# DIFFERENT DATE BLOCK SIZE USING TO EVALUATE THE PERFORMANCE BETWEEN DIFFERENT SYMMETRIC KEY ALGORITHMS

[1]Ali M Alshahrani [2]Prof. Stuart Walker

Department of Electronic Systems Engineering, University of Essex,
Wivenhoe Park, Colchester, Essex, UK, C04 3SQ

***ABSTRACT***

*The different computer networks whether wired or wireless are becoming more popular with its high security aspect. Different security algorithms and technique are using to avoid any aforementioned attacks. One of these technique is a cryptography technique that makes the data as unreadable during the transfer hence; there is no chance to reclaim the information. Presently, most of the users are using various media types and internet to transfer the data but, it has the chance to retrieve the data by using these media types. The perfect solution for this problem is to provide security on time-to-time basis; this stage is always significant to the security related community discussions. This paper explains the comparison between the run time of three different encryption algorithms which are DES, AES and Blowfish The compression includes using different modes, data block size and different operation modes. As a result, Blowfish algorithm followed by AES take less time for running compared to DES.*

***KEYWORDS***

*AES, DES, Blowfish, Encryption and Decryption.*

## 1. INTRODUCTION:

Real time applications (RTA) are a set of technologies that are used to allow multimedia, such as voice calls, videoconferences to transfer the data from sender to receiver through the Internet Protocol (IP). There are many reasons that help to appear such services like the low of cost. Consequently, many companies enroll to this market and develop several of system that are provide a good quality of service. Recently, the computer and internet network has developing and that allow to multimedia to be the best choice for most of people to contact.

Sensitive information, financial transactions and political meetings are an example of data that must have a high level of security. The cryptography system technique has long been used to ensure this sensitive information can be transmitted in a way that protects them when they are transported through an unsecured network (e.g. the internet).

To protect the stored data in computing systems, using different security techniques is highly required such as encryption and decryption technique. By using this security everyone can easily protect their stored data in computers and during transmission process. For example, data cannot be read or observed by any other persons with permission. By implementing passwords and data encryption techniques, many computers will be secured. Translation of data into a form is called as Data encryption. This is incoherent without a decode mechanism. A password is a secret word or phrase that gives a user access to a particular program or system [1][2].

DOI : 10.5121/ijcnc.2014.6208 

Security techniques are also named as information security. It is able to implement for computers and networks. Cryptography system is very important to transmit different types of data through unsecure network such as Internet. Encryption and decryptions are the process that done to move the data from the sender to receiver but by using a secret key. The procedure of changing the plain text into cipher text is called as an encryption algorithm. This process is done during the transfer the data through vulnerable channels and secret key is even used in encryption for the process of conversion. On the other hand, the process of changing the cipher text into a plain text is called as decryption algorithm. The procedure accomplished using the secret key. Plain text is the original text before encryption. After entered a secret key to the plain text, it becomes a cipher text. The basic aspect of the symmetric algorithm is a secret key, which is used in both decryption and encryption techniques. But, it needs to maintain secret to avoid the middle attacks to retrieve the information. The cryptography technique is classified into two types: Asymmetric Algorithm and Symmetric Algorithm Converting the plaint text into the cipher text by using secret key is called encryption [3][4][5].

This paper explains the description of symmetric cryptography algorithm survey, performance analysis and symmetric encryption algorithm between three of the most common algorithms which are DES, AES and Blowfish. They are implemented in Java to compare the performance by using different data block size and the standard key length.

## 2. CRYPTOGRAPHY:

Encryption and decryption systems are defined as a set of algorithms that convert plain text data by using an agreement key for the cipher text in the sender side (encryption). The decryption process is done on the receiver side by extracting the key from the data to obtain the plain text again. The encryption method is considered strong due to several factors: the initialization vectors, the length and secrecy of the key, the algorithm, and how all of these function simultaneously. Strength, in terms of encryption, generally signifies the level of difficulty by which it is possible to decipher the key or algorithm. Thus, decoding a key must involve processing a large number of probable values in order to attain a value which can be employed so as to decrypt or decode a particular message. In other words, non-repudiation services, authenticity, confidentiality, and integrity can be provided by means of a cryptosystem. The basic types of cryptographic systems are symmetric keys, also called secret keys, or asymmetric keys, also called public keys (see next section) [3][5].

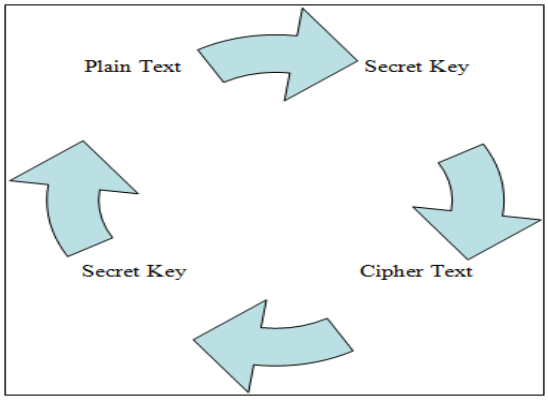


Figure1: Encryption and decryption process.

### 2.1 The basic types of cryptographic system:

The basic types of cryptographic systems are symmetric keys, also called secret keys, or asymmetric keys, also called public keys. The idea behind symmetric key systems is for both the sender and the recipient to have the same key. The sender uses this key in order to encode or encrypt the information or data, and once more, the recipient utilizes it in order to decrypt the information or the data[3][6][7]. Figure below shows the Symmetric key:

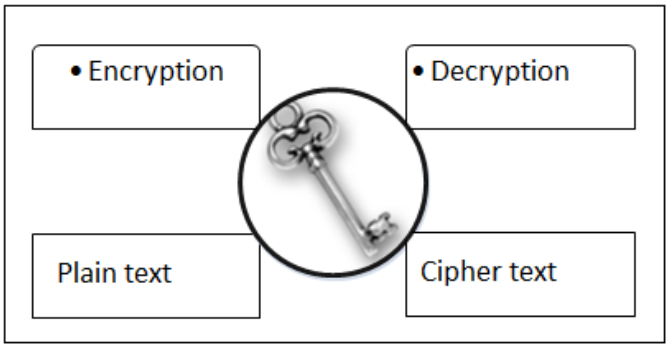


Figure2: Symmetric technique.

On the other hand, asymmetric cryptographic systems are believed to be far more adaptable and compliant. Normally, each user holds a public key as well as a private key. Therefore, one key is used in order to encrypt or encode messages while the other key is utilized to decrypt or decode the messages [3][6][7]. The figure below shows the asymmetric key procedure.

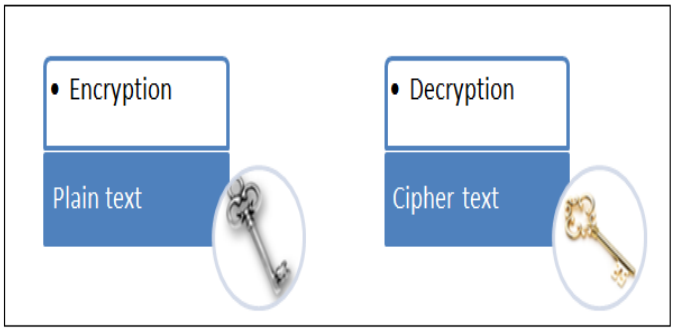


Figure 3: Asymmetric key

## 3. BLOCK CIPHER VS. STREAM CIPHER

Block and stream ciphers are considered as symmetric ciphers. In fact, stream ciphers are based on producing an "unlimited" cryptographic keystream and applying it to encrypt a bit or byte simultaneously. Conversely, block ciphers operate concurrently on larger pieces of data that is, blocks, frequently joining blocks in order to provide extra security.

The stream cipher idea is simply to divide the text into relatively unit by unit to allow every block encoding to be based on numerous preceding blocks. The concept of a block cipher is to divide the text into fairly bulky blocks, for instance, 128 bits, then to encode every block individually. Normally, each block encoding is based on at the maximum a block of the former ones. The key remains unchanged when applied with every block [8][9].

## 4. MODE OF OPERATION:

Modes of operations are the algorithms used in a cryptography system with a block cipher technique to provide security requirements, such as confidentiality and authenticity. The modes identify the way that data will be encrypted. The standard modes are the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode [10][11][12].

### A. Electronic codebook (ECB):

ECB is a raw cipher that was published in 1981; it provides confidentiality and does not use IV. The main concept of this mode is to split the message into fixed-length blocks and encrypt each block independently. In this operation mode, the data are divided into 64-bit blocks, which are encrypted one at a time. For example, if data are transmitted along the network and any transmission occurs, it will affect only the blocks that contain the error. The blocks should be rearranged, and then the data sent. The greatest disadvantages of this encryption technique are, first, problems being encountered when protecting the affected data from the attack, and second, this mode being less effective when compared to the remaining modes. However, it is fast and easy to implement compared with the other modes [10][11][12].

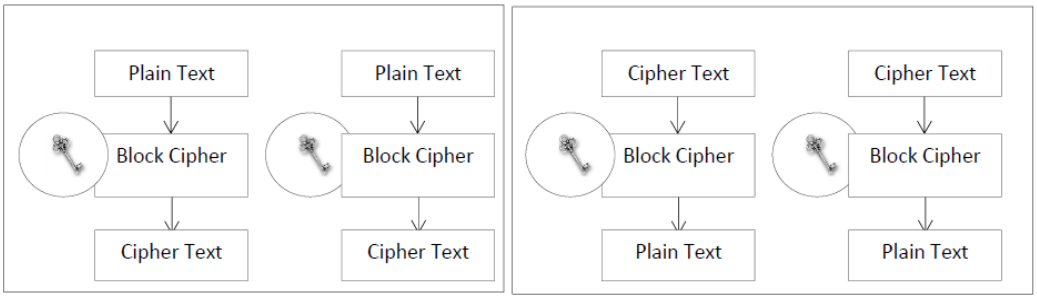


Figure 4: ECB mode encryption and decryption process.

### B. Cipher-block chaining (CBC)

The main concept of this mode is that IV is X-ORed with plaintext before encryption and for later blocks, uses the previous ciphertext as the IV. In order to know the plain text for a particular block, it is also necessary to know the key and cipher text for the previous block. As the first block is encrypted but has no previous cipher text, a 64-bit block is used to encrypt the block; this is called an initialization vector. If any problem occurs during the transmission, the error is forwarded to all the blocks because each is dependent on the other; thus it will affect the subsequent block. So the data will not be affected. This operation mode is more secure than the ECB operation mode [10][11][12].

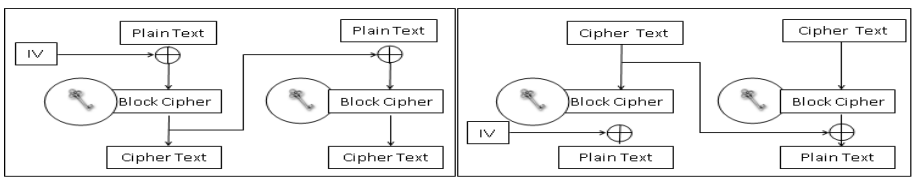


Figure 5: CBC mode encryption and decryption process.

### C. Cipher feedback (CFB):

In this operation mode, the input data are considered as the blocks of input, but not is not necessary to store the 64 bits of data. First, the 64 bits are stored in the one block called the shift register. Then, this shift register is considered as an input in plaintext. This block is already set to some arbitrary values. This cipher text is then passed through the extra components, called M-boxes. The M-boxes select only certain bits for encryption. This output is in plaintext. This cipher text is again fed into the shift register, and it acts as an input for the next block. This process is the same as the CBC, but additional functionalities are added to this system. If any error occurs, it will affect the subsequent blocks only. Compared to CBC, its performance is slower because of some added complex functionalities [10][11][12].

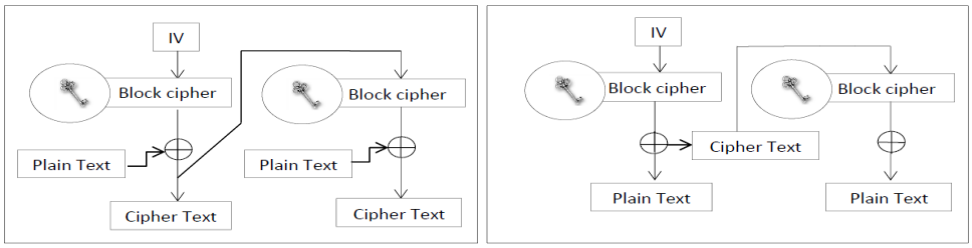


Figure 6: CFB mode encryption and decryption process.

### D. Output feedback (OFB)

This operation mode is the same as the CBC but there are slight changes in the system performance. This takes the input into the shift register and sets it to an arbitrary initial value, and this is then passed into the algorithms. From there, it is passed into the M-boxes. This is the final output cipher text. This value is X-ORed with the real plain text, and this is the final output. In CBC and CFB, if any error occurs, it will affect all the subsequent blocks but when in OFB and once the shift register has been initialized, it will continue to affect all the blocks of the shift registers. Because each block output does not depend on the previous block, it will not affect the remaining blocks. However, it is less secure than the CBC and CFB because only the cipher text and DES cipher text values are needed to find the original plain text; the key is not required [10][11][12].

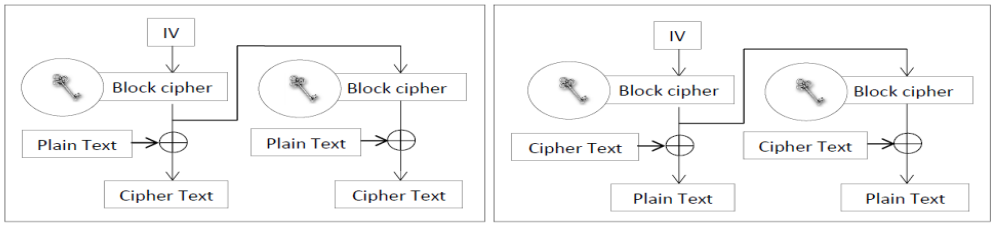


Figure 7: OFB mode encryption and decryption process.

## 5. ENCRYPTION ALGORITHMS:

### A. Data Encryption Standard (DES)

DES is one of the block cipher techniques developed by the National Bureau of Standards in the USA in 1976. It is used for security purposes to protect sensitive, unclassified, and commercial data by using the 56-bit key and 64-bit block size [13][14].

### B. Advanced Encryption Standard (AES) :

AES technology (Rijndael) is a block cipher symmetric algorithm published in 1997 by NIST for use instead of DES. Generally, the AES standard allows a block size of 128-bits and selects one key out of three keys, such as 192, 265 and 128-bit keys. AES is used to provide security for data by encrypting the original data to the cipher data [15][16].

### C. Blowfish:

This technique has a 64-bit block size and the length ranges from 32-bits to 448-bits. Blowfish is a 16-bit round Feistel cipher and utilizes the large key dependent S-boxes, which are rigid, and each line allows 32-bits. These S-boxes allow input of up to 8-bits and give an output of up to 32-bits. Given that the key length of Blowfish can be extended from 38-bits to 448-bits, this provides more security for data. The 32-bit key input is separated into four 8-bit quarters and uses one-by-one quarter as inputs[17][18][19].

## 6. EXPERIMENTAL METHODOLOGY, RESULT AND ANALYSIS:

The Java environment was used to evaluate the run time performance of three different types of encryption algorithms (DES, AES and blowfish) and four different types of operations modes. The aim of the experiment is to calculate each algorithm's run time speed efficiency to encrypt and decrypt many blocks of different sizes of text in different modes of operation. The key size of DES, AES and blowfish are 56, 128 and 128 respectively. While the block sizes are 64 for DES and 128 for AES and blowfish. The below figure shows the GUI of the Java program.

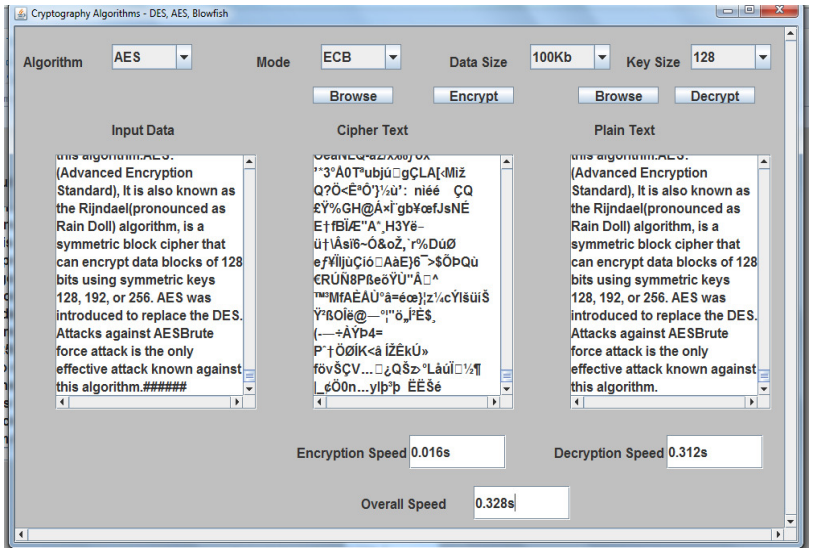


Figure 8: GUI of the Java program.

## RESULT AND ANALYSIS:

The experiment has been done to compare between DES, AES and Blowfish which are consider as symmetric key cryptography algorithms. Different sizes of data blocks and standards key size used to evaluate the algorithm's run time speed. 100, 200, 300, 400, 500 and 1000 kb are the data block size that using in the experiment and the user can choice one of these size or can choice any block size. The DES key size is 64 and AES and Blowfish are 128 kb.

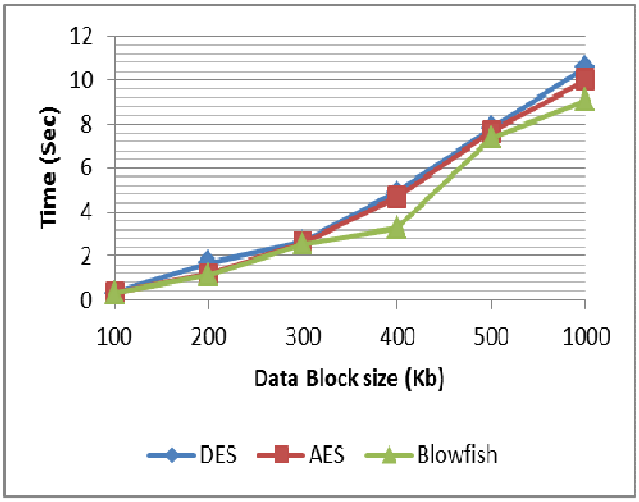


Figure 9: run time performance speed with ECB mode

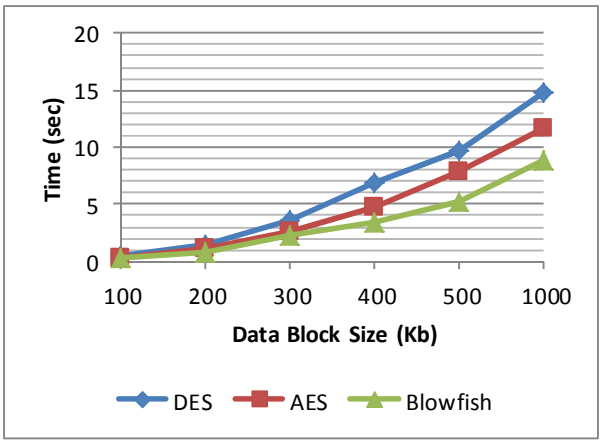


Figure 10: run time performance speed with CBC mode.

CBC requires more processing time than ECB because of its key-chaining feature. However, compared to ECB, CBC is much better in terms of security.

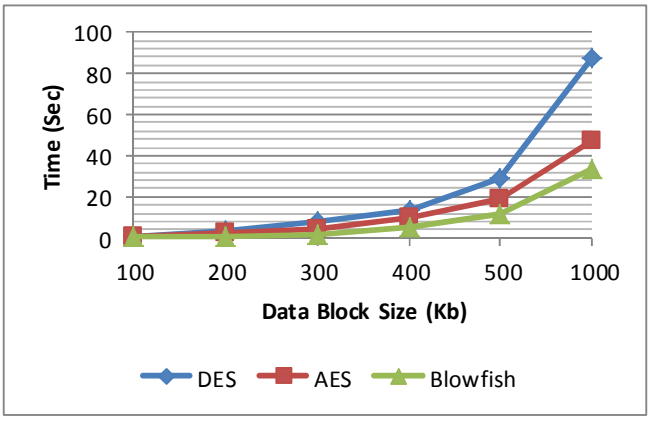


Figure 11: run time performance speed with CFP mode.

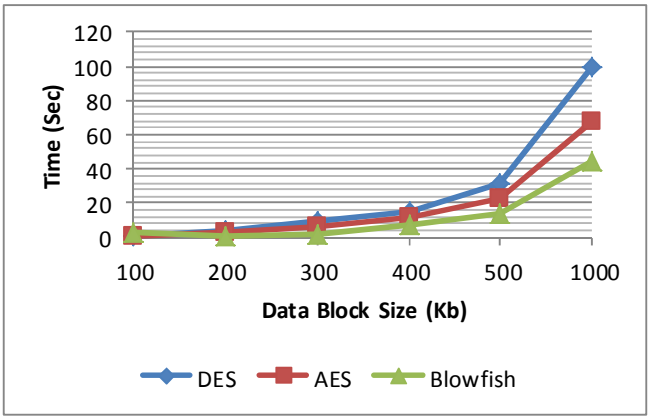


Figure 12: run time performance speed with OFB mode.

The OFB mode has a different procedure for the security processes because it uses the XOR operation, and its cipher output is a key stream so it needs more time compared to previous modes. Finally, as expected, CFB requires less processing time than does OFP.

## CONCLUSION:

Performance of the symmetric encryption algorithms DES, AES and Blowfish has been evaluated for the different modes (ECB, CBC, CFB, and OFB) of encryption and decryption. Key size for DES algorithm is fixed as 56 bits, AES and Blowfish algorithms have the key size of 128 bits. Execution time is evaluated by varying different data sizes of 100,200,300,400,500 and 1000 Kb. The result shows that Blowfish run time is the fastest algorithm compared to AES and DES.

## FUTURE WORK:

In future, the work will extend this project to allow the encryption and decryption of all different types of data, such as image, sound, and video. Then, a new algorithm will be developed that will fulfil the QoS requirements.

## ACKNOWLEDGEMENTS:

I would like to express my very great appreciation to Prof. Walker for his advice and completely supporting during this paper.

## REFERENCES


[1] M. Hil. and G. Zhang, "A Web Services Based Frame work for Voice over IP", Proceedings of the 30th Euromicro Conference, vol. 10, pp. 258 –264, 2004.

[2] Obaida. Al-Hazaimeh, " Increase the Security Level for Real-Time Application Using New Key Management Solution", International Journal of Computer Science Issues(IJCSI), Vol. 9, Issue 3, 2012.

[3] D. Stinson," Cryptography Theory and Practice", CRC Press Inc., NY, USA, 1995.

[4] E. Cole, R. Krutz and J. W. Conley," Network Security Bible", Wiley Publishing Inc, 2005.

[5] Katz, Jonathan and Yehuda Lindell (2007).' Introduction to Modern Cryptography'.

[6] P.C. van Oorschot, A.J. Menezes, and S.A. Vanstone, "Handbook of Applied Cryptography,"CRC Press, Inc., 1997.

[7] Network Associates, Inc., '' An Introduction to Cryptography.'', June 2001.

[8] B. Moeller ,''Security of CBC Ciphersuites in SSL/TLS: Problems and Countermeasures'', (May 20, 2004),

[9] William F. Ehrsam, Carl H. W. Meyer, John L. Smith, Walter L. Tuchman, "Message verification and transmission error detection by block chaining", US Patent 4074066, 1976.

[10] Dworkin M. '' Recommendation for Block Cipher Modes of Operation', NIST Special Publication 800-38A 2001 Edition.

[11] Biham, Eli and Shamir, Adi, ''Differential Cryptanalysis of the Data Encryption Standard'', Springer Verlag, 1993. ISBN 0-387-97930-1, ISBN 3-540-97930-1.

[12] Hristof Paar, Jan Pelzl, "Stream Ciphers", Chapter 2 of "Understanding Cryptography, A Textbook for Students and Practitioners", 2009.

[13] Knudsen, Lars R., The Block Cipher Companion. Springer. ISBN 9783642173417, (2011).

[14] Daemen J, Rijmen V, "The Design of Rijndael: AES – The Advanced Encryption Standard." Springer, 2002. ISBN 3-540-42580-2.

[15] H Wang ; H Zheng ; B Hu ; H Tang .'' Improved Lightweight Encryption Algorithm Based on Optimized S-Box', Computational and Information Sciences (ICCIS), 2013 Fifth International Conference.

[16] T Sharma. ; R. Thilagavathy. '' Performance analysis of advanced encryption standard for low power and area applications'', Information & Communication Technologies (ICT), 2013 IEEE Conference, 2013 , Page(s): 967 – 972.

[17] B. Schneier, "The blowfish encryption algorithm-one year later," Dr. Dobb 's Journal, 1995.

[18] B Schneier (1993). "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish).

[19] A. Alabaichi ; F. Ahmad ; R. Mahmod, '' Security analysis of blowfish algorithm'' Informatics and Applications (ICIA),2013 Second International Conference.


**Authors:**


Ali Alshahrani was born in Saudi Arabia in 1982. He received his M.Sc. from University of Essex in 2011. He is currently PhD student at Essex University, UK, Colchester. His research interests include Network Security, Image Processing, Mobile Payment and e-learning.

Prof. Stuart D.Walker was born in Dover, U.K., in 1952.He received the B.Sc. (Hons) degree in physics from Manchester University, Manchester, U.K., in 1973, and the M.Sc. degree in telecommunications systems and the Ph.D. degree in electronics from Essex University, Essex, U.K., in 1975 and 1981, respectively. After a period of postdoctoral work at Essex University, he joined the then British Telecom (BTPlc) Research Laboratories, Martlesham Heath, Ipswich, U.K., in 1982. Initially, he was concerned with regenerator design issues in submarine optical transmission systems. While at BT Plc, he was jointly responsible (with Prof. P. Cochrane) for pioneering the unrepeatered-transmission-system concept. In 1987, he was promoted to head the transatlantic link-repeater group, where he supervised the design and fabrication of high-reliability integrated circuits. In 1988, he became a Senior Lecturer at Essex University. There, his research interests included fiber-polarization studies and novel optoelectronic-device configurations. He then developed an interest in access-network design and construction, where he formed a specialist research group. In 2003, he was promoted to Reader and to Full Professor in 2004. He has published over 150 journal and conference papers and has 6 patents granted.