A Novel Key Generation for FMET

Fauzan Saeed[†], **Abdul Basit Abdul Qadir**[††], **Yar M.Mughal**[†††], **Mustafa Rashid**[††††]

[†]Faculty of Engineering, Usman Institute of Technology, Karachi, Pakistan
[††]MS/M.Phil, Institute of Business & Technology, Biztek, Karachi, Pakistan
[†††]H.O.D, Institute of Business & Technology, Biztek, Karachi, Pakistan
[††††]Network Department, Usman Institute of Technology, Karachi, Pakistan

Abstract:
Encryption plays a vital role in Data and Network Security and scores of algorithms have been introduced in this regard. The aim of this study is to enhance the strength of already proposed technique. The drawback in that technique was absence of Key generation which is essential for any Encryption Algorithm; here we have proposed a key generation mechanism and amalgamated it with the proposed technique [1] whose name we suggested as "Fauzan-Mustafa Encryption Technique (FMET)".

Keywords:
Network security, key generation mechanism, FMET, Fauzan-Mustafa encryption technique.

1. Introduction:

Encryption Algorithms are considered essential in any secure communication environment. Several encryption techniques are proposed in this regard, one of the recent techniques [1] talks about an algorithm that have surpassed DES, SDES, vigenere and playfair algorithm in terms of avalanche Effect, in [1] they compared their proposed idea with the above mentioned techniques and found that the proposed technique [1] have better results and Avalanche effect was in the region of 65% in contract to DES which has avalanche effect 54% but a drawback was observed in the proposed technique which was absence of key generation on which we are going to focus in this paper. [2] also discusses an algorithm that lacks proper key generation techniques. [2] and [3] has shown that average avalanche effect of blowfish algorithm is 28.71% approximately i.e. change of 19bits which is much lower than the algorithm proposed by Fauzan and Mustafa [1].

2. Amendments in Classical Encryption Techniques:

In this section, we will focus on some of the recent advancements in encryption techniques, these latest researches can be further molded and new improvements can be made. Following is a brief overview of some of the most recent evolutions in the field of cryptography.

1.1 Integration of Classical Encryption With Modern Technique:

In this technique [1], the amendments were being made in the classical encryption technique which were playfair and vigenere used in the algorithm being further enhanced by collaborating with modern encryption technique structure of DES and SDES. The algorithm begins by producing two sub keys from playfair and vigenere to induce more disguise. The plaintext is taken in 64-bit block size which is fixed [1]. Black box is introduced in the algorithm in which 64-bit block size is fed which is divided into 8 octets, these 8octets takes 8 bits each and these 8 bits are further divided into two parts, R.H and L.H. R.H is of 2bits and remaining 6bits are of L.H which is passed through 'special function', these 6bits are further divided into as first 2bits represents rows in the 'special function' values box and remaining 4bits represents column, the value is being selected with the special function selection method by rows and columns values. After the 'black box', the 64bit block size comes to create more confusion when they are divided into 8 octets where the octets further subdivides into two halves of R.H and L.H dividing 4 bits each. This algorithm provides more efficiency of complexity when all the 4bits of R.H are being combined together into forming a 32bits block at R.H and 4bits of all L.H are being combined together into L.H forming 32bits block, the L.H is XORED by R.H and completes the first cycle, this algorithm proposes N=3 cycles of repetitions.
The avalanche effect of this proposed method is much better then the classical encryption techniques and modern encryption techniques mentioned in [1]. The Avalanche Effect is 42bits, 65.6% as compared to DES (35bits, 54.6%), SDES (5bits, 7.8%), playfair (7bits, 10.9%), vigenere (2bits, 3.1%) [1].

1.2 Designing an Algorithm with High Avalanche Effect:

This encryption technique [2] also gives high avalanche effect. Including the same category of classical and modern encryption techniques, but comparison with

Manuscript received June 5, 2011
Manuscript revised June 20, 2011

blowfish technique is introduced in this paper by the researchers of this proposed technique. In this algorithm the key size is of 64bits or more [2]. The proposed technique got some amendments from the previous technique that the plaintext undergoes scrambling of bits after the generation of first sub key from playfair, after passing through vigenere which provides more disguise in the key the plaintext undergoes into S-BOX which is substitution box, this substitution box contains of 16x16 rows and column. The first part (4bits) is taken as the row and the second part (4bits) is taken as the column [2]. Now, the 64 bits block is being further divided into 8octets of 8bits which more further subdivides into 4bits each of R.H and L.H, these subdivided 4bits of R.H and L.H undergoes into the four 16bits block each as first 32bits of R.H goes into the first 16bit block and 32bits of L.H goes into the second 16bit block and same with 3rd and 4th 16bit block with the remaining 64bits subdivided into 4bits of R.H and L.H. The first 16bit block and last 16bit block perform XOR with each other and combining down to two blocks of 32bits each and L.H 32bits block is XORED with R.H 32bits block which completes the cycle = 1 by forming into one 64bit block. This loop is N=16 rounds.

45bits (70.31%) is the avalanche effect of this proposed encryption technique, and comparison mentioned below shows its strength. Playfair cipher (7bits, 10.9%), vigenere cipher (2bits, 3.1%), caeser cipher (1bit, 1.56%), DES (35bits, 54.6%), Blowfish (19bits, 28.71%) [2].

1.3 Modified Version of Playfair Cipher Using Linear Feedback Shift Register

Among amendments of classical encryption techniques, this encryption technique proposed a smart method by generating random numbers by LFSR (linear feedback shift register) for the mapping of cipher text generated by playfair algorithm. Linear Feedback Shift Register is a good candidate for generating random numbers because logical circuit variations are high [4], [5],[6],[7]. In this era, playfair cipher technique is outdated and easily breaks by brute force attack, that’s why amendments are necessary to enhance the classical encryption techniques, the working of this technique is first the playfair cipher algorithm implies without any changes and then LFSR comes into play, in this encryption technique [4], ‘5’ connections have been proposed with XOR operation implies between these connections except between 3 and 4, this LFSR operation is being done to generate random numbers which would map the cipher text generated by playfair algorithm. When the random numbers are generated through iterations, they are being set diagonally 5x5 in the table as same by playfair algorithm and these randomly generated numbers are then placed in the playfair generated cipher text table mapping up the cipher text with the randomly generated numbers. The advantage of LFSR are many and one of them is that it generates random numbers every time the cycle is started, so no such numbers could predict the mapping of cipher character. This method doesn’t increase the size of cipher text [4]. This encryption technique is quite efficient and easily implementable upon hardware and software.

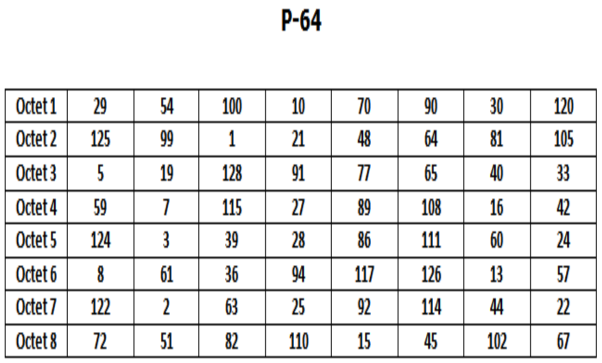
3. Drawbacks:

In this section, we will focus on proposed technique by Fauzan and Mustafa [1] which has proven itself when compared with algorithms like DES, SDES, vigenere, playfair. It was an attempt to improve classical encryption technique, but there is a drawback in the paper [1][2]. [1],[2] discusses encryption methodologies but not effective key generation has yet been proposed, as we know that key plays a critical role in any proper encryption algorithm, the more a key is secure the better an algorithm is, this is a major drawback which we identified in our present study.

4. Proposed Key Generation Technique:

Key generation is the process of generating keys for cryptography [8]. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted [8]. In the general life, key plays an important role, such as for entering house you need a key, for starting your car, you also need a key and in technical language we keep a secret key which is also called password for accessing our computers, email accounts, bank accounts, etc. Key is a major factor of accessing anything. And without an strong key or password, its an invitation for the hackers to attack and crack easily. This what we have analyzed in [1] and [2] that encryption algorithm is strong, giving high avalanche effect but no key generation, and when there is no key generation, its an call for hackers to attack. Basically, generation of key produces more and more confusion for the hacker to guess and crack the key, and this is the challenge we propose of key generation mechanism. The key generation mechanism is proposed in connection to the already proposed encryption technique by FMET [1]. In our proposed key generation mechanism the length of the key is 64bits, when the Key is input as you can see in figure1, it is character left shifted-4 twice, L.H and R.H is assembled which is of 128bits now. hence this will yield Key 1. After generating Key 1, It is again character leftshift-4 to yield Key 2. Now, we will convert character into bits and these bits will be fed to permutation table 64 (P-64). This permutation table was generated to induce as much confusion as possible in the key, the overall structure of this permutation table can be seen below:

Table 1:Depicting permutation table 64

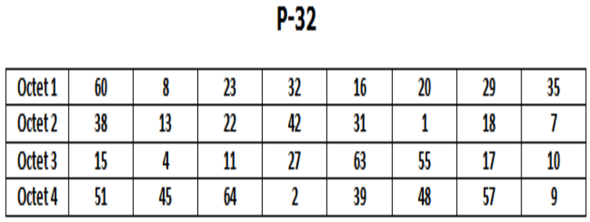


P-64

Octet 1	29	54	100	10	70	90	30	120
Octet 2	125	99	1	21	48	64	81	105
Octet 3	5	19	128	91	77	65	40	33
Octet 4	59	7	115	27	89	108	16	42
Octet 5	124	3	39	28	86	111	60	24
Octet 6	8	61	36	94	117	126	13	57
Octet 7	122	2	63	25	92	114	44	22
Octet 8	72	51	82	110	15	45	102	67

The 64bits are being divided into L.H and R.H of 32bits each. L.H is XORED with R.H and then R.H is XORED with the output of XORED L.H. After the completion of XOR operations, the 32bits of each L.H and R.H forms 64bits. These 64bits will now go into our permutation table 32 (P 32) , the output of which will give us our subkey3.

Table 2: Depicting permutation table 32

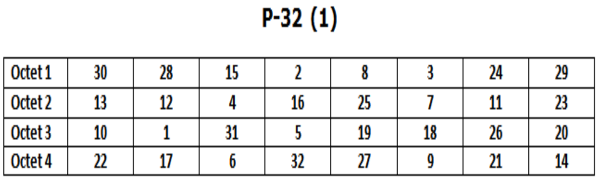


P-32

Octet 1	60	8	23	32	16	20	29	35
Octet 2	38	13	22	42	31	1	18	7
Octet 3	15	4	11	27	63	55	17	10
Octet 4	51	45	64	2	39	48	57	9

The 32bits of subkey3 is further divided into L.H and R.H of 16bits each, which are both leftshift-4 again, after left shift the two ends are joined together to constitute 32bits, these 32bits will now pass through our permutation table 32-1 (P 32-1).

Table 3: Depicting permutation table 32-1



P-32 (1)

Octet 1	30	28	15	2	8	3	24	29
Octet 2	13	12	4	16	25	7	11	23
Octet 3	10	1	31	5	19	18	26	20
Octet 4	22	17	6	32	27	9	21	14

and L.H is XORED by R.H, and R.H is XORED by L.H which generates subkey 4. For the generation of subkey 5, subkey 4 is divided into L.H and R.H of 16bits each for the purpose of leftshift-4 which is done, then the result goes into permutation table 32-1 (P 32-1) and L.H is XORED by R.H which generates subkey 5 of 32bits.

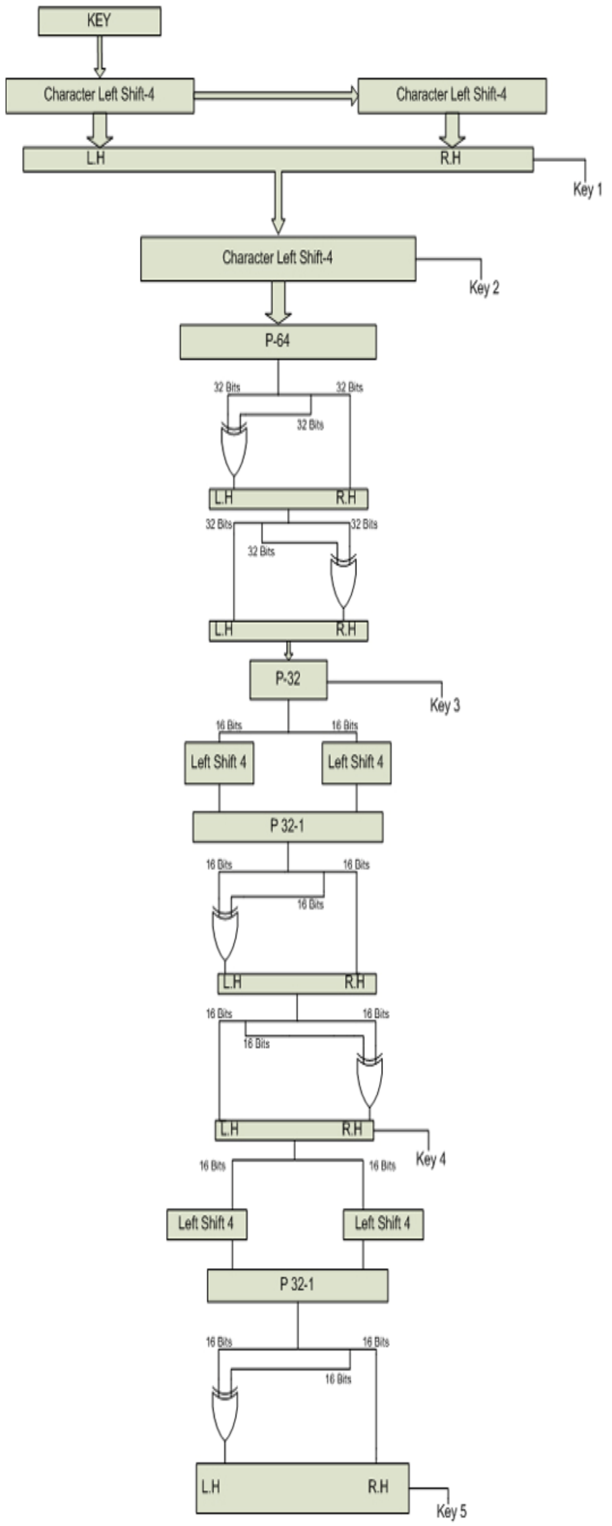


Figure1: Proposed Key Generation Mechanism

5. Integrating Key Generation with FMET:

The proposed key generation mechanism fulfills the weakness in the FMET algorithm [1] which has no key generation mechanism, by proposing this key generation mechanism the FMET [1] would get stronger in encryption and complex for the hacker to crack or guess the key. Without a key, the algorithm would produce no useful result [9]. The Figure 2 shows how the proposed key generation mechanism would integrate with the FMET algorithm [1]. According FMET algorithm, we have proposed generation of 5 keys. Key 1 undergoes playfair and Key 2 undergoes vigenere, whereas Key 3 is XORED with the L.H of encryption algorithm and remaining cycles are completed along with the keys generation, such as the FMET [1] is N=3 cycles, so the subkey4 and subkey5 completes the cycle. The key generation mechanism enhances the FMET [1] algorithm as there was no key generation mechanism before, not even in [2]. By generation of keys the hackers would be in complexity of guessing the key.

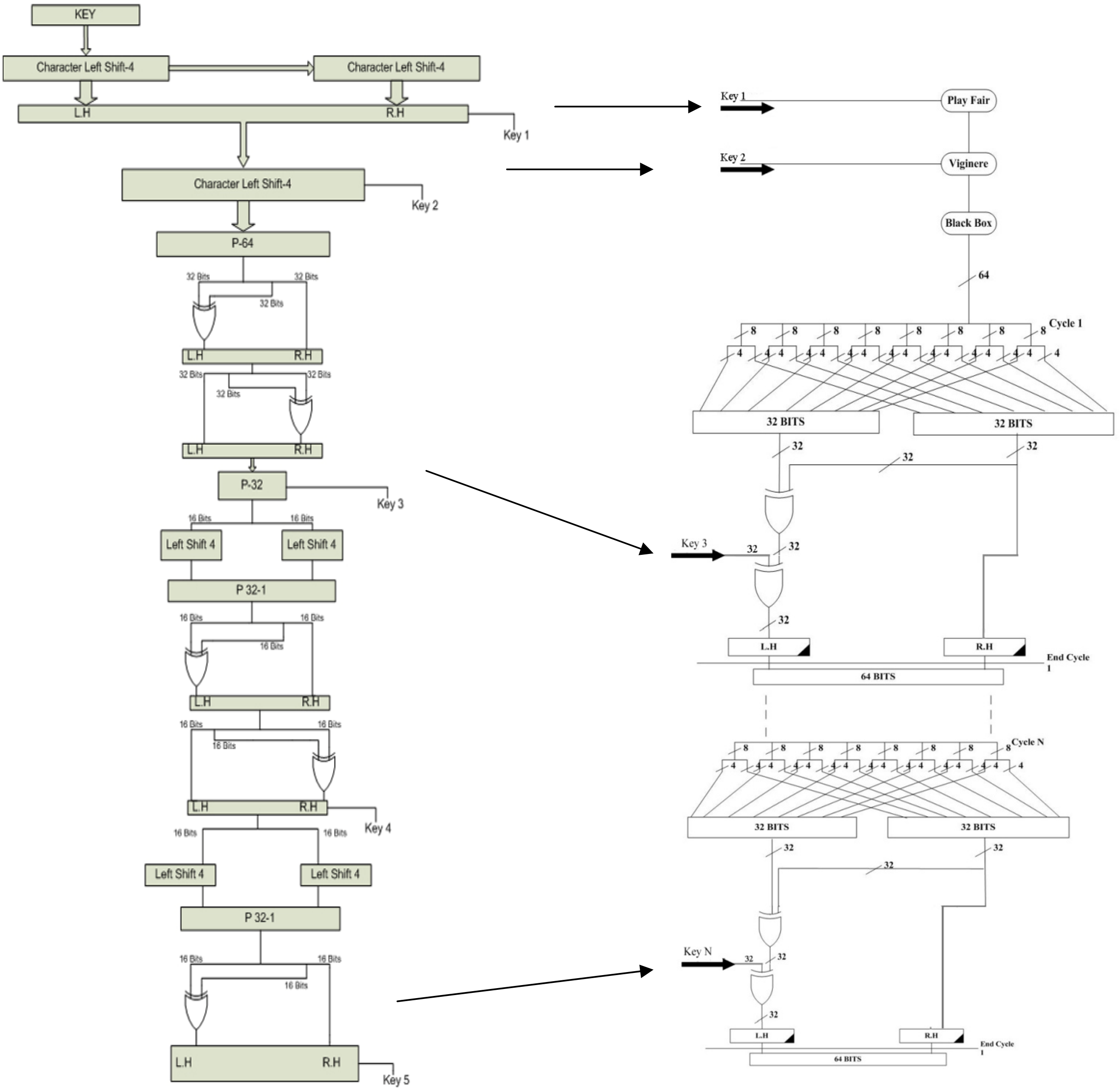


Figure2: Proposed Key Generation Mechanism showing how our key generation will interact with the FMET Algorithm[1].

A practical and secure crypto system needs keys that cannot be guessed [10].There should be no way for an outsider to predict what keys are being used, or even to guess approximately which keys might be used [10].

6. Subkeys:

Now, In this section we will discuss the subkey that were generated, here we will compare the subkey in order to see if they are different from each other or not. It is essential that the subkeys should be different from to some extent because if we use the same key in every round it wont bring any change in the output, for this reason we will compare our subkeys. The result comparison is given as follow :

6.1 Difference in Subkeys:

KEY: **BASITWON**

SubKey 3:
0 0 1 1 0 0 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 1 1 1 0 1 1 0 0 0 0 1
Subkey 4:
0 1 1 1 1 1 0 1 1 1 1 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 1 1 0 1 1 1
Subkey 5:
0 0 0 0 0 0 0 1 0 1 0 1 1 1 1 0 1 1 1 1 0 0 1 0 0 0 1 0 1 0 0 1

6.2 Comparison between Subkey3 and Subkey4:

Comparison:
00110001101001100101111101100001 Subkey3
01111101111001111110000000110111 Subkey4

Difference:
As it can be seen from the above comparison that the difference between subkey3 and subkey4 is of 16bits below we are going to calculate the percentage change between the above two mention keys.
Percentage= no.of change bits/total no.of bits x 100
Percentage= 16/32 x 100
Percentage= 50%

6.3 Comparison between Subkey 4 and Subkey 5:

Comparison:
01111101111001111110000000110111 Subkey 4
00000001010111101111001000101001 Subkey 5

Difference:
Again it is obvious from the above comparison where we compared subkey4 and subkey5 the difference was of 16bits below we are going to calculate the percentage change between the above two mentioned keys.

Percentage= no.of change bits/total no.of bits x 100
Percentage= 16/32 x 100
Percentage= 50%

6.4 Comparison between Subkey3 and Subkey5:

Comparison:
00110001101001100101111101100001 Subkey3
00000001010111101111001000101001 Subkey5

Difference:
Here we compared subkey3 with subkey5 and analyzed the difference between the two.
Percentage= no.of change bits/total no.of bits x 100
Percentage= 14/32 x 100
Percentage= 43.75 %
From the above comparison results we can see that there is an average difference of 47.91% between the three subkeys where the difference between subkey 3 and subkey 4 was 16bits, same was the difference between subkey4 and subkey5 and finally, a difference of 14bits was seen between subkey3 and subkey5 which gave an average difference of 47.91%.

7. Conclusion:

From the above proposed key generation mechanism, We conclude that it enhances the integrity of [1] which has no key generation mechanism mentioned before. Upon the basis of [1], we propose key generation mechanism and enhance [1] further, because the major feature of any algorithm is Key. And the key generation mechanism can also be used for [2] as the key generation is missing in [2] algorithm. The difference between the subkeys were sufficient enough as there is no other key generation mechanism yet proposed for this algorithm.

8. Future Work:

In future we would be focusing on improvement in playfair portion by using randomly generated table; similarly key generation can also be proposed for similar new techniques and algorithms.

Acknowledgement:

We would like to thank the Management and Administration of Biztek and Usman Institute of Technology for their support. We would like to thanks the Dean of Biztek for his support and especially Director of Usman Institute of Technology Dr.Waseem Akhtar who is always supportive towards young researchers and encourages research culture and Engr.Mohammad Arif, for his moral support & advises.

References:

[1] Fauzan Saeed and Mustafa Rashid, "Integrating Classical Encryption with Modern Technique", IJCSNS Vol. 10 No.5, May 2010.

[2] Sriram Ramanujam and Marimuthu Karuppiah, "Designing an algorithm with high Avalanche Effect", IJCSNS, VOL.11 No.1, January 2011.

[3] Janan Ateya Mahdi, "Design and Implementation of Proposed B-R Encryption Algorithm", IJCCCSE, Vol. 209, No.1.2009.

[4] Packirisamy Murali and Gandhidoss Senthilkumar, Modified Version of Playfair Cipher using Linear Feedback Shift Register, IJCSNS, VOL.8 No.12, December 2008

[5] Schnier B."Applied cryptography: protocols", algorithms and source code in C. New York: John Wiley and sons; 1996.

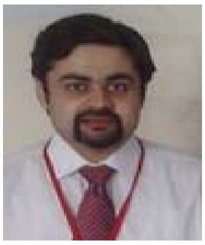
[6] Menezes AJ, Oorschot PCV , Vanstone SA ."Handbook of applied cryptography" . Boca Raton , Florida , USA : CRC Press ; 1997.

[7] Johannes A.Buchmann . Introduction to Cryptography, Second Edition 2001, Springer –Verlag NY, LLC

[8] http://en.wikipedia.org/wiki/Key_generation

[9] http://en.wikipedia.org/wiki/Key_%28cryptography%29

[10] Richard E.smith, "Internet Cryptography"



Fauzan Saeed Working as Assistant Professor in Usman Institute of Technology, completed his masters in Mobile computing after which he acquired another masters degree in computer Networks presently doing PhD from Hamdard University ,he has 9 research publication to his name, his field of expertise include Network security and Mobile communications presently supervising MS thesis of Abdul Basit.

Abdul Basit Abdul Qadir received BCS(HONS)degree, in 2006 from Institute of Business & Technology-Biztek, Karachi, Pakistan. Now, he is currently doing his thesis in MS/M.Phil upon which this research work is based, from Institute of Business & Technology-Biztek. As a source of interest, he is looking for more research works and interested in doing Ph.D.

Yar M.Mughal Received degree of MS in computer engineering from Mid Sweden University, Sweden in 2009.Presently he is Head of Department and Internal Supervisor of Abdul Basit in Institute of Business & Technology-Biztek'

Mustafa Rashid Received degree of BS (Computer Science) in 2008. Doing MS in Computer Networks and Communications. He did Microsoft (Microsoft Certified System Engineer) and Juniper certifications, presently working as Assistant System Administrator in Usman Institute of Technology.