Volume 65, Issue 1, 2021
Journal of Scientific Research
Institute of Science,
Banaras Hindu University, Varanasi, India.

Elliptic Curve Layered: A Secure Polyalphabetic Vignere Cryptographic Algorithm for Textual Data

Deepika Bhatia* and Meenu Dave

Department of Computer Science, Jagannath University, Jaipur, India.
deepika.18850@gmail.com*, meenu.s.dave@gmail.com

Abstract: **Digital content is unsecured during public data transmission. Cryptography is a technique to provide data security to transfer user's information securely in a cloud computing environment without the intervention of a third party. Cryptographic methods provide data security and have become important nowadays to enhance the security of this digital data. Sensitive data and information when exchanged using the cloud services, lead to eavesdropping. Unauthorized access leads to data breach and various types of security attacks. A distributed network environment is very critical maintaining the confidentiality of the user's data. Cloud services provide encryption and decryption of data while transfer using the TLS protocol. But to use this feature a trusted third-party source is needed. Thus, data security gets affected in such a cloud infrastructure. This paper discusses various issues with different classical cryptography techniques and proposed a hybrid approach using symmetric and asymmetric key algorithm. A new combination of Vignere cipher and Elliptic curve is proposed and implemented and the result is analysed based upon Friedman test and Index of Coincidence. The results show that the novel method provides double layer security to user's data and information. More randomness and confusion have been added in the resulted ciphertext using the new scheme.**

Index Terms: **Cloud, Cryptography, Security, Technology, Text.**

I. INTRODUCTION

Cloud computing is a new computing paradigm providing various services to users. Different organizations are using services such as data sharing, processing, storage, application and computations etc. These services are provided using the cloud models such as System as a service (SaaS), Infrastructure as a service (IaaS), and platform as a service (PaaS). User's avail the benefit of such services when and wherever on-demand. Amazon, Google, Government organization and various companies are also using such services. Confidentiality of online data from the outer world is of prime importance nowadays. Data security is a big challenge and concern in this current scenario. Cryptographic (Diffie W. et al. 1976) algorithms play a crucial role in providing security of data shared via small sized smart IoT devices. Various real time applications such as messages, passwords, images, online transactions etc. can be secured using cryptology. Many cryptographic techniques are available in the market. These are classified into symmetric and asymmetric cipher techniques are discussed in brief: 1. Symmetric key methods use the same set of keys for encryption and decryption. It is also known as secret or private key cryptography. Polyalphabetic ciphers are the classifications of classical substitution symmetric key ciphers. Vignere cipher is an example of such methods. 2. Asymmetric key algorithm uses a public and private key pair for data security. It is also known as public-key cryptography. In this case, a public key is used for encryption and a private key is used by the receiver to decrypt and read the message. ECC method is a type of asymmetric key algorithm.

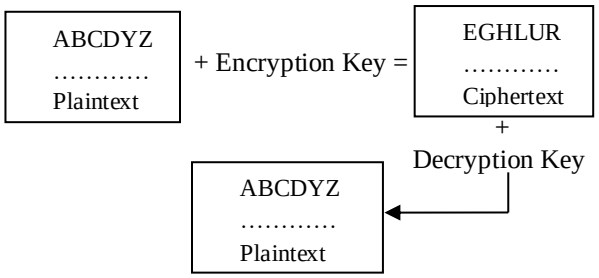

Fig.1: Encryption-Decryption Process

Data is encrypted and decrypted using a public-private key pair. During encryption, the plaintext sent by the sender is converted into ciphertext with the help of an encryption key. This ciphertext

* Corresponding Author

is decrypted using a decryption key. The complete process uses encryption and decryption key algorithms and is elaborated in the Fig.1 above.

Vignere cipher converts given plaintext into ASCII code for the English alphabets. The scheme alone is not much secured as it only provides data security and privacy but is hack-able. ECC is a fully homomorphic scheme that can perform various number of addition and multiplication operations over the given data. It uses a public and private key pair for encryption and also increases the security level both at cloud customer and service provider side. ECC provides data authentication, integrity and confidentiality as compared to Vignere alone that provides only customer side security of information. In this paper, Vignere cipher is studied and implemented in detail and its security level has been improved with the help of Elliptic Curve Cryptography (ECC) technique.

II. LITERATURE REVIEW

This section provides the literature review related to comparative research conducted on Cryptographic techniques by different authors.

An asymmetric cryptosystem is given and also implemented. The Diffie-Hellman key exchange distribution method while proposing a novel signature scheme is suggested by the author (ElGamal T. 1985). The schemes are based upon the solvable difficulty of discrete logarithmic problems. The methods are based upon finite fields over prime numbers. The author proposed a new digital signing scheme giving its verification. Various attacks such as to discover the value of a prime number, and to forge signatures are performed over this new approach. The scheme is compared with other cryptosystems like RSA. It has been observed that the new scheme offers benefits such as greater file sizes and larger cipher size as compared to RSA cryptosystem justifying the advantages of this scheme over security aspects.

A new mechanism is introduced (Paillier et al. 1999) for trapdoor function, and also a novel number-theoretic problem is given. Two new schemes such as trapdoor permutation and homomorphic probabilistic schemes were designed and implemented and it is proved that this new approach gives better results compared to the RSA scheme. The author chose a Composite Residuosity Class (CRC) Problem to investigate the number theory framework. A new probabilistic encryption mechanism based upon the CRC problem is proposed which used the factorization method as a trapdoor function. So, it is a kind of one-way trapdoor method that makes the scheme comparatively secured. The authors used the Chinese Remainder Theorem and random number generation method for faster key generation, modular exponentiation schemes for encryption, and decryption process. Encryption and decryption of input are checked on various levels of prime numbers. The additive homomorphic property is exhibited by the new scheme. It has been suggested that in future chosen-ciphertext attacks should be worked upon and homomorphic properties of the proposed technique can be an area of further research in a distributed environment.

A fully homomorphic encryption method is proposed (Gentry C. 2009) using additive and multiplicative properties for digital data encryption and decryption. The author evaluated arbitrary circuits. Asymmetric encryption based upon ideal lattices with low circuit complexity using fully homomorphic properties is evaluated. The author also presented an improved version of the scheme using ideal lattices later on.

Suggested improvement over homomorphic encryption is done by Gentry (Liangliang Xiao et al. 2012). To prevent collusion between a few users and the server to derive the master key, one or more key agents can be added to mediate and resolve (if any issue) during the multiparty interaction. Earlier Gentry's homomorphic encryption scheme took more than 900 seconds to add two 32-bit numbers, and more than 67000 seconds to multiply them. The results showed that by implementing this novel approach multiplication takes took 108 milliseconds and addition took 1024.

Secure multi-party computation based upon the ECC, Elliptic Curve Cryptography, technique is given (Hong Q. M. et al. 2016). It has been observed that trusting the third party over the cloud environment is a big issue for data security. Thus, ECC scheme is introduced that reduces computation and communication overheads and introduces data privacy. The proposed method is compared with other asymmetric encryption techniques based upon GPS data of earthquake and the results showed outstanding performance.

Various optimization algorithms such as swarm or grasshopper optimization method and PSO i.e. Particle Swarm Optimization algorithms were implemented to secure medical images data (Elhoseny Mohamed et al., 2018). As this medical data is publicly available on the cloud, so the authors emphasized the security of patient's information and d medical images. The author compared various cryptographic algorithms such as RSA, AES, ECC, ECC with PSO, ECC with Genetic optimization, and ECC with Cuckoo search optimization are compared with each other and GO with PSO yields the best performance.

The Least Significant Bit (LSB) approach is used to hide messages (Ariyus Dony et al. 2019) into images to improve its security. The author used the Image dataset and implemented the method on social media like Google drive, Whatsapp, and Facebook, etc. Vignere substitution cipher is embedded with the LSB method. Vignere, Hill Cipher, Caesar, and One Time Pad algorithms have been modified by the authors.

The k-means clustering algorithm that partitions the keyword and is used as an index to search data in a hybrid cloud computing environment. The authors (Hua Dai et al. 2020) also proposed the improved version of the algorithms combining it with a complete binary pruning tree. It boosts the search efficiency of the previous approach. The new approach is evaluated in comparison with the FMRS scheme and gives better performance over search time cost and other parameters such as space and average number of keywords.

Different authors discussed (Seongmin Park et al. 2019) that Vignere cipher can be attacked if it is broken into smaller shift ciphers. Frequency analysis can be done easily by the hacker and data security may be breached. The authors implemented a twist algorithm and also gave its improved version to attack the Vignere cipher.

III. PROPOSED METHODOLOGY

In this research paper, a novel Polyalphabetic Vignere Elliptic Curve Cryptography technique is proposed. Vignere cipher is a type of Polyalphabetic substitution cipher and is a classical encryption approach. Initially, Vignere Table 1 is generated for 26 alphabets for the English language. The first row and column of the table show the plaintext and keywords combination. There are 26*26 entries in the table. Alphabet 'A' to 'Z' is taken in the top row which shows the plaintext. These 26 alphabets taken as a first column on the left-hand side of the table shows keyword characters. The intersection of plaintext and keyword character shows the resultant ciphertext. The Left circular shift is applied to fill these rows of the Vignere table. The entire plaintext is encrypted and decrypted using this repeated process. The process involves Encryption and decryption of user's data using Vignere method and is discussed below:

Vignere Encryption Process: In the Encryption process, the sender encrypts the message with his own randomly generated private key. Ci is the array of cipher text characters which get generated after applying key Ki over the plaintext. In the formula given below, Pi depicts the plaintext letter and Ki is the key letter array similar to be applied for encryption or decryption.

$$Ci = Encryption\ (Pi) = (Pi + Ki)\ mod\ 26$$

Vignere Decryption Process: During the Decryption process at the receiver side, the applied key Ki at the sender side, is subtracted from the received ciphertext Ci array of characters. Thus, Pi plaintext is received by the receiver in a secured manner.

$$Pi = Decryption\ (Ci) = (Ci - Ki)\ mod\ 26$$

Table 1. Vignere Cipher Table for English Alphabets

	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**
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Both the processes are performed using a mathematical modulo operation. Here key applied is in the form of alphabetic characters. Modulo-26 arithmetic is applied for computations. Vignere ciphers are generated using the above formulas for English capital alphabets taken as input. For example, let the user wants to encrypt the message "MORNING" using the keyword "HELLO".

In this case, the length of the keyword is lesser than the plaintext. So, the keyword is repeated to make it as equal in length with the plaintext. The Vignere Encryption and Decryption process is shown below in Table 2.

Table 2. Vignere Ciphertext Generation

Plaintext	Keyword	Ciphertext
M	H	T
O	E	S
R	L	C
N	L	Y
I	O	W
N	H	U
G	E	K

The plaintext message "MORNING" is encrypted as "TSCYWUK" using the Vignere encryption formula. The decryption process is the reverse of encryption. Vignere decryption formula is applied here to regenerate the plaintext. In this case, the keyword and ciphertext pair is used to find the plaintext. For example, the ciphertext 'T' and keyword 'H' will give the plaintext 'M'. This process is repeated to find the plaintext message "MORNING".

It is very difficult to break Vignere substitution cipher (Stalling William 2005) with the help of statistical analysis but still, it can leak user's data and information. Earlier Vignere cipher (Kartha S. et al. 2020) is considered to be unbreakable when longer key sizes were used. But if shorter keys are used, or if the size of plaintext is larger than the key length, it becomes trackable. Thus, Vignere cipher becomes unsecured over shorter key sizes. This paper improves the security level by using Elliptic Curve Cryptography (ECC) technique with Vignere ciphers. Elliptic Curves are secured as it performs a one-way trapdoor function which adds complex calculations to the computed ciphertext.

Polyalphabetic Vignere Elliptic Curve Cipher Algorithm: The new approach named Polyalphabetic Vignere Elliptic Curve Cipher Technique overcomes the weakness of Vignere cipher. This method is based upon Elliptic Curves (EC). These curves are considered to be secured by various researchers. Elliptic curves are generated using the formula:

$$y^2 = x^3 + a*x + b \text{ modulo } p$$

Here a, and b are constants and 'p' is a large prime number agreed upon between two users.

Algorithm: The algorithmic steps for the novel Polyalphabetic Vignere Elliptic Curve Cipher Technique are given below:

Step 1: Data is encrypted using Vignere cipher first and ciphertext is doubly encrypted using the Elliptic curve encryption method given below.

Step 2: Encoding of data is done with the help of the Koblitz method. Enciphered Text data is converted into 'x' and 'y' coordinates over the Elliptic Curve.

Step 3: After that these coordinates are sent to the receiver for decoding and decryption process. This encoding of data increases its security against adversaries.

Step 4: At the receiver's side, the data is first decrypted and the decoding process is applied to it.

Step 5: Vignere deciphering is applied to this enciphered text data using the same key as was used for Vignere encryption process.

Step 6: The receiver can now read the data sent by the sender.

Now, the ECC encryption-decryption (Moncef Amara et al. 2011) process is applied to generate the Vignere input text, is explained below:

ECC- Encryption process: The Vignere ciphertext is sent over the ECC curve in encrypted form using specified parameters. Let 'Pm' is the Vignere encrypted message, 'Pb' is the public key of the receiver shared using the ECC-Diffie-Hellman key exchange algorithm (DHKE). 'k' is the chosen parameter and this value should be $1 < k < p$, where p is prime modulo for the given Elliptic Curve. 'G' is the generator point of the curve. 'Pc' is the generated ciphertext.

$$\mathbf{Pc = [k * G, Pm + k * Pb]}$$

ECC-Decryption process: Plaintext is obtained by the receiver using the following formula. Where, 'β' is the private key of the receiver.

$$\mathbf{P_m = [P_m + k * B] - \beta * k * G}$$
$$\mathbf{= [P_m + k * (\beta * G)] - \beta * k * G}$$
$$\mathbf{= P_m}$$

'Pm' is the message obtained after the decryption process. This message is decoded with the help of the Koblitz method.

IV. RESULTS AND DISCUSSION

Elliptic Curve Cryptography technique is implemented and the results have been shown in Table 3 below. It shows the encoded (x, y) coordinate values for English capital alphabet symbols. The curve chosen to generate it is given below:

$$y^2 = x^3 + 2x + 2 \text{ modulo } 1213$$

Modulo prime value of 1213 is chosen to implement the algorithm. In this case, 'G' = (37, 47) is the generator point agreed

between two users on the Elliptic curve. The Elliptic curve for the given equations generates 1219 finite fields over the cyclic Abelian group. Example: The encoded value of the alphabet 'K' is (113:436) calculated. ASCII values are also shown in the table for all the English language capital alphabets.

Table 3. Encoded Values of English Alphabets

English Alphabets with ASCII code and Encoded x, y-coordinates value on the given Elliptic Curve with a=b=2 and modulo 1213.				**Symbol**	**A**	**B**
				Encode	(14: 541)	(21: 381)
				ASCII	65	66
Sym	**C**	**D**	**E**	**F**	**G**	**H**
Enc	(32: 36)	(41: 77)	(51: 460)	(61: 525)	(72:91)	(81: 465)
AS	67	68	69	70	71	72
Sym	**I**	**J**	**K**	**L**	**M**	**N**
Enc	(93: 511)	(101: 376)	(113: 436)	(121: 243)	(131: 150)	(142:311)
AS	73	74	75	76	77	78
Sym	**O**	**P**	**Q**	**R**	**S**	**T**
Enc	(15 1: 395)	(16 1: 260)	(175: 548)	(181: 31)	(191:205)	(201:110)
AS.	79	80	81	82	83	84
Sym	**U**	**V**	**W**	**X**	**Y**	**Z**
Enc	(21 1: 353)	(22 5: 528)	(233: 482)	(242:229)	(257: 40)	(261: 174)
AS.	85	86	87	88	89	90
*Sym – Symbol, *Enc- Encoded Value, *AS. – ASCII						

The Elliptic points are generated for the given curve parameters. Fig. 2 above also shows the distribution of these points on the Elliptic curve. Character mapping of curve points shows uniform distribution of user's data increasing its security from the third-party service provider.

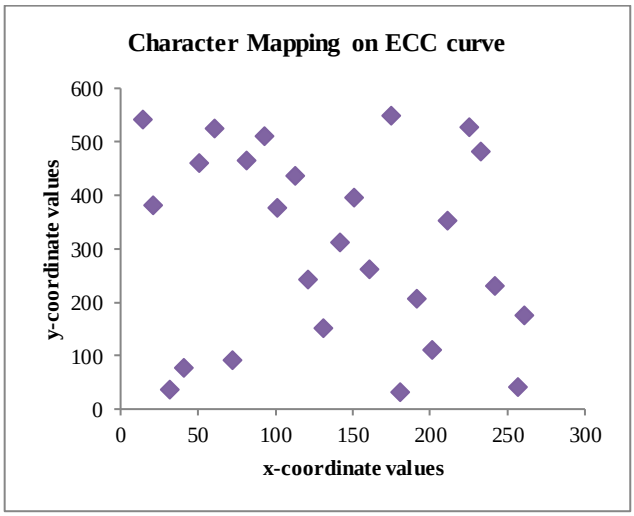

Fig.2: Character mapping of Elliptic Curve points

Polyalphabetic Vignere Elliptic Curve Cipher Encryption Process: Vignere encryption formula is applied on the plaintext and after that ECC encryption is applied. In this case, the private key chosen over here is '3'. For the given curve parameters, the user's data is encrypted with the help of Vignere encryption key. Steps for Polyalphabetic Vignere Elliptic Curve Cipher encryption process are given below:

1. Let us chose Vignere key for encryption as 'HILL'.
2. Encryption key using Vignere cipher is generated using the Vignere key repetition logic and this key is calculated in '0' milliseconds and Vignere encryption time taken using this key is computed as 1.76923 milliseconds.
3. Public key for ECC encryption is generated and shared via cloud domain. User's data is now encrypted using this public key. The point calculated over the Elliptic curve is given as (537:1032). ECC-Key generation time is 0.002 seconds.
4. Now sender chooses the encoding key value as '10'.
5. Let us assume that text data to be encrypted is: "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
6. The data is encrypted using the Vignere key 'HILL'. The output generated is "HJNOLNRSPRVWTVZAX ZDEBDHIFH"
7. This encrypted data is doubly encrypted using ECC curve parameters making it secure. So two-tier encryption is applied to the user's input.
8. Time taken for level one encryption is calculated as 15.6538 milliseconds.
9. ECC encoding time is 2.30769 milliseconds.
10. The encoded data is sent using public media to the recipient.

Polyalphabetic Vignere Elliptic Curve Cipher Decryption: Encoded data is received by the client and the reverse process is applied for decryption. The data is decoded with the help of the receiver's private key. Authorization of users is checked with the help of a shared secret key. A shared secret key is matched first at both ends. If the key is not similar on both sides, the data can't be decrypted by the client. Thus, the decryption process is also secured. It will work only for authorized users. Steps for Polyalphabetic Vignere Elliptic Curve Cipher decryption process are given below:

1 The recipient chooses a random private key. The public key is generated with the help of chosen curve parameters in 0.002 seconds.
2 The public key for decryption is (1020:1032).
3 The input file received is of 281 bytes.
4 Now the receiver chooses an encoding key and encryption key.
5 The curve points for the encoded values are generated by the receiver too.
6 The generated decoded file is given as:- "HJNOLNRSPRVWTVZAXZDEBDHIFH"
7 ECC decryption time to decrypt this file is 1.00 milliseconds and decoding time is 9.6385 milliseconds.

8 Now the user applies the decryption key "HILL" and receives the decrypted message as "ABCDEFGHIJKLMNOPQRSTUVWXYZ".
9 Vignere cipher decryption time is 0.576923 milliseconds.
10 The data has been successfully decrypted at the receiver's side.

Table 4 below shows different performance parameters for the suggested approach. The size of the text file and the key length are taken in bytes. Vignere and ECC encryption-decryption time are calculated in milliseconds. The time taken for the ECC key generation is in seconds.

Table 4. Analysis of Performance parameters

Polyalphabetic Vignere Elliptic Curve Cipher Technique	
Text File Size	26
Key Length	4
Vignere Encryption Time	1.76923
Vignere Decryption Time	0.576923
ECC Key Generation Time	0.002
ECC Encryption Time	15.6538
ECC Decryption Time	1

Table 5 below also shows the encoding and decoding time (in milliseconds) taken by the Elliptic Curve algorithm using the same curve parameters. The size of the EC encipher file is computed as 281 bytes.

Table 5. EC Encoding-Decoding Time

Polyalphabetic Vignere Elliptic Curve Cipher Technique	
Encipher file size	281
Encoding Time	2.30769
Decoding Time	9.6385
Total Time Taken	11.94619

V. RESULTS AND ANALYSIS

In the research paper, the Cryptanalysis of Vignere cipher is done by obtaining the length of the applied key. In Vignere ciphers, there are 26^n ways to encrypt the given message with the keyword of length 'n'. So, the encryption process is considered secure. Mapping of plaintext and ciphertext gives a random sequence of ciphertexts. Friedman in 1863, tried to attack the Vignere cipher. The key length once estimated leads to a security breach. The data is analyzed based upon the Friedman test for the key length estimation. Statistical analysis can be done to break the Vignere cipher. Friedman test and Index of Coincidence is computed for the proposed approach. After applying the Elliptic Curve Cryptographic technique with Vignere cipher, the results show that data becomes safer, secured, and authenticated. Friedman test and Index of Coincidence are explained below:

1. ***Friedman Test for the Key length estimation:*** Friedman test (Seongmin Park et al. 2019) is used to find the length of the applied key. The key length of the keyword is estimated using the following Friedman's equation:

$$l = (0.027*n) / ((n-1) * I - 0.038*n + 0.065)$$

Here, '*l*' is the estimated length of the key applied. 'n' is total letters in the ciphertext (26 letters considered for the English language).

'I' is the index of coincidence calculated using the formula given in equation (i) given below. The value = 0.065 is IOC for the English language.

For example, using the key "HILL" and the input characters "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

The Key length estimated using this test and formula given above is 2 or 3. The length of the encrypted file is 26. Thus, it confuses the attacker and it is difficult to find the correct key length using the Friedman test.

2. ***The Index of Coincidence (IOC):*** Index of Coincidence is defined as a measure of similarity index of frequency distribution to that of uniform distribution of letters. It is given as:

$$I.O.C. = \sum_{i=1}^{26} fi\,(fi-1) / (n\,(n-1)) \qquad (i)$$

Here, fi is the frequency of letter occurring in the sent ciphertext message. 'n' is the total length of the alphabets. 'i' is the iteration counter from 1 to 26 as in case of 26 English alphabets.

IOC is the probability of selecting two similar letters. It is different for different languages. For example, for the English language approx. 0.06 and for Spanish it is 0.072. This value should be less to hide the structure of given text. The resultant ciphertext is analyzed based upon IOC (Seongmin Park et al. 2019). Various parameters are calculated for the given problem. The index of coincidence using Vignere cipher is calculated as 0.0246154. This value induces confusion and diffusion in the plaintext and thus increases the security level of the ciphertext against the adversary attacks.

Length of the Vignere-Key Encrypted file is:
N = 26
Friedman Test Key-Length is = 2.28207
Length of the estimated Vignere Keyword= 3 or 2
Index of Coincidence (IOC) = 0.0246154

Conclusion And Future Work

In this paper, Vignere cipher is implemented in combination with the Elliptic curve cryptography technique. The problems of Vignere cipher are overcome with the help of the ECC algorithm. Double-layered security architecture is proposed. Using the ECC method over the Vignere cipher increases the security level. The proposed method encrypts and decrypts English alphabet characters but, in the near future it can be enhanced for other languages such as German, French, etc. Furthermore, this method can also be implemented for digits, space, and special characters. The method is considered to be cost effective and efficient for small sized and memory constrained devices. It can be used in the case of smart IoT and wireless devices as it provides greater bandwidth and thus less battery consumption for such devices. It improves the security level of user's data and also, a greater number of users can share their data using the common digital communication channel. The method also shows improvement over decryption time using the Elliptic curve method and key generation time is also minimal.

Acknowledgement

I would like to thank my advisor, Professor Dr. Meenu Dave, for her continuous support and guidance to conduct this research work. I like to thanks Vivekananda Institute of Professional Studies (VIPS), New Delhi, for providing me all the required facilities to complete experimentation and computations related to the research work.

References

Diffie W., & Hellman M. (1976). New directions in cryptography *IEEE Trans. Inform. Theo., Vol. 22*, 644–654.

ElGamal T. (1985), A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Trans. Information Theory, Vol.-31*, No.4, 469–472.

Pascal and Paillier (1999), Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. *J. Stern (Ed.): EUROCRYPT'99, LNCS 1592*, Springer-Verlag Berlin Heidelberg, 223-238.

Lauter K. (2004), The advantages of elliptic curve cryptography for wireless security. *IEEE Wireless Commun., Vol. 11*(1), 62-67.

Gentry C. (2009), Fully Homomorphic Encryption Using Ideal Lattices. *Proc. 41st Ann. ACM Symp. Theory of Computing (STOC 09)*, 169–178.

Gentry Craig and Halevi Shai (2011), Implementing gentry's fully-homomorphic encryption scheme. *In Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'11).* Lecture Notes in Computer Science, Springer, Berlin, *Vol. 6632*, 29–148.

Liangliang Xiao, Osbert Bastani, Ling Yen (2012), An Efficient Homomorphic Encryption Protocol for Multi-User Systems.

Hong Q. M., Zhao B. W., Wang Y. P. (2016), Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing. *2nd International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, IEEE International Conference on Intelligent Data and Security*, 152-157.

Elhoseny Mohamed, Shankar K., Lakshmanaprabu K. S., Maseleno Andino, Arunkumar N. (2018), Hybrid optimization with cryptography encryption for medical image security in Internet of Things. *Neural Computing and Applications, https://doi.org/10.1007/s00521-018-3801-x, Springer*,1-15.

Elhoseny M, Abdelaziz A, Salama AS, Riad AM, Muhammad K, Sangaiah, (2018), A hybrid model of internet of things and cloud computing to manage big data in health services applications. *Future Gener Comput Syst 86*, pp. 1383–1394.

Al Hasib A., & Haque AAMM (2008), A comparative study of the performance and security issues of AES and RSA cryptography. *Third international conference on convergence and hybrid information technology*, ICCIT'08, *Vol 2. IEEE*, 505–510.

Shankar K, & Eswaran (2016), An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm. *Adv Intell Syst Comput Springer 394*, 705–714.

Ariyus Dony, & Ardiansyah (2019), Optimization Substitution Cipher and Hidden Plaintext in Image Data Using LSB Method. *IOP Conf. Series: Journal of Physics: Conf. Series 1201, 012033, doi:10.1088/1742-6596/1201/1/012033, International Conference on Electronics Representation and Algorithm (ICERA 2019) IOP Publishing*, 1-10.

Hua Dai, Yan Ji, Geng Yang, Haiping Huang, And Xun Yi (2020), A Privacy-Preserving Multi-Keyword Ranked Search Over Encrypted Data in Hybrid Clouds. *Digital Object Identifier 10.1109/ACCESS.2019.2963096, Vol. 8, IEEE*, 4895-4907.

Yang Y., Liu J., Cai S., and Yang S. (2017), Fast multi-keyword semantic ranked search in cloud computing, *Chinese Journal of Computers, Vol. 40*, 158–171.

Seongmin Park, Juneyeun Kim, Kookrae Cho & Dae Hyun Yum To (2019), Finding the key length of a Vigenère cipher: How to improve the twist algorithm. *ISSN: 0161-1194 (Print) 1558-1586(Online), DOI:10.1080/01611194.2019.1657202, Taylor & Francis Group, LLC*, 1-9.

Stallings William (2005), Cryptography and Network Security Principles and Practices. *Fourth Edition, Prentice-Hall*.

Kartha S. Ranju, Paul Varghese (2020), New Polyalphabetic Substitution Scheme for Secure Communication. *International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, DOI:10.35940/ijitee .C9043.019320, Vol.-9*, Issue-3, 3303-3310.

Leelavathi G, Shaila K, & Venugopal K R. (2016), Elliptic Curve Cryptography Implementation on FPGA using Montgomery Multiplication for Equal Key and Data size over GF(2m) for Wireless Sensor Networks. *IEEE Region 10 Conference (TENCON) — Proceedings of the International Conference*, 978-1-5090-2597-8/16, IEEE, 468-471.

Qizhi Q., & Qianxing Xiong (2003), Research on Elliptic Curve Cryptography. *The 8th International Conference on Computer Supported Cooperative Work in Design Proceedings, 0-7803-794 1 -1/03, IEEE,* 698-701.

Moncef Amara, & Amar S. (2011), Elliptic Curve Cryptography and Its Applications. *7th International Workshop on Systems, Signal Processing and their Applications (WOSSPA), 978-1-4577-0690-5/11, IEEE,* 247-250.

Shabieh F., Ayesha S., & Nazeer Muhammad (2020), A Novel Application of Elliptic Curves in the Dynamical Components of Block Ciphers. *Wireless Personal Communications https://doi.org/10.1007/s11277-020-07628-0,* 1-8.

Rijswijk-Deij Van R., Hageman K., & Sperotto A., Pras A. (2017), The Performance Impact of Elliptic Curve Cryptography on DNSSEC Validation, In *IEEE/ACM Transactions on Networking*, April, *Vol. 25*, Issue 2.

***