Designing an algorithm with high Avalanche Effect

Sriram Ramanujam[†] **and Marimuthu Karuppiah**[††],

[†]School of Computing Science and Engineering, VIT University, Vellore, TN, India
[††]Asst. Professor, School of Computing Science and Engineering, VIT University, Vellore, TN, India

Summary
Usage of Cryptography or the art of hiding messages dates back to 1st century B.C. Ancient ciphers used the process of scrambling of the message to encipher. One serious drawback with this method is that it is prone to brute force attack. Modern methods are less affected by brute force attack because of the usage of keys. In this paper, we design an algorithm that combines the process of scrambling of bits and substitution boxes resulting in high avalanche effect.

Key words:
Cryptography, Avalanche Effect, Scrambling of Bits, Substitution Boxes, Ancient Ciphers.

1. Introduction

A Cipher is something that is used to change the actual data into a format that cannot be recognized by anyone except the sender and receiver. One of the important considerations for measuring the strength of any cryptographic algorithm is its Avalanche Effect. A good algorithm has high Avalanche Effect. Modern techniques of encryption either use a single symmetric key or two keys. The algorithm is called as Symmetric Key Cryptography if only one key is used and it is called as a Public Key Cryptography if two keys are used.
Some of the well-known examples of Symmetric key cryptography are the Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish etc. These algorithms use a single key for encrypting the data. Public key cryptography, on the other hand, uses two keys and hence is more secure and provides digital signature also[1]. The most commonly used Public Key algorithm is the Rivest-Shamir-Adleman algorithm (RSA). The main disadvantage of Public key cryptography is that it requires excessive communication and processing resources[3].
In this paper, we have taken the advantages of classical or ancient cryptography and clubbed it with the important features of modern cryptographic algorithms. In order to understand the concept of Avalanche Effect and comparison purposes, we have taken several algorithms like the Playfair Cipher, Vigenere Cipher, Caesar Cipher, the Data Encryption Standard (DES) and Blowfish.
In the next section, we discuss about the above mentioned algorithms including the proposed algorithm and finally compare the results of avalanche effects of all the methods.

Manuscript received January 5, 2011
Manuscript revised January 20, 2011

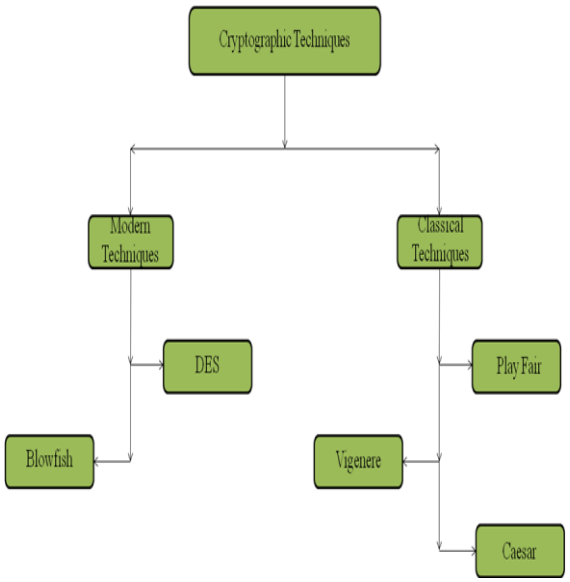

Fig. 1: Various Cryptographic Algorithms

2. Ancient or Classical Techniques:

As we have already seen, classical encryption techniques use scrambling of bits in order to encipher the message. In this section, we discuss three important classical cryptographic techniques namely,

1. Playfair Cipher
2. Vigenere Cipher
3. Caesar Cipher
4.

2.1 Playfair Cipher:

The Playfair cipher uses a 5 by 5 table containing a key word or phrase. To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in

some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. Then the message is taken and is encrypted using the following rules [4]:

1. If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue.
2. If the letters appear on the same row of the table, replace them with the letters to their immediate right.
3. If the letters appear on the same column of your table, replace them with the letters immediately below.
4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair.

2.2 Caesar Cipher:

In cryptography, a Caesar cipher, also known as the shift cipher, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on [7].

2.3 Vigenere Cipher:

The Vigenere Cipher is the process of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. To encrypt, a Vigenere square is used. It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword.

For Example:

KEY: SRIRAMSR
TEXT: DISASTER

After encrypting using the Vigenere square, the Cipher text is WABSTGXJ.

3. Modern Cryptographic Algorithms

We know that classical cipher methods are prone to brute force attacks. Symmetric Key Cryptographic algorithms are not easily broken down by brute force attacks. We look at two of the most important algorithms namely:

1. DES
2. Blowfish

3.1 DES:

The Data Encryption Standard (DES) is a block Cipher that uses shared secret encryption [5]. It is based on a symmetric-key algorithm that uses a 56-bit key. DES is an archetypal block cipher – an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. 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. DES takes plain text in 64-bits of block these 64-bits are divided into 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 initial 64-bits are permuted and finally the reverse of permutation is performed after a 32-bit swap.

3.2 Blowfish:

Blowfish is a keyed, symmetric block cipher. Blowfish has a 64-bit block size and a variable key length from 32 up to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. The Blowfish function uses a function which splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 2^{32} and XORed to produce the final 32-bit output. [9]

4. Proposed Technique

The proposed algorithm (fig 5) uses the positive features of the classical cryptographic algorithm like scrambling of bits and combines it with the main advantage of a modern cryptographic algorithm, i.e., the usage of a key. In this algorithm, the key is of 64-bits or more. The actual message to be encrypted is split into block of 64-bits (8 alphabets). Every block is enciphered using a Playfair cipher. The resulting encrypted text undergoes intensive scrambling as shown in fig 2. The scrambled text, which is also 8 bits, is further enciphered using a Vigenere cipher.

	a0	a1	a2	a3	a4	a5	a6	a7
+	a1	a1	a3	a3	a5	a5	a7	a7
=	b0	b1	b2	b3	b4	b5	b6	b7
+	b2	b3	b2	b3	b6	b7	b6	b7
=	c0	c1	c2	c3	c4	c5	c6	c7
+	c0	c1	c2	c3	c0	c1	c2	c3
=	d0	d1	d2	d3	d4	d5	d6	d7

Fig. 2: Scrambling of input text

The Vigenere ciphered text (d0d1…d7) is split into 2 parts of 4 bits each. These 2 parts are used for selecting the particular value in the 16 X 16 Substitution Box (fig 3). The first part (first 4 bits) is taken as the row and the second part (last 4 bits) is taken as the column. The resultant 64 bit is virtually unrecognizable and unbreakable using brute force approach.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	99	124	119	123	242	107	111	197	48	1	103	38	254	215	171	118
1	202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
2	183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
3	4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
4	9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
5	83	209	0	237	32	252	117	91	106	203	190	57	74	76	88	207
6	208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
7	81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
8	205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
9	96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
10	224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
11	231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
12	186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
13	112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
14	225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
15	140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

Fig. 3: 16 X 16 S-Box

Now the 64 bits are XOR-Scrambled M times (M=1, 2 or 3) (fig 4). Then, the 64-bits are further spilt into 4 blocks of 16 bits each which are then XOR-ed block-wise as shown in fig 5. The blocks are further merged and XOR-ed again as shown. The whole process is performed N times. In our experiment we take the value of N between 1 and 16. Finally the output is further scrambled using the same S-Box as shown in fig 3.

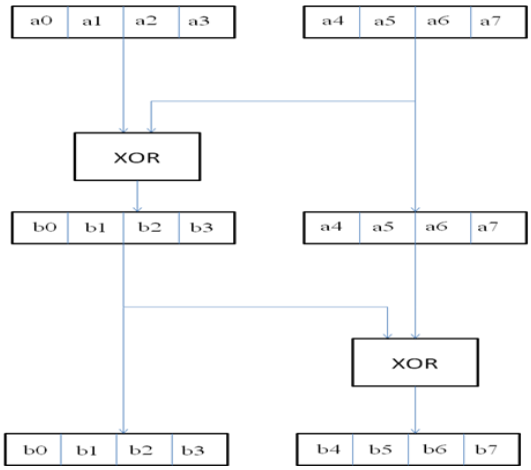

Fig. 4: XOR Scrambling

5. Calculation of Avalanche Effect

The Avalanche Effect is calculated as:

$$\text{Avalanche Effect} = \frac{\text{No. of flipped bits in the ciphered text}}{\text{No. of bits in the ciphered text}} \times 100\ \%$$

6. Comparison of Avalanche Effect

Avalanche Effect refers to a desirable property of cryptographic algorithms where, if an input is changed slightly (for example, flipping a single bit) the output changes significantly (e.g., more than half the output bits flip). In our case, we take the input plain text as “DISASTER”. Flipping one bit from the plain text, we get “DISCSTER” (on flipping A (01000001) to C (01000011)). The key used is “SRIRAMSR”.

KEY: SRIRAMSR
0101001101010010010010010101001001000001010011010101001001000010100
PLAIN TEXT 1: DISASTER
0100010001001001010100110100000101010011010101000100001010100
PLAIN TEXT 2: DISCSTER
0100010001001001010100110100010101010011010101000100001010100

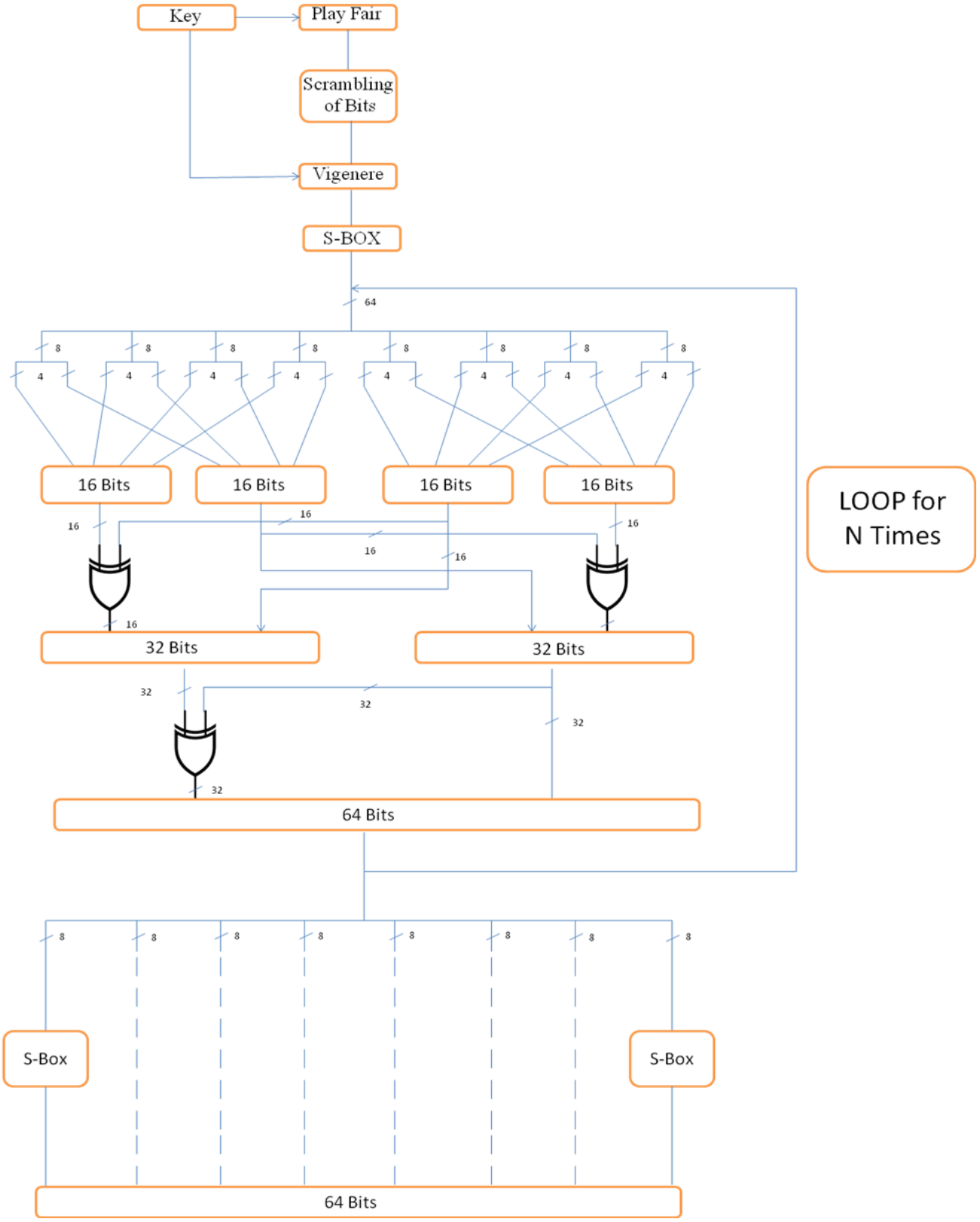

Fig. 5: Proposed Algorithm

6.1 Playfair Cipher:

CIPHER TEXT 1: KDRMAOCA
0100101101000100010100100100110101000001010011110100001101000001

CIPHER TEXT 2: KDRBAOCA
0100101101000100010100100100001001000001010011110100001101000001

We can clearly see that the avalanche effect is 4 bits, that is, 6.25%.

6.2 Vigenere Cipher:

CIPHER TEXT 1: VZARSFWI
0101011001011010010000010101001001010011010001100101011101001001

CIPHER TEXT 2: VZATSFWI
0101011001011010010000010101010001010011010001100101011101001001

The Avalanche Effect is 2 bits, that is, 3.125%.

6.3 Caesar Cipher:

CIPHER TEXT 1: GLVDVWHU
0100011101001100010101100100010001010110010101110100100001010101

CIPHER TEXT 2: GLVFVWHU
0100011101001100010101100100011001010110010101110100100001010101

The Avalanche Effect, in this case, is 1 bit only, that is, 1.56%.

6.4 DES:

CIPHER TEXT 1:
0100000011000110111110001011011101110110010010011101001011111111

CIPHER TEXT 2:
0110001000111110111010010100001110001110001111101000111000101000

After 16 Rounds of DES, there are 35-bits flipped. Hence the Avalanche Effect is 54.68%.

6.5 Blowfish:

The average Avalanche Effect in a blowfish algorithm is 28.71%. That is, there is a change of approximately 19 bits. [6]

6.6 Proposed Technique:

CIPHER TEXT 1:
0100111101011100001001101001000000100000111000111111000001011111

CIPHER TEXT 2:
0000011000010011100110011010010110000100010101000001101001000101

We can clearly see that there is a difference of 45 bits. The Avalanche Effect is calculated as 70.31%.

7. Result

The following results are obtained after calculating the respective Avalanche Effects.

Encryption Technique	No. of bits flipped	%
Playfair Cipher	4	6.25
Vigenere Cipher	2	3.13
Caesar Cipher	1	1.56
DES	35	54.68
Blowfish	19	28.71
Proposed Technique	45	70.31

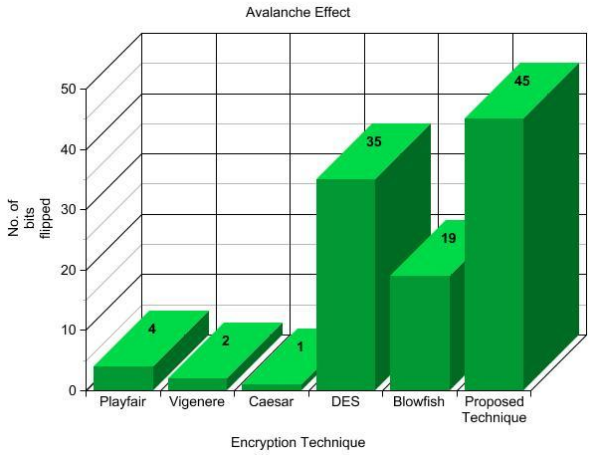

Fig. 6: Comparison of various Algorithms

8. Conclusion

From the above discussion we can clearly see that the proposed algorithm has better Avalanche Effect than any of the other existing algorithms and hence can be incorporated in the process of encryption of any plain text. Also, we can see that the classical ciphers like Playfair cipher, Vigenere Cipher, Caesar Cipher etc. have very less Avalanche Effect and hence cannot be used for encryption of confidential messages. The modern encryption techniques are better than classical ciphers as they have higher Avalanche Effect. For Example, DES has an Avalanche Effect of 54.38%.

Acknowledgement:

We would like to thank Fauzan Saeed and Mustafa Rashid of Usman Institute of Technology whose initial paper in the previous volume helped us to design a better algorithm.

References:

[1] William Stallings, "Cryptography and Network Security: Principles & Practices", fourth edition.
[2] Fauzan Saeed and Mustafa Rashid, "Integrating Classical Encryption with Modern Technique", IJCSNS Vol. 10 No.5.
[3] 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.
[4] "Information Security: Theory and Practice", by Patel, Page 20.
[5] http://en.wikipedia.org/wiki/Data_Encryption_Standard.
[6] Janan Ateya Mahdi, "Design and Implementation of Proposed B-R Encryption Algorithm", IJCCCSE, Vol. 209, No.1.2009.
[7] http://www.cs.trincoll.edu/~crypto/historical/caesar.html.
[8] Schildt, "Java: The Complete Reference", 2006.
[9] http://en.wikipedia.org/wiki/Blowfish_(cipher).

Sriram Ramanujam is pursuing final year of his B.Tech Degree at VIT University with Computer Science and Engineering as his specialization. His areas of interests include Cryptography, Information Security and Assurance and Networks.

Marimuthu Karuppiah received the BE degree in Computer Science and Engineering, in 2003 from Kamaraj University, Madurai, India; the ME in Computer Science and Engineering, in 2005 from Anna University, Chennai. He had worked as a lecturer in the department of Computer Science and Engineering, Syed Ammal Engineering College, Ramanathapuram, India from 2005-2008. Now he is working as an Assistant Professor in School of Computing Science & Engineering, VIT University, Vellore. His current research interests include Cryptography and Network Security.