Integrating Classical Encryption with Modern Technique

Fauzan Saeed[†], Mustafa Rashid[††]

[†]Faculty of Engineering, Usman Institute of Technology, Karachi, Pakistan
[††]Network Department, Usman Institute of Technology, Karachi, Pakistan

Abstract:
Alphabetical ciphers are being used since centuries for inducing confusion in messages, but there are some drawbacks that are associated with Classical alphabetic techniques like concealment of key and plaintext. Here in this paper we will suggest an encryption technique that is a blend of both classical encryption as well as modern technique, this hybrid technique will be superior in terms of security than average Classical ciphers.

Key words:
Network security, Playfair cipher, viginere cipher, Classical encryption, Modern Encryption

1. Introduction:

Cipher plays a significant role in camouflaging the true nature of data; this is achieved by inducing the factor of confusion through a series of shift and other mathematical functions. In the field of cryptography there exist several techniques for encryption/decryption these techniques can be generally classified in to two major groups Conventional and Public key Cryptography, Conventional encryption is marked by its usage of single key for both the process of encryption and decryption whereas in public key cryptography separate keys are used. Further on conventional techniques are further broken in to Classical and Modern techniques. In this paper we have focused on the well known classical techniques the aim was to induce some strength to these classical encryptions for that purpose we blended classical encryption with the structure of modern techniques like S-DES our proposed method showed that it is better in terms of providing perplexity to any given text. In our experiments we took Playfair, Vigenere and Caesar cipher as representatives of Classical Techniques and Simplified DES and standard DES as examples of modern technique to give a clear view of how these ciphers are inter related a comprehensive hierarchal diagram can be seen below.

Public key cryptography is also an option when it comes to encryption but it require excessive communication and processing resources[8].
In next sections we will discuss some of the conventional methodologies after which we will come to our proposed technique and finally we will compare our proposal with some standard conventional encryption models and display the results.

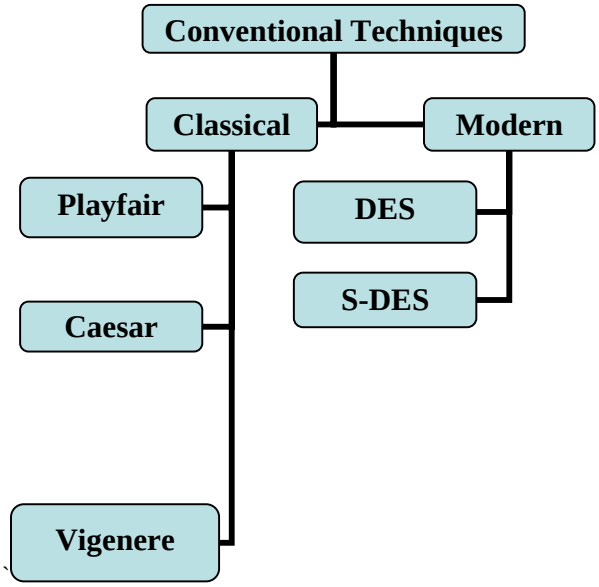

Fig1: Depicting some of the techniques of Classical and Modern encryption.

2. Classical Encryption:

Several encryption algorithms are available and used in information security [4, 5, 6] There are several algorithms that can be categorized as classical but out of many in this section we will be shedding some light on 3 such techniques:

i) Caesar Cipher:
ii) Vigenere Cipher
iii) Playfair Cipher

2.1 Caesar Cipher: it is a classical substitution cipher, and one of the simplest example of substitution cipher [9], which replaces the letter of alphabet with a letter that is 3 paces ahead of it [1], for example "ZULU" will be converted in to "CXOX" as one can see that such a

Manuscript received May 5, 2010
Manuscript revised May 20, 2010

cipher may be difficult to break if you are trying to solve it on paper and have no clue of the key, but it has no standing these days in the age of computers and technology and through brute force attack it can be easily broken because in the end there are only 25 possible options of key available.

2.2 Vigenere Cipher: This cipher when compared with Caesar gives some level of security with the introduction of a keyword; this key word is repeated to cover the length of the plain text that is to be encrypted example is shown below:

KEY: f a u z a n f a u z a n
P.T: c r y p t o g r a p h y
Cipher: H R S O T B L R U O H L

As we can see from above example that "fauzan" is our keyword and plain text is "cryptography" which was encrypted in to "HRSOTBLRUOHL" this was done using Vigenere table which contains alphabets in form of rows and columns left most column indicates keywords and top most row indicates plaintext and at the junction of two alphabetic letters resides our replacement and after individually transforming every letter we get an encrypted message.

2.3 Playfair Cipher: Another example of classical cipher is Playfair cipher that has a square of matrix of 5X5 alphabetic letters arranged in an appropriate manner [2]. We can select a key and place it in the matrix the remaining letters of English alphabet are then one by one placed in the matrix of Playfair cipher, the plain text is broken in to pairs and if a pair has same alphabet then they are separated by introducing a filler letter like 'x', other wise if the pair are different alphabetic letters and reside in the same row of matrix then each letter is replaced by the letter ahead of it. If the pair of letters are in same column of matrix then each letter is replaced by the letter below it, and when the pair of letters are neither in same column nor in same row then are they replaced by the letter in their row that resides at the intersection of paired letters.

3. Modern Techniques:

Several modern encryption techniques exist but here in this paper we will focus on two variants of Data Encryption Standard one is DES other is S-DES.

3.1 S-DES: simplified DES has a process of key generation instead of using key as it is for encryption and decryption the key generation process of S-DES generates 2 sub keys after processing the initial 10 bit input, it has 8 bit plaintext input the two sub keys are generated at both transmission and receiving ends the two keys are applied to 2 complex functions respectively, with the inclusion of initial permutation, expansion permutations expansions and s-boxes the security is substantial when compared with the classical techniques, S-DES gave some structure and formation to encryption techniques with step to step procedures for both encryption and decryption.

3.2 DES: DES enhances the structure of S-DES by increasing the key size from 10-bits to 64-bits out of which its affective length is 56-bits **[3].** 16 rounds are introduced with each round containing XOR, substitutions and permutations for 16 rounds 16 keys are generated each of 48-bits which strengthens the security of this algorithm further. in terms of processing DES is 3times faster than 3DES [7]. DES takes plain text in 64-bits of block these 64-bits are divided in to 32-bits each the right half of 32-bits goes through the expansion block which increases the bit count from 32 to 48-bits by reusing some bits after expansion block comes XOR operation with the sub-key which is also of 48-bits result of this operation is again of 48-bits these 48-bits now goes in to 8 S-boxes the 48-bits are divided in to 8 parts of 6-bits each going in to S-box1 to S-box8 , the overall result of S-box substitution is reduced from 48 to 32-bits which is then XOR with the left half of the initial plain text block to give a 32-bit result which is placed on right and the initial right half of the block is placed at left to get the 64-bit output of 1st round similarly this output of 1st round becomes input of the 2nd round and same procedure is pursued till the 16th round , after 16th round there is a 32-bit swap and finally the bits are placed in inverse permutation table to get the encrypted message reverse method is applied to yield the result.

4. Proposed technique:

Our proposed technique emphasizes on improving classical encryption techniques by integrating modern cipher with classical methods in our proposed idea we blended playfair and vigenere cipher with the structural aspects of DES and SDES, our methods to some extent deals with some of the drawbacks of classical techniques that includes usage of key as it is without inducing any confusion in the primary key we changed that by generating two sub-keys from the primary key, similarly the key size of proposed concept varies from 4character or 32bits to onwards it can be 64-bits ,128-bits and so on whereas on the other hand we have example of SDES and DES that have fixed key structure. The variation in key introduces the aspect of uncertainty which is a positive aspect when it comes to encryption, the plaintext

is taken in 64-bit block size which is fixed, in our amended technique we introduced a “Black Box” in which the 64-bit plaintext is divided in to two halves, left half has 2bits whereas right half has 6-bits these 6-bits are fed in to “special function” block where further these 6-bits are divided in to two halves first two bits represent the row whereas last four bits represent column by identifying rows and column we

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	55	58	57	61	51	59	56	48	54	62	52	60	44	53	57	50
1	39	42	37	36	41	46	45	44	47	34	33	38	43	35	32	40
2	23	22	21	24	31	30	27	16	19	20	29	28	18	26	25	17
3	7	10	5	4	9	14	13	12	15	2	1	6	11	3	0	8

Can select the corresponding values from **table 1** shown above

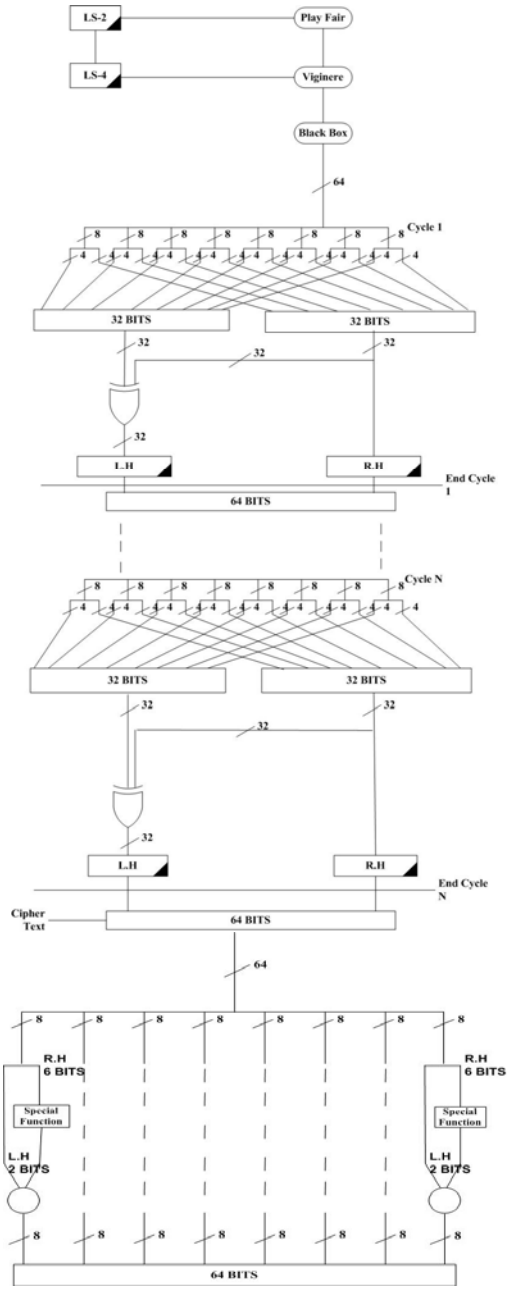

Fig1: Depicting the structure of proposed technique
Fig2: Above is the diagram of black box which contains special function

The above described function is applied to all 8 octets of the output of vigenere block the resultant of black box is again of 64-bits it is further processed by taking first 4bits from every octate and constructing four new octates similarly right 4bits are united to formulate right halves of this new arrangement finally left and right halves are XORed to obtain the left half of this Arrangement this process is repeated 3 times, the proposed amendments are depicted in the diagram below. It has N cycles (**N=3**).

5. Avalanche Effect:

Avalanche effect is the phenomenon that describes the effect in the output cipher text if a single or few bits are changed in the plain text. This change that occurs at the output should be sufficient if we want to create a secure algorithm, here in this section we will shed light on avalanche effect of our proposed technique by taking an example and finally in the next section comparison will be made with other techniques on the basis of avalanche effect.

KEY**: FAUZANCE**
010001100100000101010101011010010000010100111001000011010010

PLAINTEXT: **DISASTER**
010001000100100101010011010000010101001101010100010001010101010

CIPHER:
00010000 0100 000101010111 0100 0111
111100111011 001110001101 11101010

Now we will keep the key same and will introduce 1 character change in plaintext our plaintext will become “DISCSTER”

KEY: **FAUZANCE**

PLAINTEXT: **DISCSTER**

CIPHER:
11000111 1111 0110 11011100 1111 1100
00101101 0000 1101 00001011 01011111

AVALANCHE EFFECT
Original plaintext’s (DISASTER) cipher output
00010000 0100 000101010111 0100 0111
111100111011 001110001101 11101010

Change in one character
11000111 1111 0110 11011100 1111 1100
00101101 0000 1101 00001011 01011111

As it can be seen from the above results that there is 42-bit difference in the cipher of DISASTER and DISCSTER this means that 65.6% bits were changed when we changed a single character of our plain text.

6. Comparison:

In this section we will make comparison between playfair, Viginere SDES, DES and our proposed concept on the basis of avalanche effect. We used same key and plaintext for our testing

6.1 SDES:
As SDES takes 8bit data and 10bit key we will divide our text in to bits we took F’s 8 bits and 2bits of A to constitute our key in DISASTER and DISCSTER the only difference is in the letter A and C so we made the calculations of these two letters rest will be the same.

0100011001 key F and 2 bits of A
A 01000001 of “DISASTER”

Result
01110011

Now change in plaintext from DISASTER to DISCSTER

C=01000011

Result
11001110

Avalanche effect
01000001
11001110

5 bit difference was noted when one character was changed from “A” to “C”

6.2 DES:
Key: FAUZANCE:
010001100100000101010101010110100100000101001110010000110100010

Plaintext: DISASTER
010001000100100101010011010000010101001101010100010001010101010

Cipher: DISASTER
010101111010010100000100110110111011000101011101100011100001011

Cipher: DISCSTER

11111011010101000100100100101111111101110100001
101001110101110111
Avalanche effect
When we encrypted our message using DES and changed the same character “A” to “C” the change or avalanche effect we got was spread over 35 bits which is quite significant if we compare it with SDES.

6.3 Playfair:
We placed the same key and plaintext in playfair algorithm and calculated the avalanche effect

KEY: FAUZANCE
PLAINTEXT: DISASTER
CIPHER: ELPNOYDP

CHANGE PLAINTEXT: DISCSTER
CIPHER: ELOGOYDP

We compared the two ciphers in bits to calculate the difference and found out that there was a change in 7-bits.

6.4 Viginere:
Same data set of key and plaintext were used for vigenere and results were taken.

KEY: FAUZANCE
PLAINTEXT: DISASTER
CIPHER: IIMZSGGV

CHANGE PLAINTEXT: DISCSTER
CIPHER: IIMBSGGV

We compared the two cipher texts in bits and found the difference to be 2-bits.

6.5 Our proposed technique:
Our technique which is an amalgamation of both classical and modern techniques was also put through the same test

KEY: **FAUZANCE**
010001100100000101010101010110100100000101001110010
000110100010

PLAINTEXT: **DISASTER**
010001000100100101010011010000010101001101010100010
0010101010010

CIPHER:
00010000 0100 000101010111 0100 0111
111100111011 001110001101 11101010

KEY: **FAUZANCE**

PLAINTEXT: **DISCSTER**

CIPHER:
11000111 1111 0110 11011100 1111 1100
00101101 0000 1101 00001011 01011111

Our technique gave promising result and when compared with cipher of original text the amended text had a difference of 42 bits.

7. Results:

After comparison the results that were obtained can be well represented in form of table that describes the avalanche effect in the above discussed algorithms.

ENCRYPTION TECHNIQUE	AVALANCHE EFFECT	%
DES	35 bits	54.6
SDES	5 bits	7.8
PLAYFAIR	7 bits	10.9
VIGENERE	2 bits	3.1
PROPOSED IDEA	42 bits	65.6

Table2: Indicating effect of Avalanche in various Algorithms

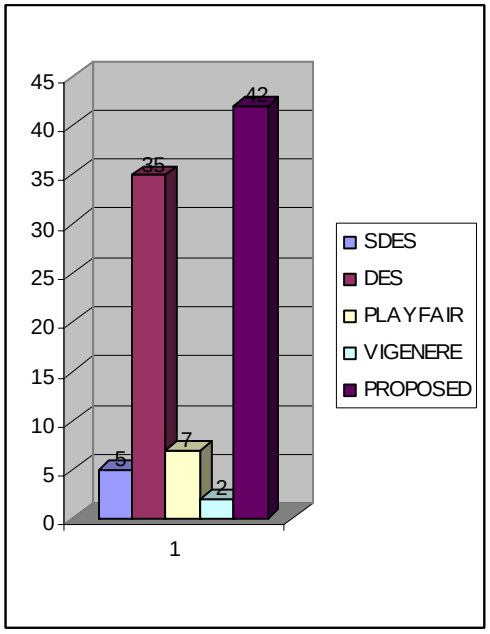

Diagram1: Depicting Algorithms & their Respective Avalanche change in percentage

Above results clearly shows the superiority of our proposed technique when compared with Playfair, vigenere, SDES and DES in terms of avalanche effect.

8. Conclusion:

From all the test and experiments that we conducted the outcome was in the favor of our proposed technique, this study showed that in terms of avalanche effect the worst technique is Vigenere that gives a difference of 2 bits when a character was changed similarly we saw playfair giving better results than Vigenere by giving a difference of 7 bits DES that uses 16 rounds gave 35 bit difference when a single character was changed and for the same sample our proposed technique gave an avalanche effect of 42 bits hence it was proved here that our proposed technique was superior to the ones mentioned and compared in this paper.

Acknowledgement:

We would like to thank Dr pervez Akhter may God give him health for his support and guidance. We would also like to thank mirza umair baig for his moral support

Reference:

[1] William stallings, “Cryptography and Network Security: Principles & Practices”, second edition, chapter 2 pg 29.

[2] V. Umakanta Sastry , N. Ravi Shanker and S.Durga Bhavani “A modified Playfair Cipher Involving Interweaving and Iteration” International journal of Computer theory and Engineering Vol.1,No. 5, December,2009 .

[3] V. Umakanta Sastry1, N. Ravi Shankar2, and S. Durga Bhavan “A Modified Hill Cipher Involving Interweaving and Iteration” International Journal of Network Security, Vol.11, No.1, PP.11{16, July 2010

[4] M. S. Hwang and C. Y. Liu, \Authenticated encryption schemes: current status and key issues," International Journal of Network Security, vol. 1, no. 2, pp. 61-73, 2005.

[5] M. H. Ibrahim, \A method for obtaining deniable public-key encryption," International Journal of Network Security, vol. 8, no. 1, pp. 1-9, 2009.

[6] M. H. Ibrahim, \Receiver-deniable public-key encryption," International Journal of Network Security, vol. 8, no. 2, pp. 159-165, 2009

[7] Results of Comparing Tens of Encryption Algorithms Using Di®erent Settings- Crypto++ Benchmark, Retrieved Oct. 1, 2008. (http://www.eskimo.com/ wei-Dai/benchmarks.html)

[8] Y. C. Hu, A. Perrig, and D. B. Johnson, “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,” Proceeding of IEEE Workshop on Mobile Computing Systems and Applications, 2003.

[9] http://www.cs.trincoll.edu/~crypto/historical/caesar.html

Received degree of BS (computer engineering) in 2004 he did MS in mobile Communications in 2006 and MS in computer networks in 2008 presently he is doing PhD in Telecommunications from Hamdard university and working as assistant professor in Usman Institute of technology.

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.