HYBRID APPROACH USING ENCRYPTION ALGORITHMS FOR DATA STORAGE

Kashish Goyal, Supriya Kinger

Abstract— *Cryptography is an art and science of converting original message into non readable form. Fast progression of digital data exchange in electronic way, information security is becoming much more important in data storage and transmission. Cryptography has come up as a solution which plays a vital role in information security system against malicious attacks. In this paper author presents HYBRID encryption system for security. Author used Three algorithms in this paper. Caesar cipher is a monoalphabetic cipher which substitute with another character. Rijndael Algorithm uses block length at 128 bits and key sizes of 128, 192 or 256 bits. Vernam cipher (or one-time pad) has played an important rule in cryptography. The key is at least as long as the message. The key is truly random. Each key is used only once, and both sender and receiver must destroy their key after use*

Index Terms— ***Encryption, Decryption, symmetric encryption, plaintext, ciphertext***

1 INTRODUCTION

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted [1]. As the importance and the value of exchanged data over the Internet or other media types are increasing, the search for the best solution to offer the necessary protection against the data thieves' attacks along with providing these services under timely manner is one of the most active subjects in the security related communities. The explosive growth and the open nature of the Internet and e-commerce have caused organizations to become more vulnerable to malicious electronic attacks than ever before. With the increasing quantity and sophistication of attacks on IT assets, companies have been suffering from breach of data.

Cryptography is the branch of cryptology dealing with the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of message. Cryptography is usually referred to as "the study of secret". Encryption is the process of converting normal text to unreadable form. Decryption is the process of converting encrypted text to normal text in the readable form [2]. With the increasing trend of internet & technologies numerous security issues are arising Cloud users are also victim of the security issues. In cloud computing security issues are faced by the Cloud providers as well as customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' personal data and applications are protected while the customer must ensure that the Cloud provider has taken the proper security measures to protect their information. So security issues are everywhere [3]. In cryptography original message called plaintext, it is converted to random bits known as cipher text by using a key and an algorithm. Figure 1 shows the encryption process

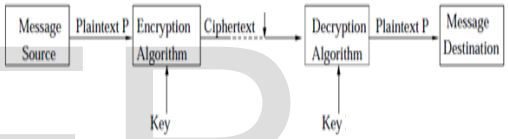

Fig. 1

2 TYPES OF ENCRYPTIONS

There are two main categories of cryptography depending on the type of security keys used to encrypt/decrypt the data. These two categories are: Asymmetric and Symmetric encryption techniques [4].

2.1 Symmetric Encryption

The concept of symmetric encryption is perhaps familiar from childhood: friends share a single code book, and use the codes to both encrypt and decrypt secret messages. This technique is sometimes called shared key encryption, because the same password and process is used both to hide secrets and reveal them. The simplicity of symmetric encryption belies its utility. Today, businesses commonly use symmetric encryption to encode communications among internal systems, or to encrypt archival data. Figure 2 shows the working of symmetric encryption.

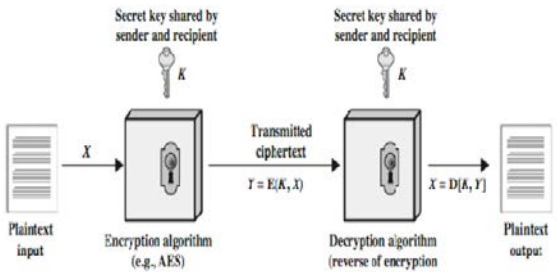

Fig. 2

- *Kashish Goyal is currently pursuing masters degree program in computer science and engineering in Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India E-mail: er.aggarwalkashish@gmail.com*
- *Supriya Kinger is Assistant Professor Department of Computer Science and Engineering in Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India E-mail: supriya@sggswu.org*

Figure 3 shows the classification of encryption methods.

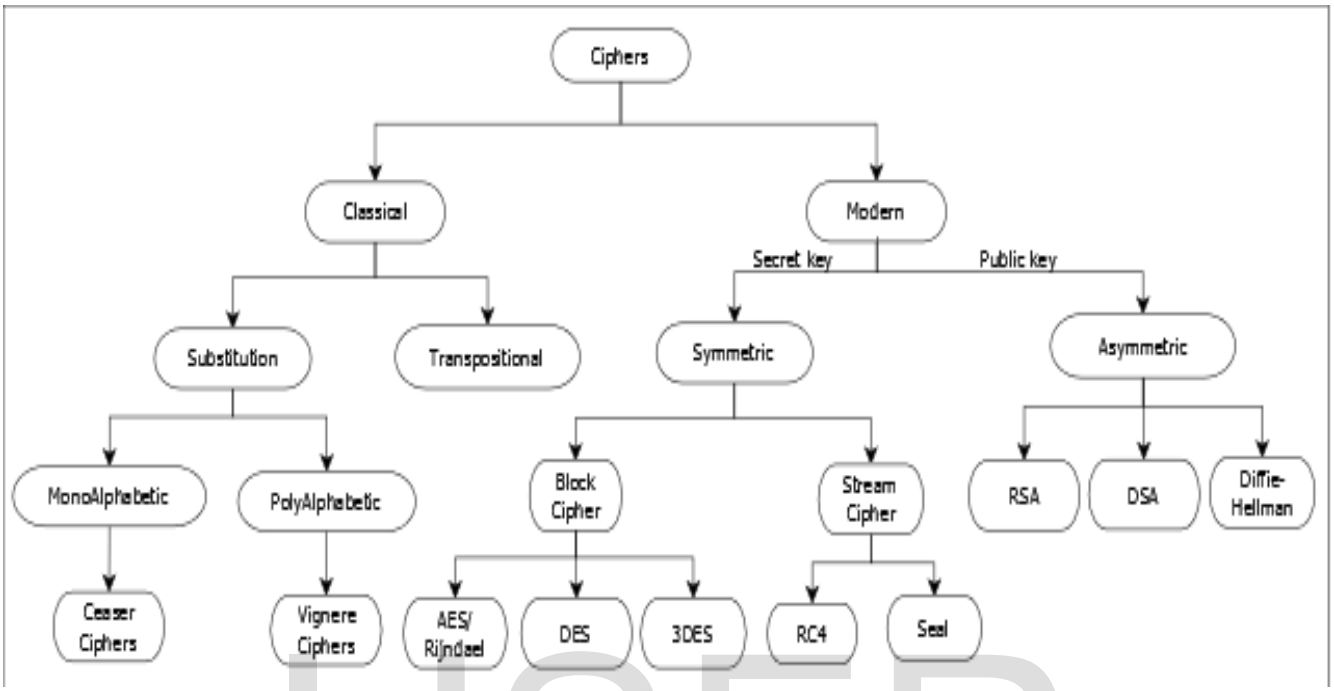

Fig. 3

2.2 Symmetric Encryption

It is also called as public key cryptography. It uses two keys: public key, which is known to the public, used for encryption and private key, which is known only to the user of that key, used for decryption. Following figure shows the symmetric encryption process. The public and the private keys are related to each other by any mathematical means. In other words, data encrypted by one public key can be encrypted only by its corresponding private key [5].

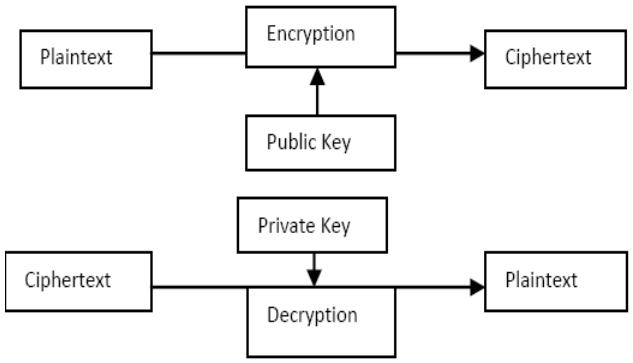

Fig. 4. Asymmetric Encryption

3 PROPOSED ALGORITHM

To encrypt a Text file proposed algorithm requires Text file and encryption key. The encryption key is an integer value And it determines alphabet to be used for substitution. It is based on modulo twenty six arithmetic to ensure that integer Value wraps round in case encryption key supplied is more than twenty six. Decryption follows reverse operations per Formed during the process of encryption. It requires decryption key, and encrypted text. The decryption key should be complement to the encryption key so that reverse character substitution can be achieved. As stated earlier, Caesar cipher simply shifts encrypted character by number of positions. In this paper author proposed a new method, where key size is fixed as one. In this method firstly alphabet index is checked if the alphabet index is even then increase the value by one else the index is odd decrease the key value by one. Furthermore, the characters of the encrypted text are scrambled in such a way that if an attempt is made to decrypt the cipher text it would not be easy to decrypt the text.

Encryption Algorithm
Step1: Take the plain text as input.
Step2: Firstly alphabet index is checked if the alphabet index is even then increase the value by one else decrease the key value by one.
Step3: Get the encrypted text.

Decryption Algorithm
Step 1: Insert cipher text.
Step2: Check alphabet index if the alphabet index is even then increase the value by one else decrease the key value by one.
Step 3: Get the plain text.

3.1 Modified Caesar Cipher Algorithm

TABLE 1

TEXT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
KEY	B	A	D	C	F	E	H	G	J	I	L	K	N	M	P	O	R	Q	T	S	V	U	X	W	Z	Y

TABLE 2

text	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
key	b	a	d	c	f	e	h	g	j	i	l	k	n	m	p	o	r	q	t	s	v	u	x	w	z	y

TABLE 3

NUMBER	1	2	3	4	5	6	7	8	9	0
KEY	2	1	4	3	6	5	8	7	0	9

TABLE 4

TEXT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
KEY	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

IJSER

TABLE 5

TEXT	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
KEY	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Encryption
C=E (P) = (P+1) if P is even or zero than add one
Else
E (P) = (P-1) (mod 26) if p is odd than subtract one

Decryption
P=D(C) = (C-1) if C is Odd than subtract one
Else
D (C) = (C+1) if P is even or zero than add one

4 HYBRID ENCRYPTION ALGORITHMS

4.1 Caesar Cipher

To encrypt a Text file proposed algorithm requires Text file and encryption key. The encryption key is an integer value and it determines alphabet to be used for substitution. It is based on modulo twenty six arithmetic to ensure that integer value wraps round in case encryption key supplied is more than twenty six. Decryption follows reverse operations per formed during the process of encryption. It requires decryption key, and encrypted text. The decryption key should be complement to the encryption key so that reverse character substitution can be achieved. As stated earlier, Caesar cipher simply shifts encrypted character by number of positions. In this paper author proposed a new method, where key size is fixed as one. In this method firstly alphabet index is checked if the alphabet index is even then increase the value by one else the index is odd decrease the key value by one. Furthermore, the characters of the encrypted text are scrambled in such a way that if an attempt is made to decrypt the cipher text it would not be easy to decrypt the text.

4.2 Rijndael Algorithm

The Rijndael algorithm (Daemen and Rijmen, 2002) is a cipher that was invented by Vincent Rijmen and Joan Daemen.Rijndael algorithm is an iterative block cipher. It has a variable key and blocks length, which gives it a degree of flexibility when choosing an appropriate implementation. The block and key sizes can be any multiple of 32 bits between 128 bits and 256 bits. This is the key difference between the Rijndael algorithm and the version of it specified as the AES,

as the AES fixes the block length at 128 bits and key sizes of 128, 192 or 256 bits. The Rijndael algorithm takes a block of data as the input and performs a number of 'Round Transformations' on it. The Round transformation is actually a series of four separate transformations. These operations are applied in order for a set number of rounds, followed by a slightly altered final round which completes the encryption [6].Figure 5 shows the working of Rijndael algorithm.

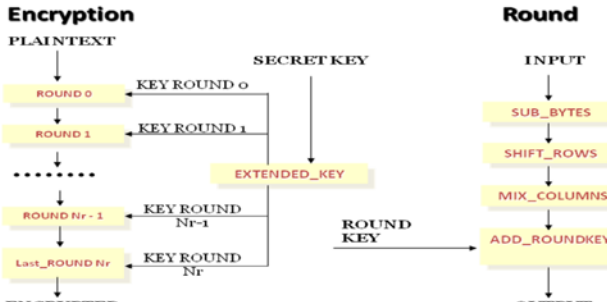

Fig. 5

4.3 Vernam Cipher

The Vernam cipher **was** designed by Gilbert Vernam in 1917.which is **an** implementation of one-time pad. However, using each key only once obviously leads *to* a severe key distribution problem, and the one-time pad is only useful for relatively short messages which are to be sent infrequently [7].Gilbert Vernam of AT&T invented the first electrical one time pad. The Vernam cipher was obtained by combining each character in the message with a character on a paper tape key. There were other developments in the 1920s which resulted in the paper pad system. An OTP was used for encrypting a teletype hot-line between Washington and Moscow. OTPs were also used successfully by the English in World War II. These were especially useful in battlefields and remote regions where there were no sophisticated equipments for encryption, all that they used were OTPs printed on silk. The final discovery of significance and theoretical importance of the OTP was made by Claude Shannon in 1949 [8].

5 EXPERIMENATAL RESULTS

A. Encryption

Step 1: Suppose Text file contain text Computer123

Step 2: Now apply Caesar cipher to encrypt the plain text. shifting the key as one .

PlainText : Computer123
Cipher Text : Dpnovsfq214

Step 3: Now apply the Rijndael Algorithm Algorithm on encrypted file .Here output file of Caesar file is now input file of Rijndael Algorithm Algorithm.

Cipher Text of Caesar cipher : Dpnovsfq214
Cipher Text of Rijndael Algorithm algorithm : •ÊDéÈè4•sVV~w]

Step 4: Now apply the Vernam cipher on encrypted file .Here output file of Rijndael Algorithm Algorithm is now input file of Vernam Cipher.

Cipher Text of Rijndael Algorithm algorithm : •ÊDéÈè4•sVV~w]
Cipher Text of Vernam Cipher : »Ò,b!L˜ýæ?s@;~F

B. Decryption

Step5: Apply the Vernam cipher on encrypted text. To decrypt the text

Decrypted Text of Vernam cipher : »Ò,b!L˜ýæ?s@;~F
Decrypted Text of Rijndael Algorithm algorithm : •ÊDéÈè4•sVV~w]

Step 5: Now apply the Rijndael Algorithm Algorithm on text .Here output file of vernam cipher is now input file of Rijndael Algorithm Algorithm.

Decrypted Text of Rijndael Algorithm algorithm : •ÊDéÈè4•sVV~w]
Decrypted Text Text of Caesar cipher : Dpnovsfq214

Step 6: Now apply the Caesar Cipher on text .Here output file of Rijndael Algorithm Algorithm is now input file of Caesar Cipher .

Decrypted Text Text of Caesar cipher : Dpnovsfq214
Plain Text :Computer123

Now we get the original text Computer123

6 CONCLUSION AND SCOPE OF FUTURE WORK

Security has become a very critical aspect of modern computing systems. The use of internet and network is growing rapidly. So requirement to secure the data is necessary. To provide security to network and data different encryption methods can be used. In this paper Hybrid algorithm is used for Security purpose. It is based on Caesar cipher, Rijndael and Vernam algorithms. Author used this method for text files. In our future work we can add various types of files in this method also we can add more algorithms to enhance the security. Using more algorithms provide secure environment for data storage and retrieval.

REFERENCES

[1] Hamdan.O.Alanazi, B.B.Zaidan and A.A.Zaidan, "New Comparative Study Between DES, 3DES and AES within Nine Factors", JOURNAL OF COMPUTING. Vol.2 , Issue 3. Pp.152-157, MARCH 2010

[2] Ochoche Abraham, Ganiyu O. Shefiu, "AN IMPROVED CAESAR CIPHER (ICC) ALGORITHM", International Journal Of Engineering Science & Advanced Technology (IJESAT). Vol. 2, Issue-5. pp .1198 – 1202 , October 2012.

[3] Kashish Goyal , Supriya, "Security Concerns In the World of Cloud Computing", IJARCS International Journal of Advanced Research in Computer Science, Volume 4, No. 4, pp. 230-234 , March 2013.

[4]"CRYPTOGRAPHY".
https://en.wikipedia.org/wiki/Cryptography

[5] Gurpreet Singh and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications, Volume 67– No.19, pp. 33-38, April 2013.

[6] L.Thulasimani , M.Madheswaran, "Design And Implementation of Reconfigurable Rijndael Encryption Algorithms For Reconfigurable Mobile Terminals", International Journal on Computer Science and Engineering (IJCSE), Vol. 02, No. 04, pp. 1003-1011, 2010.

[7] Feng-Tse Lin, Cheng-Yan Kao, "A Genetic Algorithm for Ciphertext-Only Attack in Cryptanalysis", Institute of Electrical and Electronics Engineers (IEEE). pp. 650-654,1995

[8] Nithin Nagaraj , VivekVaidya and Prabhakar G. Vaidya ,"Re-visiting the One-Time Pad", INTERNATIONAL JOURNAL OF NETWORK SECURITY, Vol.6, No.1, PP.94–102, Jan. 2008.

IJSER