THREE PASS PROTOCOL IMPLEMENTATION USING NUMBER CIPHER ENCRYPTION IN A COMMUNICATION NETWORK

V.Joseph Emmanuvel[1]
Research Scholar, Department of CS, CA & IT
Karpagam Academy of Higher Education
Coimbatore, Tamilnadu, India
Email: josejan1978@gmail,.com

E.J.Thomson Fredrik[2]
Professor, Department of CS, CA & IT
Karpagam Academy of Higher Education
Coimbatore, Tamilnadu, India
Email: thomson500@gmail.com

ABSTRACT: The foremost responsibility of Cryptography in Network Security is to ensure safety measures to the information by allowing confidentiality, integrity and authentication. More in general, cryptography is a process to construct, evaluate, investigate and analyze protocols that put off intruding inquisitive people or the spiteful public who intend to read private messages. The three pass protocol's fundamental acuity is that each one has a private encryption and decryption key where the keys are utilized autonomously, first to encrypt and then to decrypt the message. The protocol makes use of an encryption function E and a decryption function D. the main thing to be noted is that the encryption and decryption activity occurs three times using the same input or various keys in both the ends. In this research paper, a novel technique has been projected to implement three pass which will use mathematical numbers series concepts while encrypting and decrypting the message in a communication channel.

KEYWORDS: Cryptography, Encryption, Decryption, Number Series Cipher, Three Pass Protocol

I. INTRODUCTION

The discovery of personal computers has been a spinning point in the history of human life. Next has the succeeding invention of internetwork which has made some astounding variances in the day to day human life. These innovative inventions have made the human beings to make their necessities and works so easy. Moreover, the time and work have been enormously reduced to perform a work. In general, computers have the capability to t up great quantity of data and are far better than the human brain. Budding field of information technology and communications technologies are drastically changing the traditions in which we communicate and swap information. Using Internet facility, one can communicate with any one in any place in the world. Because the storage capability of computers is high, data security is mostly required to defend the information while it is being transferred in a communication channel. Using internet facility there are more than a few chances for the inquisitive people to interfere and capture the message, other than the sender and receiver. We cannot bring to an end these nosy human beings in intruding into others communication. The simply way to safe guard our message is to send it in a dissimilar format, where the sender and receiver can only know the unique message. Cryptography is the study of several mathematical techniques which concentrates on secrecy and data integrity [1]. An original communication is called the plain text and the coded message is known as the Cipher Text. Data encryption is a process of converting the plain text to cipher text which is also referred as enciphering. Restoring back the plain text from the cipher text is called deciphering or decryption. Many of the algorithms used in cryptography algorithms necessitate the establishment of shared keying material in advance. A strong encryption algorithm is needed to secure our message. The algorithm should be developed in such a way that an intruder who aims to know the algorithm finds very much difficult to decipher the cipher text or figure out the key [2]. The existing three pass algorithms use only the same keys in all the three steps of encryption. In this observe, to overcome above limitations in present system a new three pass protocol implementation using number cipher encryption has been projected that uses the symmetric key algorithm which uses different keys in each pass.

II. LITERATURE SURVEY

There are two most important types of encryption techniques in cryptography one is Symmetric and the further is an asymmetric encryption.

Symmetric and Asymmetric Encryption

Symmetric encryption is a form of cryptosystem in which encryption and decryption are

performed using the same key and it is also known as conventional encryption. This technique transforms plaintext into cipher text using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plain text is recovered from the cipher text [2]. Symmetric systems contain Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish algorithm which make use of a one and the same key for the sender and receiver. Symmetric key cryptography is furthermore referred to as secret key [3]. Asymmetric encryption is called as public key cryptography where the individuals at the source and destination use dissimilar keys for encrypting and decrypting purposes. This type of encryption contains SSL, DH, RSA and SSH algorithms [4].

In [5] Andizhan Putera Utama Siahaan proposed a new Protocol perception using Three-Pass implementation in Hill Cipher Encryption where 2X2 square matrix has been used as a key.

In [6] Amin Subandi, et al, 2017 suggested yet another Protocol Implementation using the same three pass in Vigenere Cipher Classic Cryptography Algorithm where the researchers introduced a 26X26 matrix representation as the key.

In [7] Boni Oktavianab, et al introduced a cryptographic technique which uses the Three-Pass Protocol Implementation but it is with the help of Caesar Cipher Cryptography where the key used has been 3 with shift values of 5 and 4 respectively. But this method uses the same key in all the three passes.

III. PROPOSED WORK

In the proposed work, a new three pass protocol implementation technique has been analyzed in which we use mathematical number series for encryption and decryptions processes. Odd number series, prime number series and Fibonacci number series are used in the first, second and third pass of encryption respectively.

Pass – 1: 1, 3, 5, 7, 9, …….. Key 1 (K1)
Pass – 2: 1, 2, 3, 5, 7, 11, …… Key 2 (K2)
Pass – 3: 0, 1, 1, 2, 3, 5, 8, …….. Key 3 (K3)

C1 = (PT1 + K1) Mod 26 ---------→ Pass - 1
Where C1 = Cipher Text1, K1 = Key and 26 is the total number of English alphabets.

Similarly,
C2 = (PT2 + K2) Mod 26 ---------→ Pass - 2
C31 = (PT3 + K3) Mod 26 ---------→ Pass – 3

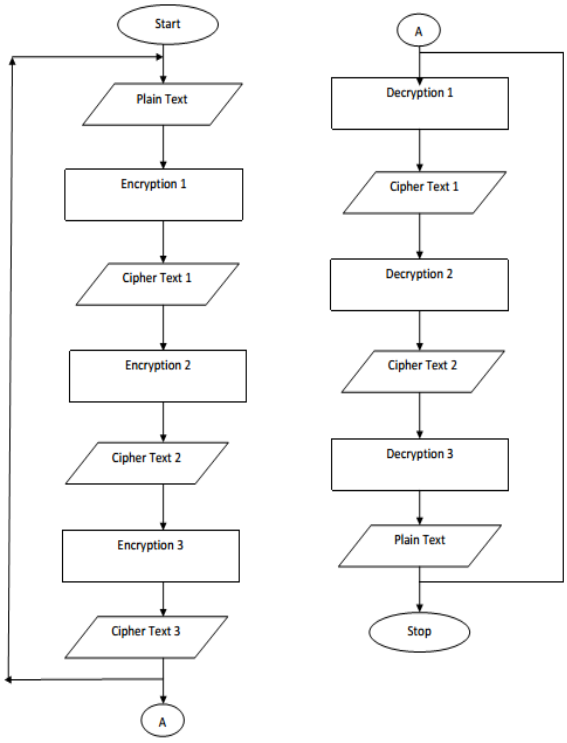

Figure – 1 Three Pass Protocol Scheme

IV. TESTING AND IMPLEMENTATION

The three pass protocol implementation scheme using number series cipher has been implemented in this section. Consider the example given below. Let us take into account the following text as the Plain text.

PLAIN TEXT: RESEARCH IS CREATING NEW KNOWLEDGE

First the key taken is an odd number series. Then the second and the third keys will be prime number and Fibonacci number sequence. Hence the encryption happens three times as per the keys used and the encryption process is as follows.

Table – 1: Encryption in First Pass

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

In the above table, the plain text is encrypted by odd number series in the first pass and the encrypted text is SHXLJCPW ZL NODFWNUP YWL HMRBSNOTT.

Table – 2: Encryption in Second Pass

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

In the above table, the plain text is encrypted by prime number series in the second pass and the encrypted text is TJAQQNCN WO ATOVNIVW ILZ CNWKLKNWY.

Table – 3: Encryption in Third Pass

ENCRYPTION									
PT	T	J	A	Q	Q	N	C	N	
CT	T	K	B	S	T	S	K	A	
PT	W	O							
CT	R	W							
PT	A	T	O	V	N	I	V	W	
CT	D	E	C	U	A	U	U	H	
PT	I	L	Z						
CT	S	G	E						
PT	C	N	W	K	L	K	N	W	Y
CT	C	S	B	Z	K	Y	A	V	M

In the above table, the plain text is encrypted by Fibonacci number series in the third pass and the encrypted text is TKBSTSKA RW DECUAUUH GE CSBZKYAVM.

The receiver can read the exact message by decrypting the cipher text three times in the reverse order. The reverse order in the three passes will be Fibonacci series, prime number series and the odd number series respectively.

Table – 4: Decryption in Third Pass

DECRYPTION									
CT	T	K	B	S	T	S	K	A	
PT	T	J	A	Q	Q	N	C	N	
CT	R	W							
PT	W	O							
CT	D	E	C	U	A	U	U	H	
PT	A	T	O	V	N	I	V	W	
CT	S	G	E						
PT	I	L	Z						
CT	C	S	B	Z	K	Y	A	V	M
PT	C	N	W	K	L	K	N	W	Y

The cipher text is still unreadable since another two passes of decryption is pending. The following table gives a clear picture of the decryption process using the prime number series in the second pass.

Table – 5: Decryption in Second Pass

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

In the final first pass, the cipher text is converted into the readable natural text in the reverse order using the key which is the odd number series.

Table – 6: Decryption in First Pass

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

Hence the final plain text obtained after the three pass decryption process is **RESEARCH IS NEW KNOWLEDGE.**

V. CONCLUSION

The proposed three pass protocol implementation using number cipher encryption is a secured way of transferring the information in a communication channel ensuring on how to make text message unreadable. By using the number series in three different ways, the three-Pass Protocol cipher text resulted is guaranteed. From the undergone research, it has been found that by using the keys differently in all the three passes this mechanism confirms more security when compared to the already existing schemes.

VI. REFERENCES

[1] A.Joseph Amalraj & Dr.J.John Rabin Jose, "A Survey Paper On Cryptography Techniques", International Journal of Computer Science and Mobile Computing, ISSN 2320–088X, IMPACT FACTOR: 5.258 Vol.5 Issue.8, August- 2016, pg. 55-59,

[2] William Stallings, "Cryptography and Network Security – Principles and Practices", Fourth Edition, 2006, Pearson Education, Prantice Hall, ISBN 81-7758-774 9.

[3] Priya Thakur & Anurag Rana, " A Symmetrical key Cryptography Analysis using Blowfish Algorithm", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 5 Issue 07, July-2016.

[4] Ayushi, "A Symmetric Key Cryptographic Algorithm"; International Journal of Computer Applications (0975 - 8887), Volume 1 – No. 15, 2010.

[5] Andizhan Putera Utama Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391, Volume 5 Issue 7, July 2016.

[6] Amin Subandi, Rini Meiyanti, Cut Lika Mestika Sandy & Rahmat Widia Sembiring." Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Key stream Generator Modification", Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 5, 1-5 (2017).

[7] Boni Oktavianab & Andysah Putera Utama Siahaan, "Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. III (Jul.-Aug. 2016), PP 26-29.

[8] A. A. Khalaf, M. S. A E.Karim Dan & H. F. A. Hamed, "A Triple Hill Cipher Algorithm Proposed to Increase the Security of Encrypted Binary Data and its Implementation Using FPGA," ICACT Transactions on Advanced Communications Technology, vol. 5, no. 1, pp. 752-757, 2016.