Journal, Advances in Mathematical & Computational Sciences
Vol. 8 No. 2, June 2020
www.mathematics-computationaljournal.info

Article Citation Format
Osagie, F.O. & Daodu, S.S. (2020): Development of an Enhanced Cryptographic Model for Data Security. Journal of Advances in Mathematical & Computational Sc. Vol.8, No. 2. Pp 1-8

Article Progression Time Stamps

Article Type: Research Article
Manuscript Received 11th April, 2020
Final Acceptance: 22nd June, 2020
Article DOI Prefix: dx.doi.org/10.22624

Development of an Enhanced Cryptographic Model for Data Security

Osagie, F.O. & Daodu, S.S.
Department of Computer Science
University of Benin
Benin City, Nigeria
E-mail: Sege.daodu@gmail.com, mailfrank126@gmail.com
Phone: +2348130762937

ABSTRACT

In this study an enhancement of Sohail's cryptographic model was developed to solve the challenges of data security in data communication systems. The existing model combined the Q' block and the R' block with the key and as such showed a pattern at the middle in the ciphertext which is easily recognizable, this limitation may give room to ciphertext only attack by an adversary. The developed model improved on the limitation by resolving the patterns in the ciphertext and gives no clue to an adversary. The improved cryptographic model has a fast encryption and decryption time, and will maintain confidentiality, integrity, and privacy of data.

Keywords: Information Security, Cryptographic models, Data Communication, decryption, Privacy, Integrity.

1. INTRODUCTION

Cryptography is the study of information hiding and retrieval. Cryptography is derived from the Greek words: kryptós, "hidden", and gráphein, "to write" - or "hidden writing". It is the art of protecting the information by transforming it into an unreadable format in which a message can be hidden from reader and only the intended recipient will be able to convert it into original message. All intruders or unauthorized readers can only see gibberish (Singh, and Shende, 2014). Today data communication over a public channel, which includes any network, particularly the Internet is core for individuals as well as businesses purpose. The need for data security to secure data transmitted over these networks has become very important and could be achieved by the use of Cryptographic model.Cryptography provides various security goals to ensure data privacy, to prevent and detect unauthorized access, cheats, and other malicious activities.

These goals are: confidentiality, authentication, data integrity, and non-repudiate.

(i) Confidentiality is to keep the content of the information for authorised users only. There are several ways to providing this goal, starting from physical protection to encryption/decryption models.
(ii) Data integrity is a service that allows only authorised users to modify information. Unauthorised users cannot manipulate data such, access such as insert, delete, or substitution of data is denied.

(iii) Authentication relates to identification. All parties that wish to communicate should identify each other. Authentication of information sent over a public communication channel should entail the origin of the message, date of origin, data content, and time sent.

(iv) Non-repudiate is a service which prevent an entity from denying previous commitment or actions, neither the sender, nor the receiver of message be able to deny the transmission. For example, one entity may authorise the purchase of property by another entity and later deny such authorization was granted (Menezes *et al*, 1996).

Cryptography is broadly classified into three types to provide data security, which are: symmetric encryption, asymmetric encryption, and hashing. For the purpose of this research work they will be categorized based on the number of keys that are used for encryption and decryption.A typical cryptographic model takes plaintext and key as input of the encryption algorithm to produce a ciphertext that is to be transmitted over a communication channel and takes the ciphertext and the key as an input of the decryption algorithm to get back the original message (plaintext).

This scenario is represented in Figure 1.

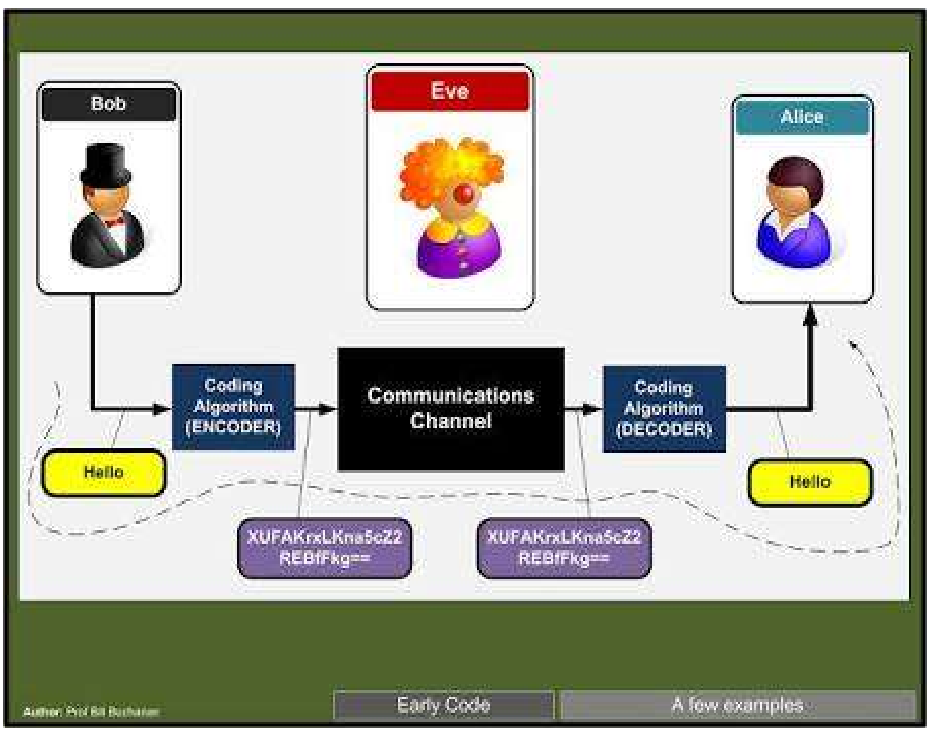

Figure 1: Cryptographic encryption and decryption model (Wikipedia).

In cryptography, unencrypted data is referred to as plaintext. Plaintext is encrypted into ciphertext, which will in turn be decrypted back into the original message (plaintext). The encryption and decryption is based upon the type of cryptography scheme being employed and some form of key (Kessler, 2019).

This process is sometimes written as:

E(p,k) = c and D(c,k) = p.

Where

p = plaintext; c = ciphertext; E = the encryption algorithm; D = the decryption algorithm and k = the key.

Cryptography is most closely associated with the development and creation of the mathematical algorithms used to encrypt and decrypt plaintext, whereas cryptanalysis is the study of analyzing and breaking cryptographic models. A cryptographic model is breakable if a third party without prior knowledge of the key pair, can systematically recover plaintext from the corresponding ciphertext within some appropriate time frame (Menezes *et al*, 1996). Cryptology is the term referring to the broad study of secret writing; it is therefore the study of both cryptography and cryptanalysis. Cryptographic models are typically classified into three types: symmetric-key cryptography, public-key cryptography, and hashing. However, in general, cryptographic models are also classified as classical cryptographic models and modern cryptographic models based on the periods these models are developed or used. Classical cryptographic models are developed in the earliest days, but some of the algorithms are still in use for providing confidentiality of information.

Modern cryptographic models are developed in recent years for providing better services like confidentiality, authentication, data integrity, and non-repudiate to the information. In order to increase the degree of security, the modern cryptographic algorithms are incredibly complex than classical cryptographic algorithms. Some of modern cryptographic algorithms are designed in such a way that repeats same procedure for many rounds, for example Feistel network. It is important to know that Symmetric-key encryption model have encryption and decryption algorithms in both of classical and modern cryptographic models. Some examples of classical models are Caesar cipher, Play fair cipher, Hill cipher, Vigenere cipher, Vernam cipher, One time pad, Rail fence and Root cipher, while DES, AES, Blownfish, Twofish are some modern cryptographic models (Saranya *et al*., 2014) For the purpose of this research work the focus will be on modern cryptographic models.

(i) Symmetric-key cryptography: uses the same secret key to both encrypt and decrypt data. The key should be made available to both the encoder and the decoder only. There are two types of symmetric-key cryptography – stream ciphers and block ciphers. Some important Symmetric-key cryptography algorithms examples are DES, TRIPLE DES, AES, TWOFISH, BLOWFISH, RC4, RC6.

Stream ciphers – encrypts plaintext bit-by-bit and are mainly of two types – self-synchronizing and synchronous stream ciphers. While Block ciphers – encrypts plaintext in blocks and uses modes of operation to provide information services such as confidentiality or authenticity. These modes of operation include: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR) mode. A mode of operation describes how to repeatedly apply a cipher's single-block (Saranya *et al*., 2014)

(ii) Public-key cryptography or Asymmetric encryption: This method uses two different keys for encryption and decryption which are the public and private keys. The public key is used to encrypt the plain text, its available to anyone on the network. Whereas private key is used to decrypt the cipher text, it's kept secret and only known to the sender and the receiver. Some important Public-key cryptography algorithms examples are RSA, Diffie-Hellman, Digital Signature Algorithm (DSA), ElGamal.

(iii) Hash functions or Message digest: hash function is one way encryption method and requires no key for encryption and decryption. A hash function is a function that can map data of arbitrary size onto data of a fixed size. The values that are returned by a hash function are called hash codes.

Some Hash algorithms in use include Message Digest (MD), Secure Hash Algorithm (SHA), Race Integrity Primitives Evaluation Message Digest (RIPEMD).

Several research works have been carried out on data security using cryptographic model for either individual or commercial purposes. Emphasis is always laid on the level of data security of any cryptographic model developed, how well it can secure personal or confidential information against adversaries, to this end the design and implementation of a model is paramount. To develop a reliable model, related works were reviewed which include:

2. RELATED WORKS

Monika Agrawal and Pradeep Mishra, (2012), presented a new approach that improves the existing Blowfish symmetric key encryption algorithm. This approach was carried out by changing the number of time the F function will be applied over the message. This intermittent decision of executing F function determined by bits representations in the random number equivalent has greatly improves Blowfish algorithm. The merit of this new model is that it runs faster than the existing model, it reduces the encryption and decryption time of Blowfish respectively and greatly increases the throughput as well. Another reviewed work proposed and developed by Aamir Sohail (2017) is a new symmetric key encryption/decryption algorithm using cryptographic model to transform data into a non-readable text. This proposed algorithm is effective and easy to apply; it's also fast and reliable compared to low level algorithm.

Gupta *et al* (2012), developed a block symmetric encryption algorithm based on block cipher and the model compared its encryption/decryption parameters to two existing cryptographic models. The advantage of this model is that the time to encrypt a message runs better than the time the two existing model will take to do the same work. Islam *et al* (2008), showed the effect of increasing block size and key size which in turn achieved a higher security level of Advance Encryption Standard (AES) algorithm. This work is less efficient to AES, but provides a higher security than AES. This was archived because security of any model is a direct function of its key size, the larger the key size. Anand *et al* (2016), proposed an efficient and easy to implement, but difficult to crack model for data security. This model is better than low level algorithm as well as classical algorithm.

Charru *et al* (2014), developed an enhanced cryptographic model. Security of an algorithm is measured by computing number of decryption steps, higher the number of decryption steps to decrypt the ciphertext to get original message shows higher level of security. From the result, the number of decryption steps taken to decrypt a ciphertext by the new model is higher than number of decryption steps of existing algorithm. The merit of this model is that the cryptographic system is stronger than the existing system and thus provided maximum security to encrypt plaintext messages. Jha *et al* (2016), used the principles of Caesar cipher and Hill Cipher to develop an encryption and decryption algorithm. It is simple to implement for individual and small scale businesses. Chatterjee *et al* (2011), improved on Nath *et al* (2010) by increasing the key size.

The merit of this method is that it is almost impossible to break the encryption algorithm without knowing the exact key matrix. Nath *et al* (2015), developed a symmetric key encryption algorithm called MSA for encrypting as well as decrypting file using a random key square matrix of 16 by 16.The merit of this work is that if we change the key text little bit then the whole encryption and decryption process will change.

3. MATERIALS AND METHODS

3.1 Description of the model

In figure (2), is a model that shows how to encrypt and decrypt data for secure transmission over unsecure communication channel. This approach is a stream cipher symmetric-key encryption model, where each plaintext and key is encrypted bit-by-bit. The secret key used to encrypt and decrypt data for this type of algorithm is the same for both the sender and the recipient.

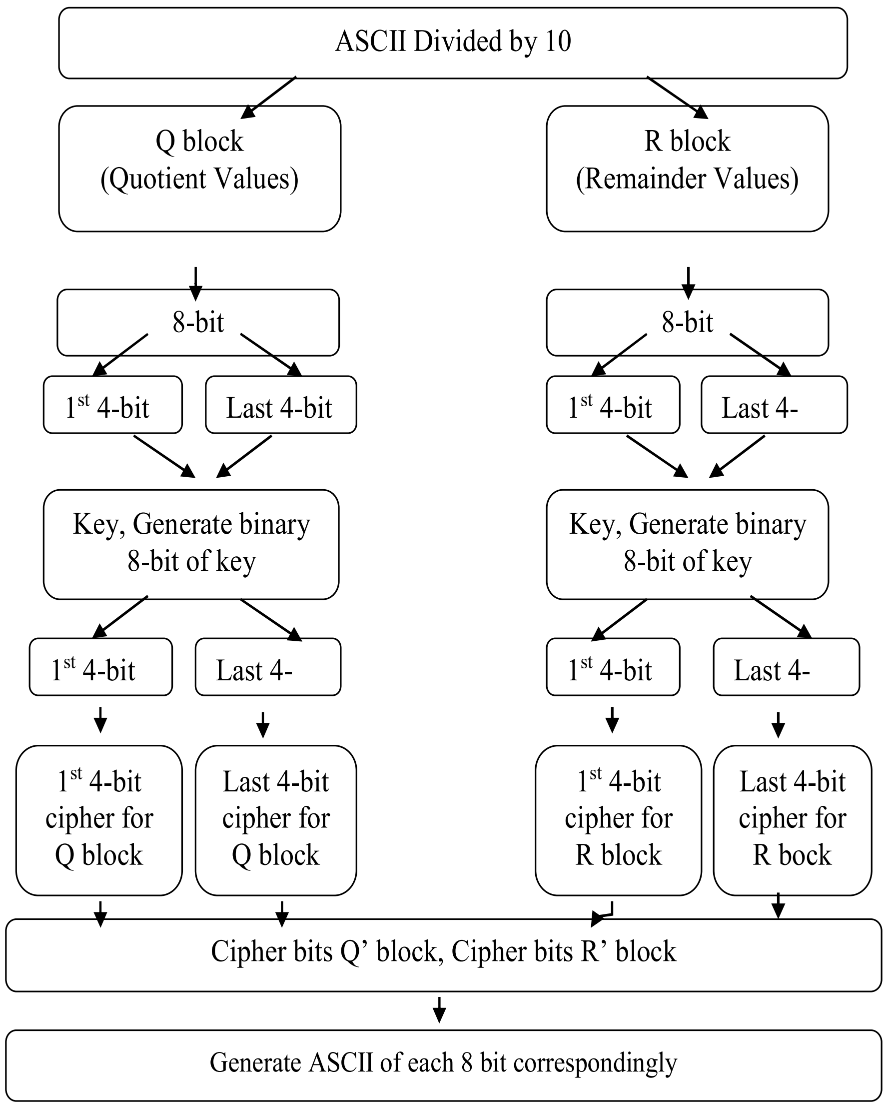

Figure 2: The developed Model.

3.2 Implementation of the encryption

The implementation sequence is given below

a) Read the user file and Generate Correspondingly ASCII value of each character in file.
b) Divide every character ASCII value by 10. Calculate Quotient value stores it in Q block, and do same for Reminder stores it in R block.
c) Calculate 8-bit binary value for each value that is stored in Q block and R block.
d) Read key from user. Calculate ASCII value of the key and convert it into 8-bit binary.
e) Every 8 bit binary key (K) is divided into 4 bits also Every 8 bit binary value in Q block and R block is also divided into 4 bits, that is K[K1K2K3K4] Q[Q1Q2Q3Q4] R[R1R2R3R4].
f) XOR Q1 with K2, Q2 with K1, Q3 with K4 and Q4 with K3. Also do the same for each 4 bits in R block, to get

   Q[Q1⊕K2Q2⊕K1Q3⊕K4Q4⊕K3]=Q'[Q1'Q2'Q3'Q4']

   R[R1⊕K2R2⊕K1R3⊕K4R4⊕K3] = R' [R1'R2'R3'R4']

g) Combine Q' cipher text block and R' cipher text block
h) convert each 8-bit binary in Q' and R' blocks into ASCII and Save ASCII value

3.3 Implementation of the decryption

a) Read Cipher text and convert cipher text into binary. The blocks obtained from the cipher text will be Q' and R'
b) Read key entered and convert key into binary value.
c) Divide 8-bits of each block (Q' and R') into 4 bits and divide 8-bits of key block into 4 bits also. The blocks obtained will be Q'[Q1'Q2'Q3'Q4'] R'[R1'R2'R3'R4'] K[K1K2K3K4]
d) XORs

   Q'[Q1'⊕K2Q2'⊕K1Q3'⊕K4Q4'⊕K3] = Q[Q1Q2Q3Q4]

   R'[R1'⊕K2R2'⊕K1R3'⊕K4R4'⊕K3] = R[R1R2R3R4].

e) Calculate ASCII value for each 8 bit in Q and R blocks.
f) Multiply each value in Q block by 10 and add the result to the value in R block
g) Convert the ASCII value back to plain text.

For the implementation of this study, a Toshiba satellite C660 laptop (Windows 10 Home Edition, 64 bit machine) with 6GB RAM and a 600GB hard drive was used. It has an Intel® Core™ i3 @2.4GHz processor. The model was evaluated using Cryptool2 and EverCrack cryptanalytic tool to check the performance and strength of the model against cryptanalysis attacks. The design of workflow using cryptool2 is to visualize the encryption and the decryption of data, while EverCrack carryout cryptanalysis on the ciphertext by attempting to crack it within a time period. Cryptool2 requires Java runtime environment (JRE) or alternatively a Java Development Kit (JDK) to run successfully on a machine. To test the strength and the weaknesses of the developed model, the existing and the developed models' ciphertext were subjected to EverCrack cryptanalysis attack. It took about 0.44 sec to brute force a 10 byte size of ciphertext of the existing model while it took about 0.53 sec to do the same for the developed model using the same byte size. Testing a 5 byte size ciphertext for both models, it took 0.19 sec to recover the plaintext of the existing model and about 0.25 sec to recover the plaintext of the developed model. Thus it takes longer time to crack the developed model's ciphertext as compared to the existing model. Some major cryptanalysis attacks are: Known plaintext attack, Known ciphertext attack, Chosen plaintext attack, and Chosen ciphertext attack. Other cryptanalysis attacks that are mainly applicable to block cipher are: Brute-force attack, Differential cryptanalysis, Linear cryptanalysis, Integral cryptanalysis, Boomerang attack.

4. RESULT AND DISCUSSION

The results presented in Table (1) show the encryption and decryption time against its byte sizes

Table 1: Result obtained from the experiment

Block Size (Byte)	Encryption Time (sec)	Decryption Time (sec)
2	5 sec	4 sec
5	12 sec	7 sec
10	13 sec	9 sec

Graphical representation of the results shown in Table 1 is presented in Figure (3).

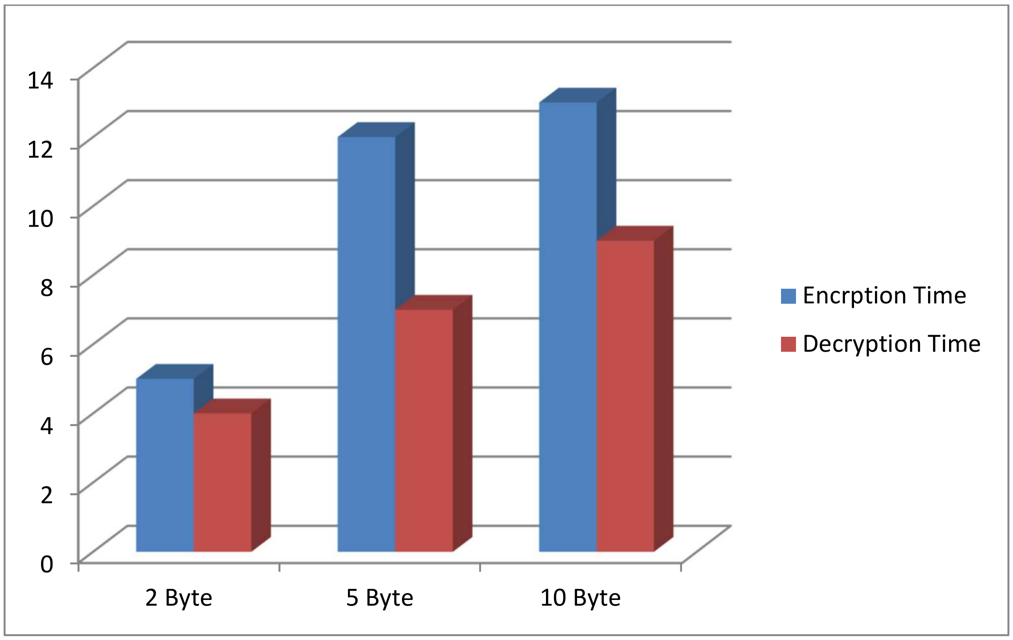

Figure 3: Graphical representation of result

From the graph it clearly shows that it takes a longer time to encrypt a plaintext than to decrypt the ciphertext. This is because more steps were used to implement the encryption algorithm to meet high level security requirement for the data, while the decryption algorithm was implemented with fewer steps to allow better response time to decrypt a cipertext by the intended recipient. Therefore, the developed model has been able to strict a balance between providing high level security for data and meeting business performance requirements which is crucial and a necessary trade off in a business environment.

5. CONCLUSION

Cryptographic models are very important to secure information over an unsecured channel as information is transmitted from one place to another. Due to the high volume of data sent each day all over the world, the field of data security has an enormous task on their hands to continue designing and reviewing to improve existing cryptographic models that secure and maintain personal and confidential information. In the industries such as the telecommunication and banking for instance, the rate of cyber-attacks are on the rise and huge amount is invested in securing their system, which is not always a guarantee and with a poorly designed data security system such companies will lose huge amount of money and will easily go out of business. However, with properly designed and implemented cryptographic model such as the proposed model, such attacks can be mitigated.

REFERENCES

1. Agrawal, M., and Mishra, P. (2012), A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm, International Journal of Engineering and Advanced Technology, **1**, (6), 79 – 83.
2. Anand, A., Raj, A., Kohli, R., and Dr. Bibhu, V. (2016), Proposed Symmetric Key Cryptography Algorithm for Data Security, International Conference on Innovation and Challenges in Cyber Security, pp. 159 – 162.
3. Charru, Singh, P., and Rani, S. (2014), Improved Cryptography Algorithm to Enhanced Data Security, Internation Journal for Research in Applied Science and Engineering Technology, **2**, (IX), 242 – 247.
4. Chatterjee, D., Nath, J., Dasgupta, S., and Nath, A. (2011), A new Symmetric key Cryptography Algorithm using extended MSA method : DJSA symmetric key algorithm, International Conference on Communication System and Network Technologies, pp. 89 – 94.
5. Gupta, V., Singh, G., and Gupta, R. (2012), Advance cryptography algorithm for improving data security, International Journal of Advance Research in Computer Science and Software Engineering, **2**, (1).
6. Islam, M. N., Mia, M. M. H., Chowdhury, M. F. I., and Matin, M. A. (2008), Effect of Security Increment to Symmetric Data Encryption through AES Methodology, ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, pp. 291 – 294.
7. Jha, D. P., Kohli, R., and Gupta A., (2016), Proposed Encryption Algorithm for Data Security Using Matrix Properties, International Conference on Innovation and Challenges in Cyber Security, pp. 86 – 90.
8. Kessler, G. C (2019), An Overview of Cryptography, Available online at: http://www.garykessler.net/library/crypto.html
9. Menezes, A., Oorschot V. P, and Vanstone, S. (1996), Handbook of Applied Cryptography, CRC press, waterloo, canada, pp. 1 - 780
10. Nath, A., Ghosh, S., and Mallick, M. A., (2010), Symmetric Key Cryptography Using Random Key Generator,International Conference on SAM, **2**, 239 - 244.
11. Saranya, K., Mohanapriya, R., and Udhayan, J. (2014), A Review on Symmetric Key Encryption Techniques in Cryptography, International Journal of Science, Engineering and Technology Research, **3**, (3), 539 – 544.
12. Singh, P., and Shende, P. (2014). Symmetric Key Cryptography : Current Trends, International Journal of Computer Science and Mobile Computing, **3**, (12), 410 – 415.
13. Sohail, A. (2017). A new Symmetric Approach to Cryptography, International Journal of Technology and Research, **5**, (4), 73 – 77.