Volume 2, Issue 2
April 2013

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Performance Evaluation of Symmetric Cryptography Algorithms: A Survey

[1]Mohsin Khan, [2] Sadaf Hussain, [3]Malik Imran

[1, 2] Department of Computing & Technology, IQRA University, Islamabad

[3] Department of Computing & Technology, ABASYN University, Islamabad

E-mail: [1]mohsin_btn@yahoo.com, [2]sadaf_malikawan2012@yahoo.com, [3]mlk.imran88@gmail.com,

ABSTRACT

Network and Internet applications are growing very fast, since the need to secure these applications are very fast. For this purpose cryptography algorithms (symmetric & Asymmetric) are proposed. These algorithms consume a significant amount of computing resources like CPU processing time, Memory, Battery power, and throughput. The performances of cryptography algorithms are different in different environments. Different cryptography algorithm faced different issues like battery consumption, CPU Processing Speed, and Memory according to their Algorithm and key generation process. Here in this survey paper we discuss about the symmetric cryptographic algorithms and their performance in context of power consumption issues, Memory and CPU processing time.

1. INTRODUCTION

In new era of information technology, information security is a big issue. For information (data) to be sent from sender to user, it is more important that to give right information to right people at a right time. Cryptography converts the message into a non readable format and sends the message over an unsecure channel. The unauthorized person will try to read the unreadable message but it is not easier. "Encryption is a process of transferring plaintext information to a form called cipher text using an algorithm called cipher which is readable only by whom who has special knowledge called encryption key" [1]. For encryption two techniques are used like symmetric algorithms, asymmetric algorithm. In symmetric encryption there is single key called secret key. Symmetric encryption is used best for small number of secure communication, and the transmission of secret key is a major problem, while in a Symmetric cryptography there are two keys used: one is called public key second is called private key. Public key are used for encryption while private key are used for decryption.

For symmetric encryption there are five requirements: plain text, cipher text, encryption algorithm, decryption algorithm, and secret key.

a. **Plain Text:** the original message which the sender wants to send to receiver is called the plain text. For example shahab wants to sends send message to mohsin "Hello friend! How are you". In this example "Hello friend! How are you" is a plain text.
b. **Cipher Text:** the plain text is converting to cipher text through encryption key/ algorithm. The cipher text is non understandable by anyone rather authorized person. In the previous example "Hello friend! How are you" is plain text and corresponding cipher text is "Ajd672#@91ukl8*^5%".
c. **Encryption Algorithm:** The process of converting plain text to cipher text are called encryption algorithm. Through cryptography a confidential message are send at unreliable channel. Encryption is done through secret key.

Volume 2, Issue 2
April 2013

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

d. Decryption Algorithm: Decryption is a process of converting cipher text to plain text. Decryption is done through same secret key.

e. Secret key: Secret key is the main requirement of symmetric key. Secret key is used for encryption and decryption. The security of secret key is more important as if intruder knows the key he/she may analyze the plain text.

Algorithms falls in symmetric encryption are AES (Rijndael), DES, 3DES, RC2, Blow fish, and RC6. There are five key terms in encryption: Plain text, cipher text, encryption algorithm, decryption algorithm, and secret key [2] [3].

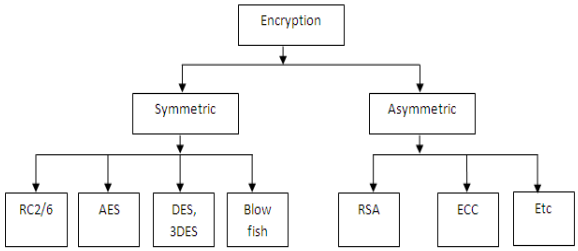


Fig 1: Cryptography Diagram

In the next diagram I will show the process of symmetric encryption algorithm. The diagram shows the equation of encryption and decryption. In encryption a cipher text y is achieved through secret key K, and Message M. decryption equation that the plain text M is derived back from a cipher text Y through secret key K.

The remaining paper is present like this: in section (2) Description of some Symmetric Encryption Algorithm is presented. In section (3) some work done on Performance Evaluation presented, and in section (4) the final conclusion of paper is presented.

This paper presents the survey of symmetric cryptographic algorithms and their performance based on algorithm and key generation process and length.

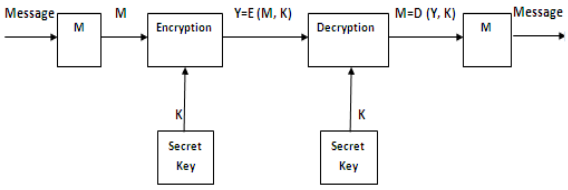


Fig 2: Symmetric Encryption Algorithm Process

2. DESCRIPTION

This section presents the description of some symmetric encryption algorithms like AES, DES, Blowfish, Modified DES, and Modified Blowfish, and their strengths and weaknesses.

a. DES (Data Encryption Standard) Algorithm

DES was the first encryption standard designed in 1973 and was recommended by NIST (National Institute of Standards and Technology) to be the most efficient method for encryption of data in 1976. This was the most widely used standard all across the world. The DES Algorithm is defined in the paper [4]. It is a block cipher which encrypts 64 bit plaintext at a time and uses 56 bit key. This was based on symmetric key algorithm which means that the same key will be used for both encryption and decryption. DES can operate in CBC, ECB, CFB and OFB modes. DES has 16 rounds which mean a total of 16 processing steps are being applied on the input plaintext to produce cipher text. First, 64 bit data is passed through the initial permutation phase and then 16 rounds of processing takes place and finally the last step of final permutation is carried out on the input plain text which results in 64 bit cipher text. The algorithm is shown in the below diagram:

Volume 2, Issue 2
April 2013

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

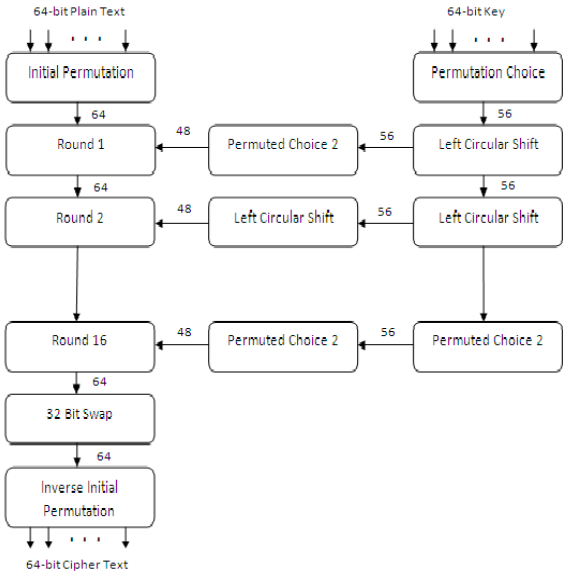


Fig 3: DES Algorithm

The drawback of this algorithm is that it can be easily prone to Brute Force Attack in which the hacker attempts to break the key by applying all possible combinations. In DES there are only 2^56 possible combinations which are quite easy to crack. So DES is not so secure.

b. AES (Advanced Encryption Standard) Algorithm

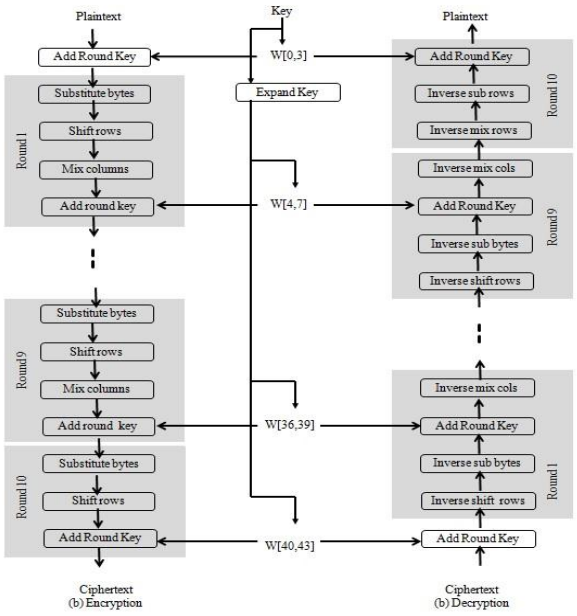
The US National Institute of Standards and Technology (NIST) recommended the use of Advanced Encryption Standard to replace Data Encryption Standard in 1998. AES has defined in paper [5]. AES is a variable bit block cipher and uses variable key length of 128, 192 and 256 bits. If both the block length and key length are 128 bits, AES will perform 9 processing rounds. If the block and key are of 192 bits, AES performs 11 processing rounds. If the block and key are of length 256 bits then it performs 13 processing rounds.
Each processing round involves four steps:

- Substitute bytes – Uses an S-box to perform a byte by byte substitution of the block,
- Shift rows – A simple permutation,
- Mix column – A substitution method where data in each column from the shift row step is multiplied by the algorithm's matrix and
- Add round key – The key for the processing round is XOR with the data.

The AES algorithm diagram is shown in Fig 4 in the next page. The figure shows all the processing of AES Algorithm.
AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. The key length is variable sense the processing speed and memory usage is variable in different environment, due to flexible key length it could be used in both higher secure and for less secure environments.

c. Blowfish Algorithm

Bruce Schneier designed Blowfish algorithm in 1993. The algorithm description is defined in the Bruce Schneier URL [6]. Blowfish is a 64 bit block cipher with variable length key from 32 bit (4 bytes) to 448 bits (56 bytes). The advantage of this algorithm is that it is highly secure and has not been cracked yet. It is suitable and efficient for hardware implementation.



The algorithm has two parts- Key expansion and Data Encryption. The key expansion step converts

Volume 2, Issue 2
April 2013

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

448 bit key into 4168 bytes. A P-array of size 18 and four S-boxes whose size is 256 each of which are initialized to hexadecimal digits of π. XOR each entry in P array and S boxes with 32 bits of the key.
There are total 16 rounds of data encryption. In each round a 32 bit subkey is XORed with leftmost 32 bits of plaintext and the result is then passed to the F function of Blowfish. This result becomes rightmost 32 bits for the next round and the output of F function is XORed with the original rightmost 32 bits of plaintext becomes leftmost 32 bits for the next round and so on.

Fig 4: AES Processing Diagram

Blowfish Processing	Blowfish Algorithm

• Initialize P array and S boxes with Hexadecimal digits of Pi.
• XOR P-array with the key bits (i.e., P1 XOR (first 32 bits of key), P2 XOR (second 32 bits of key)…
• Use the above method to encrypt the all-zero string.
• This new output is P1 and P2.
• Encrypt the new P1 and P2 with the modified subkeys.
• This new output is now P3 and P4.
• Repeat the above steps until we get all the elements of P array i.e P1, P2….
	• Divide 64-bits into two 32-bit halves: XL, XR
	• For i = 1 to 16
	  ○ XL = XL XOR Pi
	  ○ XR=F(XL) XOR XR
	  ○ Swap XL and XR
	• Swap XL and XR (Undo the last swap)
	• XR=XR XOR P17
	• XL = XL XOR P18
	• Concatenate XL and XR

Table 1: Blowfish Process & Algorithm

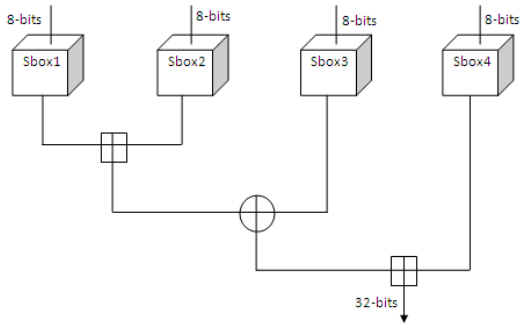


Fig 5: F Function diagram of Blowfish

The key of the Blowfish algorithm is 448 bits, so it requires 2^448 combinations to examine all keys. The advantage of blowfish algorithm is that it is simple to implement since all operations carried out are XOR and addition. Moreover the speed of

Below table 1 shows the blowfish process and algorithm in a pseudo code manner.

The F function is the distinguishing feature of Blowfish and is applied as follows .First Divide XL (32 Bits) into four 8-bit quarters: a, b, c, and d. Then apply the formula.

$$F(XL) = \{(S1[a] + S2[b])\ S3[c]\} + S4[d])\}$$

Where + means addition modulo 2^32, and means exclusive OR and S1, S2, S3, S4 are four substitution boxes.

encryption and decryption are also known to be faster than other popular existing algorithms. Moreover the blowfish algorithm is still not cracked as the key size is high. The processing speed is less than DES and AES.

d. Modified Blowfish Algorithm

A modified Blowfish algorithm is presented in [7] by Monika Agrawal and Paradeep Mashra in 2012. They modify the blowfish algorithm with a random number Rn, the remaining processing is same as blowfish.

Where Rn = rand ()

Rand is a function in MATLAB, C++, and java which creates a random number of any length but here it is restricted from 0 to 65535, equal to 2^16. Now introduced a flag, the flag value will be 0 or 1, initially it would be 0, and the random number would

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

be 16 bits from LSB to MSB. If in the string of random number a 0 is encountered the flag will be reset to 1. All the 16 bits represent the 16 rounds of blowfish. The flag value 1 will decide the f function process is required. The modified blowfish algorithm is discussed below:

- Divide X=64 bits into two 32-bit halves: XL, XR.
- Generate a random number Rn (from 0 to 65535) and set the variable Flag to 0.Represent Rn in form of 16 bit binary string say str.
- For i=1 to 16
    - If str[i] == '0'
        - Set Flag=1
    - If Flag == '1'
        - XL = XL xor Pi
        - XR= XL xor XR
    - Else
        - XL = XL xor Pi
        - XR=F(XL) xor XR
    - Swap XL and XR
- Swap XL and XR (Undo the last swap)
- XR=XR xor P17
- XL = XL xor P18
- Concatenate XL and XR

Modified blowfish algorithm uses the concept of random number and flags, and flags decide where f function process is required or not. Since the number of f function calls is reduced which increase the CPU processing time, decrease memory usage, and increased the throughput. The second advantage of modified blowfish algorithm is increased in security, as the intruder does not predict the random number and the location of 0. So it is unpredictable for intruder to know, in which round F function is working. This increased the security of the algorithm. The important thing is that for same length plain text, each time the enciphering time will be different as each time different random number is generated each time.

e. Modified DES Algorithm using Fuse Data Technique

DES algorithm is modified by Al Hamami et al in [8]. They present Fuse DES with Blowfish and Genetic Algorithm (GA). DES has a disadvantage of shortest key, since it is not more secure. On the other hand Blowfish is a fastest algorithm with a high security as used 16 rounds of F function. The Fused DES algorithm is presented to overcome the security leaks of DES algorithm. The modified DES algorithm has a 64-bits plaintext on one end and a 64-bit cipher text on the other end. The algorithm uses 2 subkeys: left subkey and right subkey. Left subkey is a 768 bit length and 16 blocks of 48 bits called Pi through both 16^{th} round left subkey is generated. The steps to create 16^{th} left subkey are:

- First initialized the 768-bits and 16 P-array of 48-bits with initial keys. These both have chosen randomly in a hexadecimal fashion.
- Convert Hexadecimal to binary
- XOR the first 48-bits of initial key with 48-bits P-array (P1), which generates the first left subkey in round 1.
- XOR the second 48-bits of initial key with 48-bits P-array (P2), which generates the second left subkey in round 2.
- XOR the last 48-bits of initial key with 48-bits P-array (P16), which generates the 16^{th} left subkey in round 16.

Right Key has initial key 100 of 48-bits taken as initial generation for genetic algorithm. By applying the proposed GA, we get best 16-bits of 48-bits to be the right sub-keys. The right subkey generation process is below:

- Take 100 seeds each of 48 bits
- Find the hamming distance of keys with known week keys
- Do the two points crossover on the randomly selected crossover points
- A mutation operator can prevent any single bit from converging to a value through the entire population and, more important, it can prevent the population from converging and stagnating at any local optima
- Probability of crossover, PC = 1, Probability of mutation, PM = 0.001 (the parameter will be used in a mutation operation)
- Continue until obtain the optimized key as a master key

The Fused DES algorithm process is shown in the Figure 7. The F function process is shown in fig 8.

Volume 2, Issue 2
April 2013

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

This is more secure encryption algorithm as it uses two subkeys left and right. With the help of genetic algorithm the key become stronger, since this is a secure method for symmetric encryption. Previous algorithms DES, and Blowfish uses only one key of length n, since a brute force attack can easily

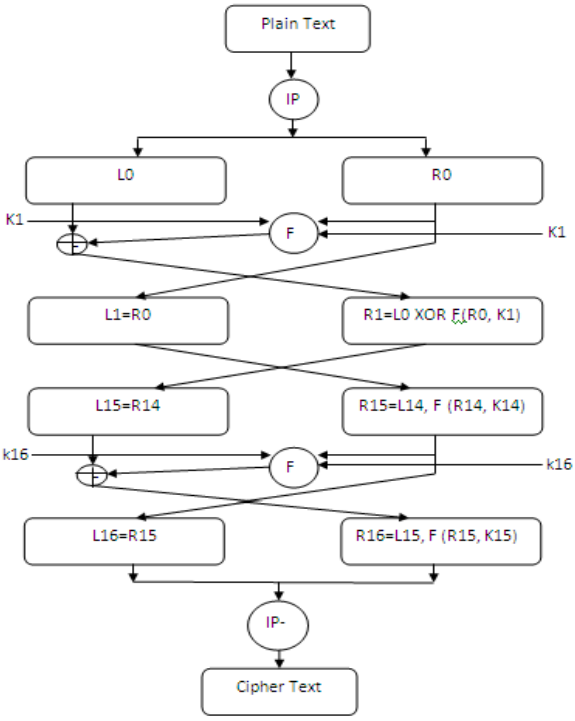


Fig 7: Fused DES Algorithm

Substitute key with 2^n substitutions. But this algorithm use 2 keys of length n and m, since cryptanalysis permutation is double now. But as used 16 rounds with F functions, the CPU time is increased, memory usage increased and due to slow processing the throughput also decreased as compared to DES. This is more secure encryption algorithm as it uses two subkeys left and right. With the help of genetic algorithm the key become stronger, since this is a secure method for symmetric encryption. Previous algorithms DES, and Blowfish uses only one key of length n, since a brute force attack can easily substitute key with 2^n substitutions. But this algorithm use 2 keys of length n and m, since cryptanalysis permutation is double now. But as used 16 rounds with F functions, the CPU time is increased, memory usage increased and due to slow processing the throughput also decreased as compared to DES.

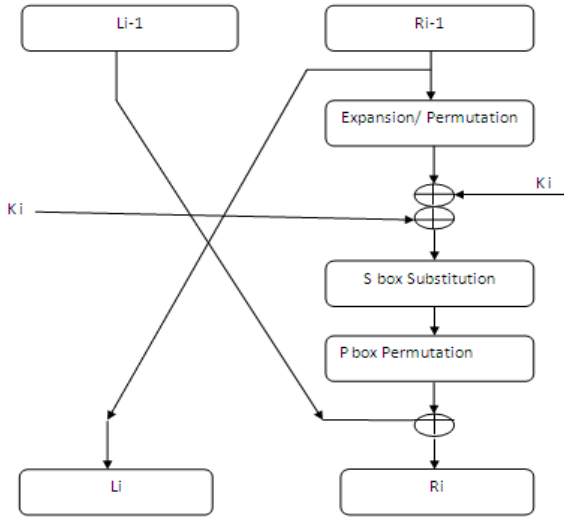


Fig 8: F Function of one round of Fused DES

3. WORK DONE ON PERFORMANCE EVALUATION

Researchers' Works on the performance of symmetric encryption. Hatem Mohamed and group work on symmetric encryption algorithm in 2006, and 2010. They works on 6 algorithms AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. The performance criteria they kept are CPU processing time, Memory consumption and Power Consumption. There results shows that at varying packet size blowfish has better performance, RC2 has poor performance than all, 3DES has still lower performance than DES [9]. Monika Agarwal in his paper [10] defined DES, 3DES, AES, and blowfish algorithms and their complexity and shows that 3DES is more complex. Agarwal also in her paper [7] discuss the performance of a modified blowfish algorithms, and conclude that it has more secure ant take less processing timing. A new Modified RC4 algorithm is discussed in [11]. They discuss the weaknesses of the RC4 key and improve them, then compare it with RC4 original which has better performance than RC4. A new version of DES proposed by Hamami et al [8] a fuse DES-Blowfish is presented. He increased the key space of DES and

Blowfish through GA, and shows better results for than Blowfish and DES.

4. CONCLUSION

In This paper we have been presented a survey on the Symmetric Encryption Algorithms. In the symmetric encryption algorithms one secret key is used. Since the symmetric key algorithms are more prior to attacks and provides less security than asymmetric algorithms. But the processing time, throughput, and memory usage of this algorithms are very less. We discussed about the DES, AES, Blowfish, Modified Blowfish, and Fused DES Algorithms in this paper. The more secure algorithm is blowfish. In modified blowfish the security has been increased while the processing of is decreased through random numbers. DES is a less secure algorithm which used 56 bits key, and a brute force easily regenerates key using 2^56 imaginations. The drawback is solved in Fused DES through GA Technique and Blowfish key generation.

5. FUTURE WORK

This is a survey paper. We discussed the merits and demerits without facts. In the next paper we In Shaha ALLAH discussed all these algorithms with graphs through implementation, and proposed our new Symmetric Encryption Algorithm.

Refferences

[1] "Encryption White Paper," 2010.

[2] Paradep Sharma Monika Agrawal, "A Comparative Survey on Symmetric Key Encryption Techniques," International Journal on Computer Science and Engineering (IJCSE), vol. 4, no. 5, pp. 877-882, 2012.

[3] William Stallings, Cryptography And Network Security 4Th Edition.: Prentice Hall, November 18, 2006.

[4] D. Coppersmith, "The data encryption standard (DES) and its strength against attacks," IBM Journal of Research and Development, pp. 243-250, May 1994.

[5] V. Rijmen J. Daemen, "Rijndael: The advanced encryption standard," Dr. Dobb's Journal, pp. 137-139, March 2001.

[6] Bruce Schneier. (2008, October) The Blowfish Encryption Algorithm. [Online]. http://www.schneier.com/blowfish.html

[7] Monika Agrawal and Pradeep Mishra, "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm," International Journal of Engineering and Advanced Technology (IJEAT), vol. 1, no. 6, pp. 79 - 83, August 2012.

[8] Alaa H. AL-Hamami, Mohammad A. AL-Hamami, and Soukaena H. Hashem, "A proposed Modified Data Encryption Standard algorithm by Using Fusing Data Technique," World of Computer Science and Information Technology Journal (WCSIT), vol. 1, No. 3, pp. 88-91, 2011.

[9] Hatem Mohamed Abdual Kader, Mohiy Mohamed Hadhoud Diaa Salama Abd Elminaam, "Evaluating The Performance of Symmetric Encryption Algorithm," International Journal of Network Security, vol. 10, no.3, pp. 213-219, May 12 2010.

[10] Monika Agrawal and Pradeep Mishra, "A Comparative Survey on Symmetric Key Encryption Techniques," International Journal on Computer Science and Engineering (IJCSE), vol. 4 no. 05, pp. 877 - 882, May 2012.

[11] Lae Lae KhineLae Lae Khine, "A New Variant of RC4 Stream Cipher," World Academy of Science, Engineering and Technology, pp. 958-961, 2009.

[12] Diaa Salma and Hateem Muhammad, "Evaluating The Performance of Symmetric Encryption Algorithms," International Journal of Network Security, vol. 10, no. 3, pp. 213-219,

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

2010.

AUTHOR PROFILES

Mohsin Khan: is a student of MS (Telecommunication & Networking) at IQRA University Islamabad. He got his BS (Telecommunication & Networking) Degree from COMSATS, Institute of Information Technology Abbottabad in July 2011. He is a research student at IQRA University Islamabad. He is also working as a LAB Engineer at IQRA University Islamabad from 10th Sep, 2012.

Sadaf Hussain: is a student of MS (Computer Science) at IQRA University Islamabad. She got her BS (Computer Science) Degree from Allama Iqbal Open University Islamabad in 2009. She is a research student at IQRA University Islamabad. Now she is working as a Computer Programmer at Rawalpindi Institute of Cardiology from May 2011.

Malik Imran: is a student of MS (Telecommunication & Networking) at ABASYN University Islamabad. He got his BS (Computer Engineering) Degree from COMSATS, Institute of Information Technology Abbottabad in July 2011. He is a research student at ABASYN University Islamabad.

Aihab Khan: working as Assistant Professor at IQRA University Islamabad from Sep 2011. He is working as a research coordinator at IQRA University Islamabad also.