A Cryptosystem Based On Vigenere Cipher By Using Mulitlevel Encryption Scheme

Akhil Verma[1], Om prakash singh[2]
[1, 2] Dept of Master of Computer Application
[1, 2] National Institute of Technology,Kurukhsetra,India.

Abstract- *In today's world securing information in internet has become a crucial task. To secure such information, encryption plays an important role in information security. In this paper Vigenere cipher is considered which is to be most efficient and simplest one. Due to its repeating nature of the key it is vulnerable to attacks like Kasiski, known plain text etc., to find the length of encryption key. To overcome this,multi level encryption is done by using Vigenere cipher to improve better security against cryptanalysis.*

Keywords- Encryption, Vigenere cipher, VPN, Diffie Hellman Key exchange protocol

I. INTRODUCTION

With the rapid development of information technology, secrecy and privacy are the key issues of cryptography. Through cryptography one can prevent an intruder from understanding the data during communication time. To this, encryption and related technologies are considered as one of the most powerful tool to secure data transmission over the communication network like Virtual Private Network(VPN) [4]. VPN or virtual private network is a network constructed by using public wires usually the Internet to connect to a private network, such as a company's internal network to transport the confidential data. These systems use security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted [5] [4]. So, to secure the information, cryptography is used where the encryption is the process of transforming plain text message into scrambled message by using a key and vice versa for decryption. Encryption techniques decryption. In Asymmetrickey encryption two keys - public and private keys, where the public key is known to all members while the private key is kept secure by the user [7]. Thus, the security of encrypted data dependson the strength of cryptographic algorithm and the secrecy of the key. In this paper classical cipher is selected and implemented for safer communications. In classical methods, two basic techniques namely substitution and transposition are used. In substitution technique, letters of plaintext are replaced by numbers and symbols. This technique is further divided into Monoalphabetic and polyalphabetic cipher. In monoalphabetic [6] [1], it replaces each letter in the plaintext with another letter to form the ciphertext. The main problem with monoalphabetic substitution ciphers is that they are vulnerable to frequency analysis. However in polyalphabetic cipher, uses multiple substitution alphabets. That is a single character in the plaintext is changed to many characters in the cipher text. So it has the advantage of hiding the letter frequency. The best known and simplest of such polyalphabetic cipher algorithm is Vigenere cipher [1]. Vigenere cipher is one of the most popular ciphers in the past because of its simplicity and resistance to the frequency analysis test of letters that can crack simple ciphers like Caesar cipher. But with the increase in the cryptanalytic skills, Vigenere cipher is no longer taken as secure cipher and is not popularly used. The most weak point of Vigenere cipher is the use of repeated words as key-streams that causes repetition of certain patterns in cipher texts at intervals equal to the length of the keyword used.

This paper is divided into following sections like, Section 2 introduce Vigenere cipher. Section 3 describes a proposed multi level encryption method for generating random key stream by using vigener cipher with a chosen keyword. Thus, the key-stream increases the tightness of security in Vigenere cipher as this makes the deciphering of the cipher text from the knowledge of the key length difficult. Implementation, generating session key and experimental results are given in section 4 and conclusions in section 5.

II. RELATED WORK

The Vigenere Cipher is an encryption scheme which was invented in the 16th century by French Blaise De Vigenere. The scheme is inspired by the Caesar Cipher in that it uses a "polyalphabetic substitution matrix" that combines two or more alphabetic tables. The Vigenere encryption [1] scheme relies on a keyword as its key along with the polyalphabetic substitution table to encode and decode a message. For instance, to encrypt the message using a Vigenère cipher table which is in fig1, by using the key will
do the following; first the key is repeated sequentially until the length of the message and aligned together. Then the words are translated by locating the rows and columns of each position in the keyword and plaintext in polyalphabetic substitution table provided below to get the encrypted

ciphertext. The same key is then used to decrypt the message to reveal the same message by using the reverse process [8].
Fig1: Vigenere Table

III. PROPOSED MULTI LEVEL ENCRYPTION METHOD

In this paper, a new method is proposed where anequivalent fixed length of plain text and a key isselected and applied in vigenere table to get a newcipher text. This cipher text is act as a new key. Withthis new key the cipher text is encrypted once againand sends the final cipher text to the receiver. Finallythe receiver does the decryption in reverse way whichis represented in fig.2. This secured information can betransmitted once the users authenticate themselves by usingDiffie Hellman Key Exchange Protocol.Fig. 2: Encryption/Decryption Process This proposed method isimplemented in virtual private network (VPN) to show itsefficiency in terms of authorization and secure datatransmission which isdescribed below,

3.1 IMPLEMENTATION WITH ILLUSTRATION

In VPN the encryption/decryption is done by using the IPSec encryption (3DES, AES [9], etc...) which is attacked by intruder like brute force attacks, known plain text attack, cipher text attack etc.,, To circumvent these problem, the proposed multilevel encryption/decryption is used to secure the data. VPN consists of two sub-protocols which provide the instructions to secure its data [5] [9];

1. Encapsulated Security Payload (ESP) encrypts the packet's payload (the data it's transporting) with a symmetric key.
1. Authentication Header (AH) uses a hashing operation on the packet header to help hide certain packet information (like the sender's identity) until it gets to its destination. In this paper, the encapsulated security payload is used for transmitting data which is shown in fig3.

Fig3: Generalized data transmission in VPN

3.2 ILLUSTRATION

First Encryption:
Key1 (K1):
KEY 1: S A N J E E
Numeric value: 19 1 14 10 5 5
The plain text is converted into equivalent numeric value like
A - 1, B-2, C-3…, Z-27, blank-28, etc.,

First Encryption:

A new key K2 is generated by assigning the plaintext in the row side and key K1 in the column side to get a common value for each letter which is generated from the table 1, Plain text message / Secrete message Key(K1) Common value in table

Plaintext: S E C R E T

Numeric value: 19 5 3 18 5 20

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

Table 1: Vigenere cipher table

From the above table 1, the new key K2 is "KAPAIX"

Second Encryption:

Now the given plain text is once again encrypted by using the new key K2 as,

S + k = 19 + 11 = 30 mod 27 =3
E + A = 5 + 1 = 6 mod 27 = 6
C + P = 3 + 16 = 19 mod 27 = 19

R + A = 18 + 1 = 19 mod 27 = 19
E + I = 5 + 9 = 14 mod 27 = 14
T + X = 20 + 24 = 44 mod 27 = 17

A new cipher text is generated "CFSSNQ" which is transferred to the receiver. The decryption is obtained by doing inverse XOR function. Ciphertext (Ci): CFSSNQ

C F S S N Q
3 6 19 19 14 17
Key (Ki): KAPAIX
K A P A I X
11 1 16 1 9 24

Decryption:

((ci-ki) mod 27) = plaintext numeric value.
(((ci-ki) mod 27) = numeric + mod = plaintext).
3 – 11 mod 27 = -8 + 27 =19.
6 – 1 mod 27 = 5.
19 – 16 mod 27 = 3.
19 – 1 mod 27 = 18.
14 – 9 mod 27 = 5.
17 – 24 mod 27 = -7 + 27 = 20.

Original plaintext:

19 5 3 18 5 20
S E C R E T

Finally the transmission is done by deriving session key through generalised Diffie Hellman key exchange protocol which is XOR'ed with the key values, encrypted data and is transferred to the receiver for decryption in a similar way. This proves that our method is more effective, elegant, robust and secure.

3.3 Generalized Diffie-Hellman Key exchange protocol:

The users A (Alice) and B (Bob) authenticatethemselves by exchanging 3 messages over a publicchannel [14]. This scheme is accomplished by using asimplified keyed hash function [15]. A hash function is a computationally efficient function mapping binary strings of arbitrary length to binary strings of some fixed length [14].

1. One time setup: Select and publish for common use a prime *p* chosen such that computation of discrete logarithms modulo *p* is infeasible and a generator *g* of the multiplicative group *p** *Z*

2. Protocol messages:

$A \cdot \ B$: h (g a mod (p) , Km, " A") (1)

$B \cdot \ A$: h (g b mod (p) , Km , "B") (2)

$A \cdot \ B$: h ((g ab mod (p)) (3)

3. Protocol Action:

Perform the following steps for each shared key required.

a) Alice chooses a random number *a* and compute *g a* mod (*p*) by hashing the value along with her identity "Alice" and the session key obtained from the server and sends it to Bob which we call as message (1).

b) Bob also chooses a random number *b* , computes *g b* mod (*p*) by hashing the value along with his identity "Bob" and the session key derived from the server is passed onto Alice as message (1).

c) Alice computes $g_{ab} \cdot \ (g_{b})_{a}$ mod (p) , and Bob computes $g_{ba} \cdot \ (g_{a})_{b}$ mod (p) . Since $g_{ab} \cdot \ g_{ba}$ mod (p) $\cdot \ K$, Alice and Bob now have a shared secret key *K* .

Once the session key is generated, it is XOR'ed with the key values, encrypted text and is passed on to the receiver for decryption in a similar way.

IV. RESULTS AND ANALYSIS

The multilevel encryption method is considered to besecure to brute force attack, frequency attack, statistical attack and known cipher text attack, etc. Also this method is simple, robust and can encrypt /decrypt confidential data without losing any key (computational/operational) in seconds and does not suffer from any mathematical complexities. The performance of multilevel encryption scheme is
Compared with the other existing algorithm in fig 4.

Factors AES BLOWFISH RC5 Proposed Multilevel Encryption

Block Size 128 Bits 128 Bits 128 Bits 256 Bits
Cipher Type Symmetric Cipher Symmetric Cipher Symmetric Cipher Symmetric Cipher and vigenere cipher

Key Length 128/192/256 Bits 128/192/256 Bits 128/192/256 Bits 128/192/256 Bits

Cryptanalysis Strong against
Differential

Strong against
Differential
Strong against
Differential
Strong against
Differential
Security Consider Secure Considered Secure Considered Secure Considered Highly
Secure
Possible Combinations 2128 2128 2128 2 512 (2256*4)
Time to Crack All
Possible Keys 1.02×1018 Yrs 1.02×1018 Yrs 1.02×1018 Yrs 4.08×1018 Yrs.

Fig: 4: Performance of Multilevel Encryption

V. CONCLUSION

Vigenere cipher regard as simplest and weakest method that mean it is very easy to detect by intruder. To overcome the limitations of this method, the proposed multilevel encryption scheme is used. Hence, the proposed algorithm becomes difficult to cryptanalyst. At the same time, the computational complexity is much lesser than most modern ciphers, making it a fit choice for light weight applications where resources are limited.

REFERENCES

[1] Polyalphabetic Cipher Techniques Used For Encryption Purpose,http://www.ijarcsse.com/docs/papers/Volume_3/ 2_February2013/V3 I2-0122.pdf.

[2] Security Analysis and Modification of Classical Encryption Scheme
by Maya Mohan, M. K. Kavitha Devi and V. Jeevan Prakash, I JST,
Vol 8(S8), 542–548, April 2015.

[3] Security Models and Proof Strategies for Plaintext Aware Encryption.Journal of Cryptology by Birkett J, Dent AW.. 2014;27(1):99–120.

[4] The security implementation of IPSec VPN [M] by CarItonR. Davis.

[5] http://www.webopedia.com/TERM/V/VPN.html

[6] Enhancing Security of Vigenere Cipher by Stream Cipher International Journal of Computer Applications by Fairouz MushtaqSher Ali, Falah Hassan Sarhan (0975 – 8887).

[7] Cryptology: From Caesar Ciphers to Public-Key Cryptosystems byLuciano, Dennis; Gordon Prichett (January 1987).. The CollegeMathematics Journal 18 (1): 2–17. doi:10.2307/2686311. JSTOR2686311.

[8] http://en.wikipedia.org/wiki/Caesar_cipher Caesar cipher. Retrievedfrom

[9] A Study of Encryption Algorithms (RSA, DES, 3DES and AES) forInformation Security International Journal of Computer Applicationsby Gurpreet Singh, Supriya, (0975 – 8887).

[10] Luciano, Dennis; Gordon Prichett (January 1987). "Cryptology:From Caesar Ciphers to Public-Key Cryptosystems". The CollegMathematics Journal 18 (1): 2–17. doi:10.2307/2686311. JSTOR2686311.

[11] [A cryptosystem based on Vigenère cipher with varying key, by Q.-Kester, International Journal of Advanced Research inComputer Engineering & Technology (IJARCET), vol. 1, pp. pp:108-113, 2012.
Developing a Modified Hybrid Caesar Cipher and Vigenere Cipherfor Secure Data Communication, by O. Omolara, et al.,ComputerEngineering and Intelligent Systems, vol. 5, pp. 34-46, 2014.

[12] Enhancing Security of Vigenere Cipher by Stream Cipher, by F. H.S. Fairouz Mushtaq Sher Ali, International Journal of ComputerApplications, vol.100, pp. 1-4, 2014.

[13] Handbook of applied cryptography, by A.Menezes, P.van Oorschot,S.Vanstone, CRC Press, Inc., 1997.

[14] HMAC: Keyed-Hashing for Message Authentication, by H.Krawczyk, M. Bellare, and R. Canetti, Internet Engineering TaskForce, Request for Comments (RFC) 2104, February 1997.