Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-5, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

A New Block Cipher for Network Security

Kripa[1], Megha R Kamat[2], Meghana[3] ,Swati D Pai[4]& Mr. Vasanth Nayak[5]
[1,2,3,4]Department of Information Science and Engineering, Canara Engineering College
[5]Assistant Professor, Department of Information Science and Engineering, Canara Engineering College

Abstract:*Now-a-days internet is widely used by a large number of people for both commercial and non-commercial purposes. Originally, internet was developed for educational and research purposes, and not for commercial applications. But today, internet is being used for entertainment, communication and education. Due to the rapid increase of users and advancements in technology, there is a great need for security. Cryptography plays a major role for providing the security for modern day applications. Many researches were carried out on secure block cipher. In this paper, we present a new network security algorithm called SF Block Cipher that uses 512 bit block size and 512 bit key size. This algorithm is implemented in .NET Framework.*

Keywords:*Encryption, 512 bit block, Cryptography, Decryption, Cipher and Substitution Permutation Network*

1. Introduction

Cryptography plays a major role for providing the security for modern day applications. Cryptography deals with transmitting of the data in a particular form so that only the intended user can read and process it. It is a corner stone to protect valuable resources. The two major classifications of cryptosystems are symmetric cryptosystems and asymmetric cryptosystems. Symmetric cryptosystems uses the same key for encryption as well as decryption. Whereas, asymmetric cryptosystems uses complementary pair of keys for encryption and decryption. Of the two keys, one is kept secret called private key and the other need not be kept secret called public key. The two key approach has resulted in simplified key management by storing and managing minimum number of keys in the network.

As the key distribution system is simpler, unprotected medium can be used for distribution of public keys. Data origin authentication or integrity of data for message can be provided as follows. Using all the data bits of the message contents and a secret key, the sender generates an Integrity Check Value which is transmitted along with the original message. On the other hand, the receiver checks the consistency of the received message content and the Integrity Check Values before accepting the message. One of the special case of the Integrity Check Value is digital signature. Any dispute between the sender and receiver of the message canberesolvedusing the digital signature. Keyed hash algorithm or symmetric encryption based approach is generally inadequate for this purpose. The more powerful digital signatures are provided by asymmetric cryptosystems.

Many researchers have introduced different cryptographic algorithms all over the globe. But many of these algorithms are breakable due to their simpler structures. The advancements in the cryptanalytic techniques are also remarkable. Aquantitative evaluation of powerful cryptanalytic techniques against security is considered essential in designing any new block cipher.

In this paper, we present a new network security algorithm called SF Block Cipher that uses 512 bit block size and 512 bit key size. The proposed algorithm is developed based on the design principle called Substitution Permutation Network (SP Network).

2.Literature Survey

Some of the earlier block ciphers are DES, 3DES, Blowfish, AES and RC6. Few of these algorithms are commonly used and were mostly implemented in C and Visual Studio to identify the weakness. Brief explanations of these techniques are as follows:

DES (Data Encryption Standard): DES uses shared secret key for both encryption as well as

decryption. It uses 64 bit block size and 56 bit key size. Decryption can be performed by only those who know the particular key used to encrypt the message, this customizes the transformation. The biggest defect of DES is 56 bit key size. The weakness of DES was recorded by many attacks, which made it an insecure block cipher.[2]

3DES (Triple DES): 3DES is an enhancement of DES. It uses 64 bit block size and 192 bit key size. The method of encryption of 3DES is similar to that of DES but it is applied three times in order to increase the average safe time and the security level.[3] The main drawback of 3DES is that it is much slower than the other cryptographic algorithms.

Blowfish: Blowfish has a block size of 64 bit. It uses a variable length key, that ranges from 32 bits to 448 bits.[4] The default key size is 128 bits. It encrypts the data 16 times to making the hacker impossible to decrypt it. Blowfish is best suited for applications where the key remains constant for a long time and where the key changes frequently.

AES (Advanced Encryption Standard): AES is a symmetric key algorithm that is, the same key is used for both encryption as well as decryption of data. It uses a variable key length of 128, 192 or 256 bits. The default key length is 256 bits. This encryption method is fast and flexible. The only attack to this algorithm is the brute force attack. The brute force attack allows the attacker to test various combinations of characters to break the security. However, it is not an easy job if the number of combinations is high.[5]

RSA: RSA is a public key algorithm which was invented by Rivest, Shamir and Adleman. It is an asymmetric cryptography that uses different keys for encryption and decryption. One among them is public and the other is private.[6] Public key is known to everyone and this key is used for encrypting the messages. The private key is used to decrypt the message. The main disadvantage of RSA algorithm is its speed.

3. Problem statement

The survey carried on the various symmetric and asymmetric algorithms such as DES, 3DES, Blowfish, AES and RSA shows that they have some performance issues as well as security issues. It is also found that Blowfish and AES are more secure when compared to other encryption algorithms. The work stated that "According to academic papers and reports regarding the security evaluation for such algorithms, it is difficult to ensure enough security by using the algorithms for a long time period, such as 10 or 15 years, due to advances in cryptanalysis techniques, improvement of computing power, and so on. To enhance the transition to more secure ones, National Institute of Standards and Technology (NIST) of the United States describes in various guidelines that NIST will no longer approve two-key triple DES, RSA with a 1024-bit key, and SHA-1 as the algorithms suitable for IT systems of the U.S. Federal Government after 2010"[7]. Based on this study, the problem statement is formulated and a new algorithm is proposed.

4. Proposed Algorithm

Based on the problem statement that is stated above, a new encryption algorithm is proposed. The block cipher used in this algorithm is a 512 bit block cipher which is based on the design principle called as Substitution Permutation Network (SP Network). The proposed algorithm is designed based on AES algorithm. This algorithm takes the key and a block of plaintext as inputs. Several alternating layers or rounds of substitution boxes and permutation boxes are applied to the input in order to generate the cipher text block. In case of the proposed block cipher, the block size as well as the key size is 512 bit. The key and the message block are arranged in a 4*16 matrix (4 rows and 16 columns). This matrix is called as State Matrix. The 512 bit SF block cipher applies its functions in N rounds for encrypting and decrypting a message block. Here N stands for round number which is calculated using the formula given below.

Round Number = (block size or key size in words) + 6

Where 1 word = 4 bytes, 1 byte = 8 bits and 6 is a constant. As the block size as well as, key size is 512 bit, which is equal to 64 bytes. 64 bytes is in turn equal to 16 words. Therefore,the total rounds for the proposed algorithm based on this formula is 22. As encryption and decryption both make use of same algorithm, 2 additional rounds are required. Hence the total number of rounds applied for this block cipher is 24 rounds. The length of the inputmessage should be a multiple of 512. Padding is used if the length of message block is less than 512 bit. In the padding method, a bit "1" is inserted after the original last message and then appended with "0" bits until the last message block has the size 512. User password is used to derive the initial key. The other round keys are generated from the key expansion algorithm.

A. Key Expansion Algorithm

The SF Block Cipher uses the same key expansion algorithm as the Advanced Encryption Standard(AES)[8]. The padded key block is used to create the round keys.

B. Encryption Algorithm

The input to the encryption algorithm is plaintext of 512 bits and the output produced is cipher text of 512 bits. It mainly consists of four steps. The first step being sub byte round followed by convert row round, shifting round and Add round key round as detailed below.

State: The input is converted into 512 bits at a time and then arranged in the 4*16 matrix called State matrix (S). Each element of the state matrix is one byte. Then each byte of the state matrix is convertedinto ASCII values as shown in the figure:

AA	BB	CC	DD	EE	FF	GG	HH	II	JJ	KK	LL	MM	NN	OO
QQ	RR	SS	TT	UU	VV	WW	XX	YY	ZZ	11	22	33	44	55
77	88	99	00	AA	BB	CC	DD	EE	FF	GG	HH	II	JJ	KK
MM	NN	OO	PP	QQ	RR	SS	TT	UU	VV	WW	XX	YY	ZZ	11

Figure 1: State Matrix

Sub byte Round: The output of the state matrix is given as input to this sub byte round. In this process, first row of the state matrix I converted in to their binary values. As each row consists of 16 columns 16 groups of 8-bit binary values are generated. The first 4-bits from each group are separated out. Again the bits are grouped into 16 groups of 8-bit value such as G0 – G15. The values of 16 groups are

{(G0,G15),(G1,G14),(G2,G13),(G3,G12),(G4,G11),(G5,G10),(G6,G9),(G7,G8),(G8,G7),(G9,G6),(G10,G5),(G11,G4),(G12,G3),(G13,G2),(G14,G1),(G15,G0) }

a	e	i	m	q	u	y	3	7	A	E	I	M	Q	U	Y
b	f	j	n	r	v	z	4	8	B	F	J	N	R	V	Z
c	g	k	o	s	w	1	5	9	C	G	K	O	S	W	%
d	h	l	p	t	x	2	6	0	D	H	L	P	T	X	@

97	101	105	109	113	117	121	51	55	65	69	73	77	81	85	89
98	102	106	110	114	118	122	52	56	66	70	74	78	82	86	90
99	103	107	111	115	119	49	53	57	67	71	75	79	83	87	37
100	104	108	112	116	120	50	54	48	68	72	76	80	84	88	64

Figure 2: Sub byte round

The value at location S (G0, G15) is substituted from substitution box(S-box). This process is repeated for remaining locations such as S(G1,G14), S(G2,G13) , S(G3,G12),S(G4,G11),S(G5,G10),S(G6,G9), S(G7,G8),S(G8,G7),S(G9,G6),S(G10,G5), S(G11,G4), S(G12,G3), S(G13,G2), S(G14,G1),S(G15,G0). Thus all the elements of first row of the cipher matrix are substituted in state matrix. This process is applied for second row of the cipher text matrix and so on. After applying the same process for all the rows of the cipher key matrix all the values are copied to state matrix and given as input to the convert row round.

Convert Row Round: In this step, the hexadecimal representation of each data element from the first row is converted into its binary form. It is then read from right to left. After that the data is again represented in its hexadecimal form. For example, consider the data element K. Its hexadecimal representation is 4b. 4b is then converted into its binary form, that is, 01001011. Reading this binaryrepresentation from right to left gives 11010010. It is then converted into hexadecimal form which gives D2. All the values in this matrix are replaced after this process is repeated for all the rows.

Shifting Round: In this step, two rows are shifted in the state matrix which is obtained from the previous step. The output matrix is then represented in its binary form. The resulting output matrix is XoRed with the original matrix from the first step. For example, in the following figure, A is the original state matrix and B is the state that is obtained after shifting the rows. C and D are the binary equivalents of the states A and B respectively. After performing XoR function on C and D, the final state obtained will be s E.

A.

AA	BB	CC	DD	EE	FF	GG	HH	II	JJ	KK	LL	MM	NN	OO	PP
QQ	RR	SS	TT	UU	VV	WW	XX	YY	ZZ	11	22	33	44	55	66
77	88	99	00	AA	BB	CC	DD	EE	FF	GG	HH	II	JJ	KK	LL
MM	NN	OO	PP	QQ	RR	SS	TT	UU	VV	WW	XX	YY	ZZ	11	22

B.

77	88	99	00	AA	BB	CC	DD	EE	FF	GG	HH	II	JJ	KK	LL
QQ	RR	SS	TT	UU	VV	WW	XX	YY	ZZ	11	22	33	44	55	66
AA	BB	CC	DD	EE	FF	GG	HH	II	JJ	KK	LL	MM	NN	OO	PP
MM	NN	OO	PP	QQ	RR	SS	TT	UU	VV	WW	XX	YY	ZZ	11	22

Figure 3: Shifting Round

Add Round Key: In the Add Round Key method the actual encryption is performed by

AddRoundKey() function where each byte from the state matrix(M) is XORed with the sub key. According to the key expansion schedule the sub key isderived from the key.

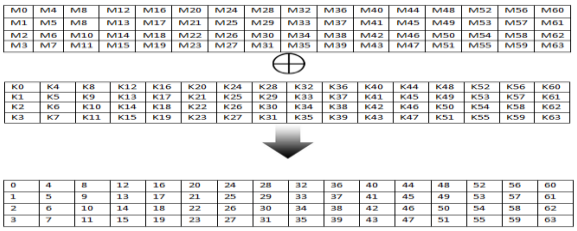

Figure 4. Add Round Key

C. Decryption Algorithm

The working of the decryption algorithm is exactly the reverse order of the encryption process as described above. The cipher text along with the key is taken as an input and the original message is outputted in the decryption algorithm. The algorithm is implemented in the .Net Framework. In order to reduce the processing speed, code optimization is done further. Text files of different sizes are given as an output.

5. Performance Evaluation

For any encryption algorithm, its performance is one of the vital components. The implementation of the algorithm that is proposed in this paper, is done keeping performance in mind. SF Block Cipher is implemented using the .NET Framework. AES algorithm is also implemented to evaluate the performance.

To evaluate the performance of the SF Blok Cipher and AES, various performance measures are used. Some of the performance metrics are Encryption time, Decryption time, Battery, CPU clock cycles and CPU process time. The total time taken by the algorithm to produce a cipher text from the plain text is called Encryption time. The average encryption time is given by the equation.

$$\text{AvgTime} = \frac{1}{Nb}\sum_{i=1}^{Nb}\frac{Mi}{ti}$$

Where,
AvgTime = Average Data Rate (Kb/s)
Nb = Number of messages
Mi = Message Size (Kb)
ti = Time taken to encrypt the message Mi

The throughput of the encrypted algorithm is calculated using the encryption time. The throughput gives the rate of encryption. It is calculated as the total encrypted plaintext (represented in bytes) divided by the total encryption time. The equation can be given as.

$$\text{Throughput} = \frac{Tp}{Et}$$

Where,
Tp = Total encrypted plaintext.
Et = Total encryption time
The total time taken to produce the plain text back from the cipher text is called Decryption time. The throughput of the decrypted algorithm is calculated using the decryption time. The throughput in this case, gives the rate of decryption. It is calculated as the total decrypted plaintext (represented in bytes) divided by the total decryption time. The time required by a CPU that is used only by a particular process of calculations is called the CPU process time. It represents the load on the CPU. The CPU clock cycle represents the energy consumption of the CPU while performing the encryption operations. Each cycle of the CPU consumes a small amount of energy.

6. Results

The proposed algorithm is evaluated using the experimental procedures discussed above. The performance of the algorithm is tested using different file sizes. The encryption time and throughput is shown using different graphs. Table 1 and Table 2 provide the encryption time and decryption time of the proposed algorithm respectively.

Table 1. Encryption Time Data of SF Block Cipher

Input Size	Time(milliseconds)	
(Kb)	AES	SF
49	59	56
59	39	38
100	94	90
247	121	112
321	167	164
694	234	210
899	254	258
963	213	208
5345	1324	1237
7310	1432	1366

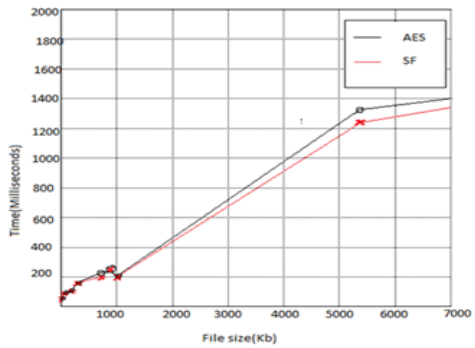

Figure 5. Encryption Time Analysis

Table 2. Decryption Time Data of SF Block Cipher

Input Size (Kb)	Time(milliseconds)	
	AES	SF
49	65	61
59	45	43
100	89	79
247	120	112
321	167	168
694	243	212
899	223	259
963	243	206
5345	1224	1216
7310	1435	1363

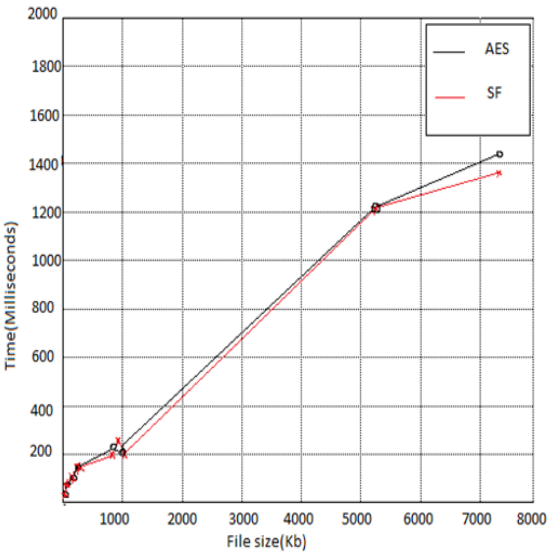

Figure 6. Decryption Time Analysis

The throughput of an encryption scheme is calculated using the encryption time. The throughput indicates the speed of the encryption. In order to calculate the throughput, total plaintext in Megabytes encrypted is divided by the total encryption time for each algorithm. The power consumption of the encryption technique decreases as the throughput value increases. Table 3 shows the throughput and average time of SF encryption algorithm. Table 4 shows the throughput and average time of SF decryption algorithm.

Table 3. Throughput Analysis (Encryption)

Input Size (Kb)	Time(milliseconds)	
	AES	SF
49	65	61
59	45	43
100	89	79
247	120	112
321	167	168
694	243	212
899	223	259
963	243	206
5345	1224	1216
7310	1435	1363
Average	388	377
Throughput	4.26	4.27

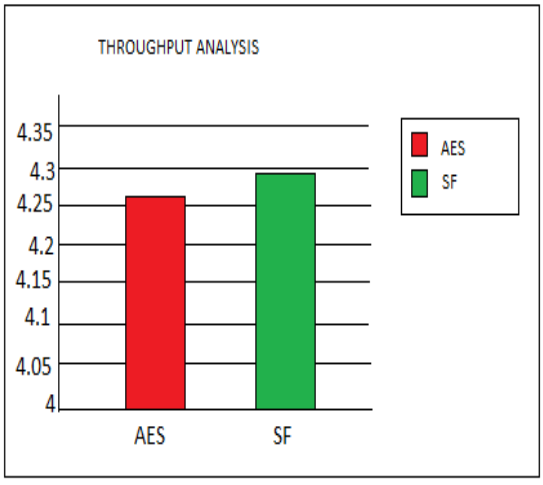

Figure 7. Throughput Analysis for Encryption

Table 4. Throughput Analysis (Decryption)

Input Size (Kb)	Time(milliseconds)	
	AES	SF
49	59	56
59	39	38
100	94	90
247	121	112
321	167	164
694	234	210
899	254	258
963	213	208
5345	1324	1237
7310	1432	1366
Average	386	374
Throughput	4.29	4.59

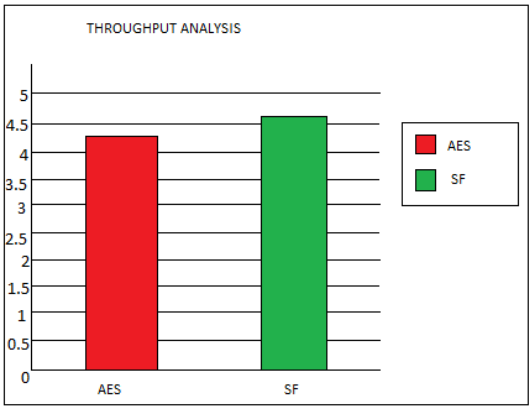

Figure 8. Throughput Analysis for Decryption

7. Conclusion

Various cryptographic algorithms are reviewed in this paper. Based on the reviews of literature survey, it was found that the cryptographic algorithm which uses block cipher of 128 bit key as well as block size couldn't provide enough security in banking sectors as well as IT fields due to the advancement in the cryptanalysis techniques and computing technology. This new block cipher called the SF block cipher was introduced in order to overcome this problem. This algorithm is capable of encrypting a 512 bit block size. Hence it is difficult to break. It was also found that the performance of this algorithm was much better when compared to other encryption algorithm. The key expansion algorithm used is similar to that of AES and is used to generate round keys. In future, a new key expansion algorithm will be propsed for this new 512 bit SF block cipher.

8. References

[1]Alaa, T., A.A. Zaidan and B.B. Zaidan, 2009.New framework for high secure data hidden in the MPEG using AES encryption algorithm. Int. J. Comput. Electr. Eng., 1: 566-571.

[2] Davis, R., "The Data Encryption Standard in Perspective," Proceeding of Communication Society magazine, IEEE, Volume 16 No 6, pp. 5-6, Nov. 1978.

[3] E. Thambiraja, G.Ramesh, Dr. R. Umarani, "A survey on various most common encryption techniques," International Journal of Advanced Research in ComputerScience and Software Engineering, Vol 2, Issue 7, July 2012.

[4]Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[5]PratapChnadraMandal "Superiority of Blowfish Algorithm," International Journal Of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, September 2012.

[6]R.L.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communication of the ACM, Volume 21 No. 2, Feb. 1978.

[7]Douligeris.C and Serpanos D., 2007. IP Security (IPSec). IEEE Book: Network Security: Current Status and Future Directions, 65 – 82.

[8]W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309.