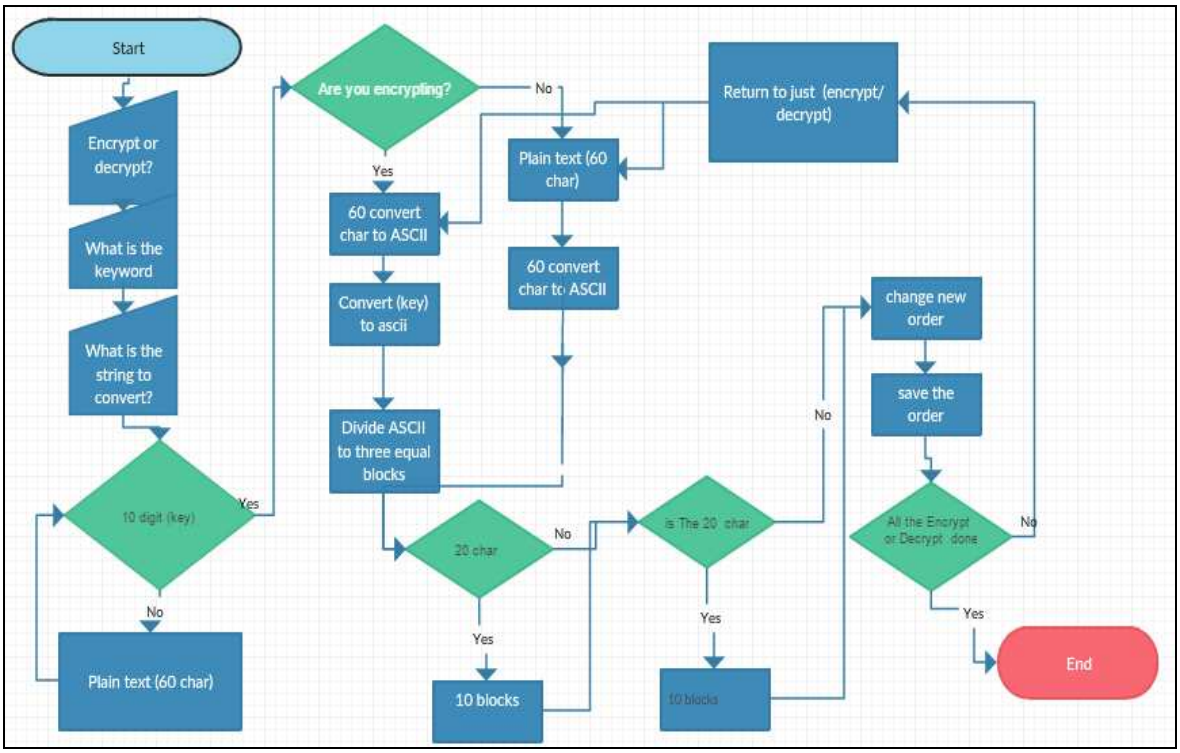

Fig. 1: Block diagram for the proposed encryption/decryption algorithm

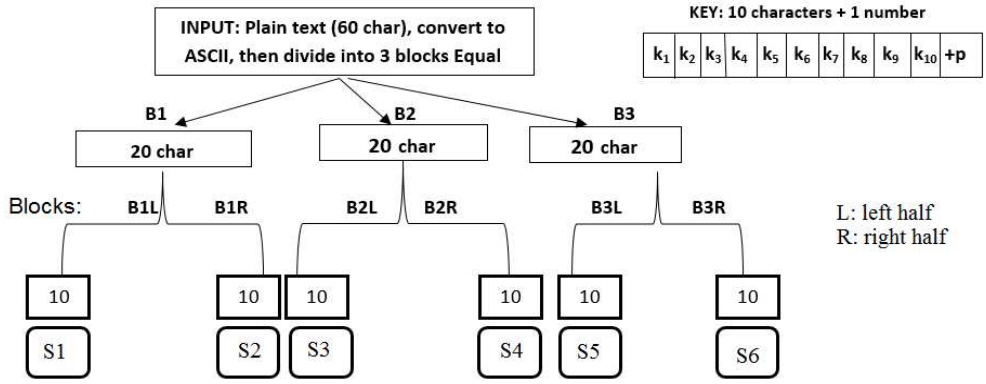

Fig. 2: Segmenting the message block

Divide the resulting 60 ASCII code character into three sub-groups, each of 20 characters length and then divide this sub-group into two segments, each of 10 character length. i.e., 60/3 = 20 character each sub-group and the 20/2 = 10 character segment, resulting into 6 segments *Si*, $i = 1, \ldots, 6$ and each segment is the set $S = \{dj, j = 1, \ldots, 10\}$.

Figure 2 shows a block diagram illustrating the following 1 to 3 steps:

- Replace all the resulting segments characters by the serial number of their ASCII code using the ASCII-code table
- The key content which consists of 10 alphanumeric characters are also replaced by the serial number of their ASCII code, using the ASCII-code table also. Let these serial numbers be expressed by ten integers ($k_1, k_2, k_3, \ldots, k_{10}$). An integer p, (which has the value $p = 1, 2, 3, 4, 5$, or 6 is attached to the key. The value of P points to one of the six segments
- Now for each of the six segments, change the value for each component using Equation 1. For example, for segment *p*, its 10 components *bj* ($j = 1, .., 10$) are altered as follows:

$$cj = (bj + kj + p) mod\ 91 + 32.... \quad (1)$$

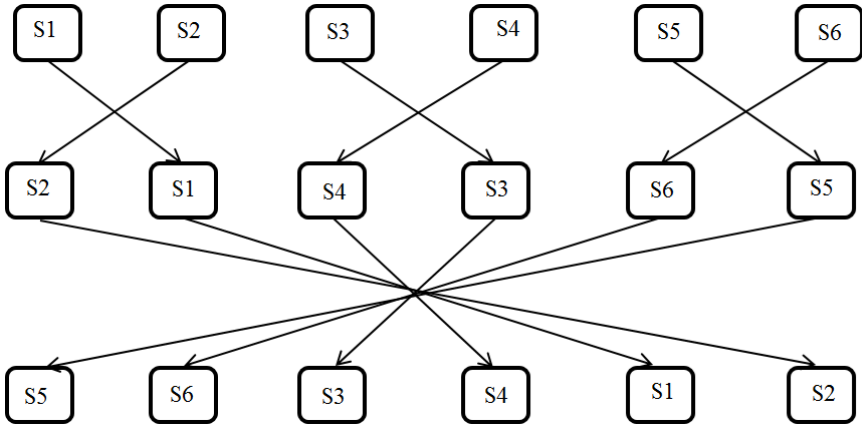

Fig. 3: Interchange of the segments

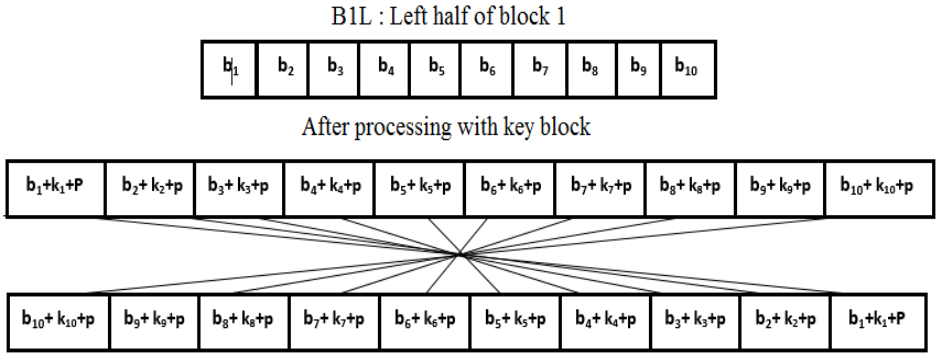

Fig. 4: Interchange of the segments

Figure 3 shows a block diagram illustrating the following 4 to 7 steps:

- Reverse the location order of the components for each segment, i.e., c1-to-c10 becomes c10-to-c1
- Reverse the segments order, i.e., S1 to S6 becomes S6 to S1
- Interchange segments of each neighboring segment pairs, i.e., S1 with S2, S3 with S4 and S5 with S6
- Replace the resulting string of component values by their corresponding characters using the ASCII code table. Then, the resulting 60 character message block C is the ciphertext of the original message block M

Figure 4 shows a block diagram illustrating the following 8 and 9 steps:

- Reverse the segments order, i.e., S1 to S6 becomes S6 to S1
- Interchange segments of each neighboring segment pairs, i.e., S1 with S2, S3
- Replace the resulting string of component values by their corresponding characters using the ASCII code table. Then, the resulting 60 character message block C is the ciphertext of the original message block M

Decryption Algorithm

Decryption process is exactly the inverse of the encryption process. After the reception of the ciphered message, it is first segmented into blocks of 60 characters each and then each block C is decrypted by the decryption algorithm using the same shared key K that is agreed upon by the communicating parties. The message and the key components are replaced by their ASCII-code serial number values (which are from number 32 to 122 in the ASCII code table for the Latin language). Then decryption process proceeds as follows:

- Convert this text file components to the serial number of their ASCII code
- Divide the resulting 60 ASCII code character into three sub-groups, each of 20 character length and then divide each sub-group into two segments, each of 10 character length. i.e., 60/3 = 20 character each sub-group and the 20/2 = 10 character segment, resulting into 6 segments *Si*, i = 1,.. 6 and each segment is the set $S = \{cj, j = 1, \ldots, 10\}$
- Reverse the segments order, i.e., S1 to S6 becomes S6 to S1

- Interchange segments of each neighboring segment pairs, i.e., S1 with S2, S3 with S4 and S5 with S6
- Reverse the location order of the components for each segment, i.e., c1-to-c10 becomes c10-to-c1
- Now the six segments are taken one by one and for each segment i (i = 1,..,6), its 10 components values are recalculated by Equation 2:

$$dj = (cj - kj - p + 241) mod\ 91... \quad (2)$$

- If the obtained *dj* is less than 32, the value is adjusted to be in the printable character range by Equation 3, otherwise it is taken as it is:

$$dj = dj + 91\ \ ....\ \ ... \quad (3)$$

- To recover the original plain message M, the resulting values are replaced by the corresponding letter using the serial numbers in the ASCII code table

Results

The proposed SBCA is designed, coded and tested for encryption and decryption using C# language and Pentium PC. Results of the algorithm testing for encryption and decryption of various messages were satisfactory. To clarify the execution of the algorithm for encryption, Fig. 5 shows an example. It shows the encryption of a short message consisting of 60 characters using a given key of 10 characters length in addition to 1 numeral. It is meant to illustrate how this message block is segmented into six segments first and then the process of encrypting the first segment using Equation 1.

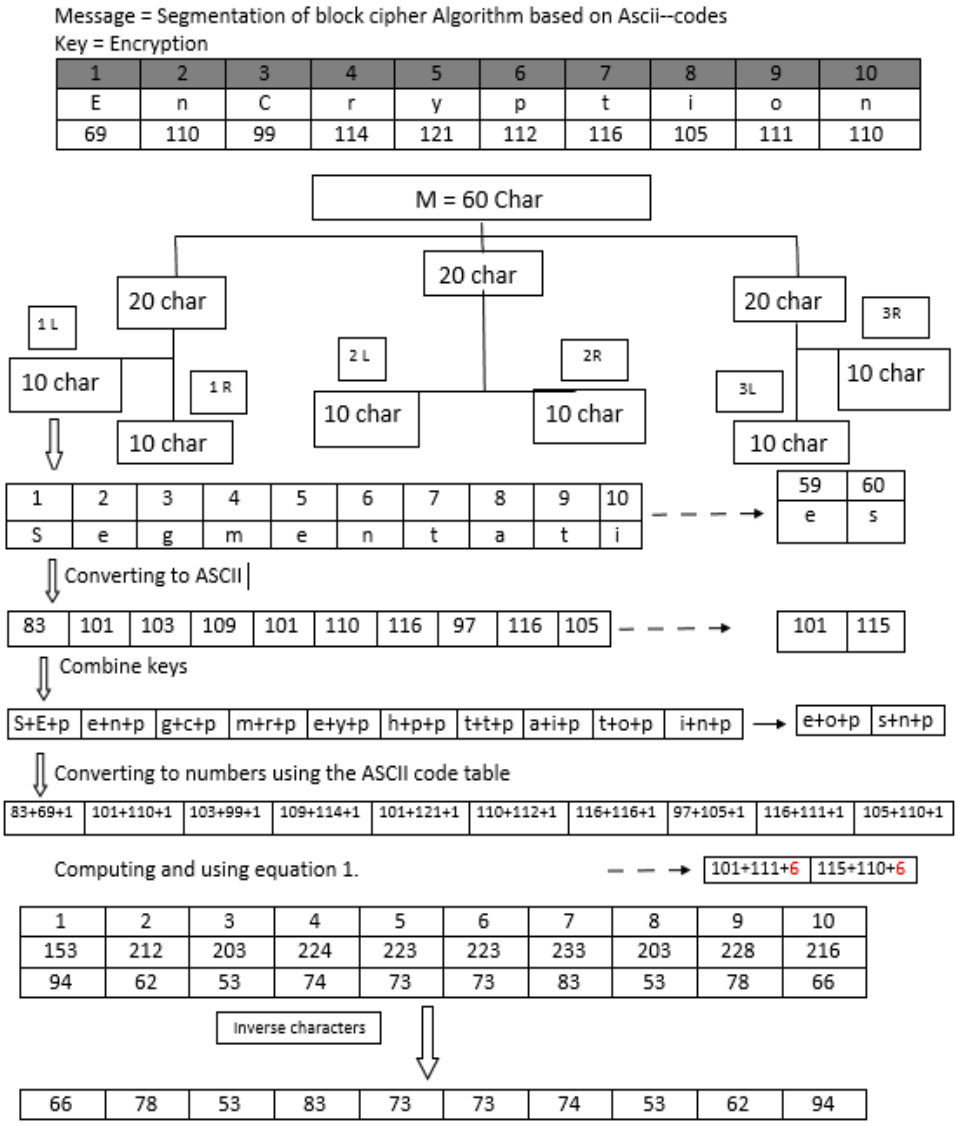

Fig. 5: An example for the encryption of a message block

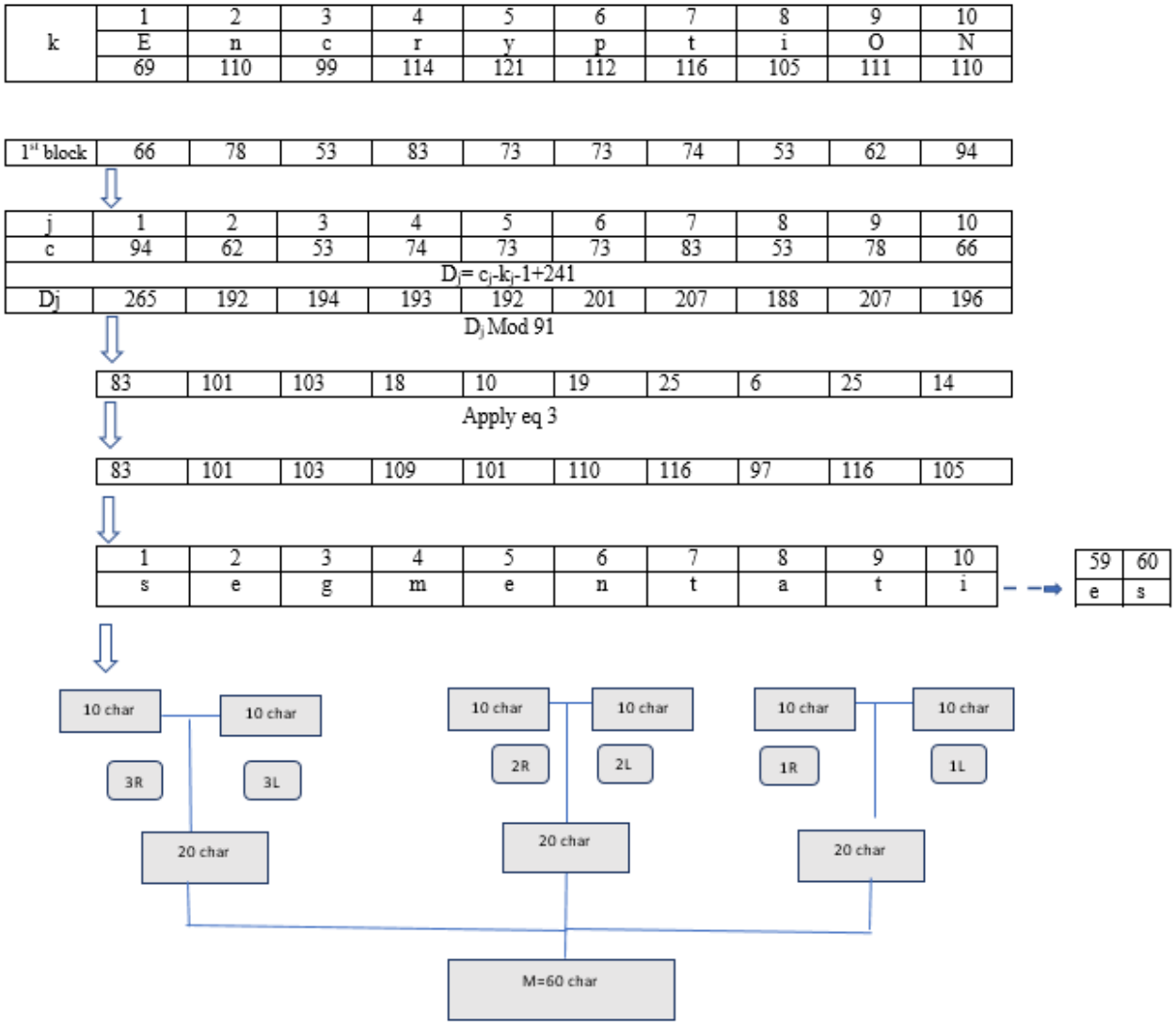

Fig. 6: An example for the decryption of a message block

The process of decryption can be done in a reverse order of the encryption process. This process is outlined in Fig. 6 for an example, decrypting the same message block encrypted in the previous figure using the same key. It must be noted that Equation 2 and 3 are implemented for this calculation.

Message Block and Key Length

The proposed SBCE used a 60 character message block length. When it is divided by 6, the segment length equals 10 characters. However, the design can be adopted for any block length provided that a proper key length is chosen. The criteria here that the number of message segments should be even and key length must equal to the message segment length. For example if a message block length equals 80 characters, then if segment length is 80/4 = 20 characters, the key length shall be 20 character and so on.

Brute Force Attack

Brute force attack means trying all possible key combination to break the security. Therefore, one of the factors for key strength is its length in order to be able to stand brute force attack. For this reason, care must be taken in selecting the key. Moreover, the proposed SBCA has the flexibility of choosing any key length.

In the proposed algorithm, the key length was 10 characters plus 1 numeral, which means it consists of 88 bits. This length might be only suitable for some application; however, to increase the key length, the algorithm can be customized to any required key length provided the criteria mentioned above are considered.

Table 1: Comparison of SBCA with DES, 3DES and AES algorithms

Algorithm	Key length (bits)	Key space	Block size	Execution time (sec)
DES	56	2^{56}	64	$64*10^{6}$
3DES	168	2^{168}	64	$256*10^{39}$
AES	128	2^{128}	128	$256*10^{36}$
SBCA	88	2^{88}	60	$256*10^{15}$

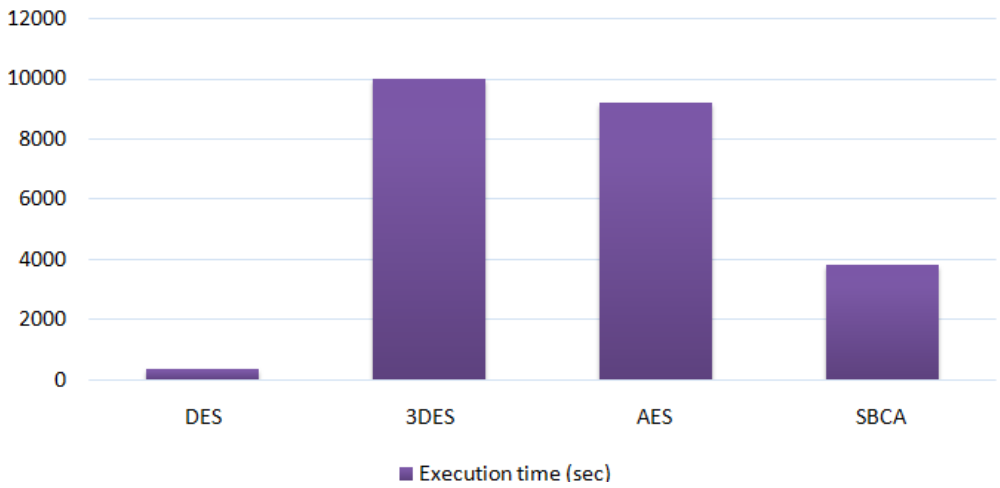

Fig. 7: Comparison of SBCA with other algorithms

Computation Time

The operations included in the SBCA technique are only addition and subtraction; therefore due to their type and number, it is expected to be much faster than other systems such as 3DES and AES. Preliminary experiments have shown this fact. More work will be conducted in the future to calculate and compare the execution time with other system.

A comparison may be done for the proposed SBCA with other cryptographic algorithms, such as DES, 3DES and AES. Such comparison includes the key lengths, the key space, the message block size and execution time as shown in Table 1. The execution time in this table is calculated approximately by assuming that a computation speed of (10^{-9} second) per key is used and all possible key values are considered (i.e. Brute force). 128 bit key length is used for AES and three different keys of 56 bit lengths are used for 3DES, while 88 bit length is used for SBCA.

The execution time for the cryptosystems considered above is plotted in Fig. 7 for quick comparison purpose. It shows clearly that the proposed SBCA algorithm is slower than DES but much faster than AES and 3DES.

Therefore, SBCA is expected to be much more efficient than DES, but less than 3DES and AES. However, it has the flexibility of increasing both, the block size and the key length by customizing the design to operate with different specification according to the required length.

Conclusion

The proposed segmented block cipher algorithm SBCA is a symmetric algorithm that has simpler arithmetic operations than many encryption techniques with a reasonable flexibility which makes it suitable for applications like mobile and remote sensing of sensitive data. It does not need to store large tables and tens of repetitions round rather it relies on simple mathematical operations and permutation processes on segmented message blocks. It can be customized to the application used for by adjusting both the message block length and the secret key length. Therefore, it would be suitable for applications that need less complexity, computation time and power requirement. More investigation would be carried out in order to compare different security factors with other systems, such as 3DES and AES.

Acknowledgment

The authors would like to thank both of Isra University and Middle East University (Jordan) for giving them the opportunity to perform and publish this research work.

Author's Contributions

Shadi Rasheed Masadeh: Organized and participated in all the experimentation plus contributed to the writing of the manuscript.

Hamza Abbass Al-Sewadi: Designed the research plan, coordinated the data analysis and contributed to the writing of the manuscripts.

Ethics

Participation during pilot and experiment trials are voluntary and participants are made known that their feedbacks will be contributing to a non-profit research project.

References

Biham, E. and A. Shamir, 1993. Differential Cryptanalysis of the Data Encryption Standard. 1st Edn., Springer Verlag, New York, ISBN-10: 0387979301, pp: 188.

Biryukov, A. and L. Perrin, 2017. State of the art in lightweight symmetric cryptography.

Bogdanov, A., L.R. Knudsen, G. Leander, C. Paar and A. Poschmann *et al*., 2007. PRESENT: An Ultra-Lightweight Block Cipher. Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Sept. 10-13, Springer, Vienna, Austria, pp: 450-466. DOI: 10.1007/978-3-540-74735-2_31

Schneier, B., 1996. Applied Cryptography: Protocols, Algorithms and Source Code in C. 2nd Edn., John Wiley and Sons, ISBN-10: 0471128457, pp: 758.

Gong, Z., S. Nikova and Y.W. Law, 2012. KLEIN: A New Family of Lightweight Block Ciphers. Proceedingss of the 7th International Workshop on Radio Frequency Identification: Security and Privacy Issues, Jun. 26-28, Springer, Heidelberg, pp: 1-18. DOI: 10.1007/978-3-642-25286-0_1

Dawood, O.A., A.M.S. Rahma and A.J. Abdul Hossen, 2017. New symmetric cipher Fast Algorithm of Revertible Operations' Queen (FAROQ) cipher. Int. J. Comput. Netw. Inform. Security, 4: PP 29-36. DOI: 10.5815/ijcnis.2017.04.04

Diffie, W. and M. Hellman, 1976. New directions in cryptography. IEEE Trans. Inform. Theory, 22: 644-654. DOI: 10.1109/TIT.1976.1055638

FIBS 46-3, 1977. Federal information processing standards publication.

FIBS 197, 2001. Federal information processing standards publication 197.

Goyal, P., G. Sharma and S.S. Kushwah, 2015. Network security: A survey paper on playfair cipher and its variant. Int. J. Urban Design Ubiquitous Computer, 3: 1-8. DOI: 10.14257/ijuduc.2015.3.1.01

Knudsen, L.R. and M.J.B. Robshaw, 2011. The Block Cipher Companion. 1st Edn, Springer, New York, ISBN-10: 364217342X, pp: 270.

Kumar, M., R. Mishra, R.K. Pandey and P. Singh, 2010. Comparing Classical Encryption with Modern Techniques. S-JPSET, 1: 49-54. DOI: 10.18090/samriddhi.v1i1.1578

Matsui, M. and A. Yamagishi, 1992. A new method for known plaintext attack of FEAL cipher. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, May 24-28, Springer, Balatonfüred, Hungary, pp: 81-91. DOI: 10.1007/3-540-47555-9_7

Matsui, M., 2007. Linear cryptanalysis method for DES cipher. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, (TAC' 07), Springer, Lofthus, Norway, pp: 386-397. DOI: 10.1007/3-540-48285-7_33

Patrick, C. and P. Schaumont, 2016. The role of energy in the lightweight cryptographic profile. NIST.gov.

Rivest, R.L., A. Shamir and L. Adleman, 1977. A method for obtaining digital signatures and public-key cryptosystems. Communication. ACM, 21: 120-126. DOI: 10.1145/359340.359342

Shannon, C.E., 1949. Communication Theory of Security Systems. Bell Syst. Technical J., 27: 656-715.

Stallings, W., 2011. Cryptography and Network Security: Principle and Practice. 5th Edn, Pearson Education, ISBN-10: 0133354695.

Van Tilborg, C.A.H. and S. Jajodia, 2011. Encyclopedia of Cryptography and Security. 1st Edn, Springer, New York, ISBN-10: 144195905X, pp: 1416.

Suzaki, T., K. Minematsu, S. Morioka and E. Kobayashi, 2013. TWINE: A lightweight block cipher for multiple platforms. Proceedings of the 19th Annual International Workshop on Selected Areas in Cryptography, (SAC' 13), Springer, Heidelberg, pp: 339-354.

Verma, V., D. Kaur, R.K. Singh and A. Kaur, 2013. 3D-Playfair cipher with additional bitwise operation. Proceedings of the International Conference on Control Computing Communication and Materials, Aug. 3-4, IEEE Xplore Press, Allahabad, India, pp: 1-6. DOI: 10.1109/ICCCCM.2013.6648913

Wilkinson, K., 2017. Using encryption and authentication to secure an UltraScale/UltraScale+ FPGA bitstream.

Wu, W. and L. Zhang, 2011. LBlock: A Lightweight Block Cipher. Proceedings of the 9th International Conference on Applied Cryptography and Network Security, Jun. 07-10, Springer, Nerja, Spain, pp: 327-344. DOI: 10.1007/978-3-642-21554-4_19

Yan, S. Y., 2009. Primality Testing and Integer Factorization in Public-Key Cryptography. 2nd Edn, Springer, New York, ISBN-10: 0387772685, pp: 371.

Zhang, W., Z. Bao, D. Lin, V. Rijmen, B. Yang and I. Verbauwhede, 2014. RECTANGLE: A bit-slice ultra-lightweight block cipher suitable for multiple platforms. IACR Cryptology ePrint Archive.