ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.5, Special Issue 2, April 2017

An International Conference on Recent Trends in IT Innovations - Tec'afe 2017

Organized by

Dept. of Computer Science, Garden City University, Bangalore-560049, India

Crypto Matrix Symmetric Multi Level Cipher (Cmsml)

Vinay S, Naveen Kumar P S

DOS in Computer Science, Davanagere University, Shivagangotri, Davanager, India

DOS in Computer Science, Davanagere University, Shivagangotri, Davanager, India

ABSTRACT: Transmission of Confidential data in the network should be secured from passive and active attacks. This paper presents a new technique to secure data against all type of threats .Here multiple private keys are used to perform encryption/decryption. Only one symmetric key is shared to receiver and remaining keys will be generated by this shared .Principles of both bit cipher & byte cipher methods with implementation of and basic transposition, substitution methods at different levels to obtain cipher text. To ensure integrity of data &detect errors or modification of message during transmission the Two dimensional parity bit method is used.

KEYWORDS: Symmetric key, Bit cipher, Block Cipher, Plain text, Cipher text, parity bit.

I. INTRODUCTION

Cryptography is a science of Securing confidential data against intruders. Increase in number, size of the encryption key and chain encryption increases the confidentiality of data.

This paper presents a cryptographic package where symmetric key encryption is applied with chain encryption using multiple keys. Whereas multiples symmetric keys are generated by one symmetric key which is shared on either side communication parties. A key matrix is prepared as per pre- negotiated standards between communicating parties, this matrix is used as base to perform encryption and decryption.

In a chain of encryptions at each level different keys are used. Basic principles of transposition and substitution method are used at each predefined level. As a part of encryption, to ensure the integrity of data against transmission errors or intrusion, error detection codes are introduced during encryption.

II. ALGORITHMS

Our Cryptographic technique consists of following algorithms

1. Generating private keys &Creation of Crypto Matrix table.
2. Symmetric Encryption using Crypto Matrix table and Padding parity bits for integrity Check.
3. Generating Symmetric keys & Decryption of Cipher Text.

Algorithm 1: Generating private keys &Creation of Crypto Matrix table.

Crypto matrix table is a 9X9 matrix of alpha numeric values which will be used as substitution characters for plain text and it works as referential table for encryption/ decryption.

Row and column ID of Crypto Matrix table consists of symbols and matrix consist of twenty six alphabets, numbers form 0-9 including primary keys and 50 other symbols and special characters like #,%,^ etc .Arrangement of characters in the table is pre negotiated with communication parties.

Two more private keys are generated using a private key named as L1pk which is the actual key shared to destination & private key generator key named as PGK. Predefined mathematical calculation is performed using PGK and L1pk to generate private keys named as L2pk & L3pk. Here L1pk is a key which can be unique for each new encryption.

Example:
PGK = 9, L1pk = a=96
PGK%L1pk =L2pk
9 % 96 = 6
Therefore L2pk =6, L3pk=10

L3pk represents position of the L1pk key value in the crypt matrix table. A standard characters sequence used in the arrangement of characters in this table and no duplicate characters are allowed in the Crypto Matrix table.

@	**#**	**$**	**%**	**^**	**&**	*****	**-**	**=**
#		1	2	3	4	5	6	7
$	9		0	@	#	$	%	^
%	*	-		=	+	Q	W	E
^	T	Y	U		I	O	P	A
&	D	F	G	H		J	K	L
*****	‘	“	:	Z	X		V	B
-	M	C	.	/	<	>		,
=	~	8	&	R	S	;	N	+

Figure 1.1: Crypto Matrix table

Algorithm 2: Symmetric Encryption using Crypto Matrix Table and padding Parity Bits for integrity check.

This includes four levels .At first and second level encryption is performed in byte level whereas in third and fourth level it’s in bit level.

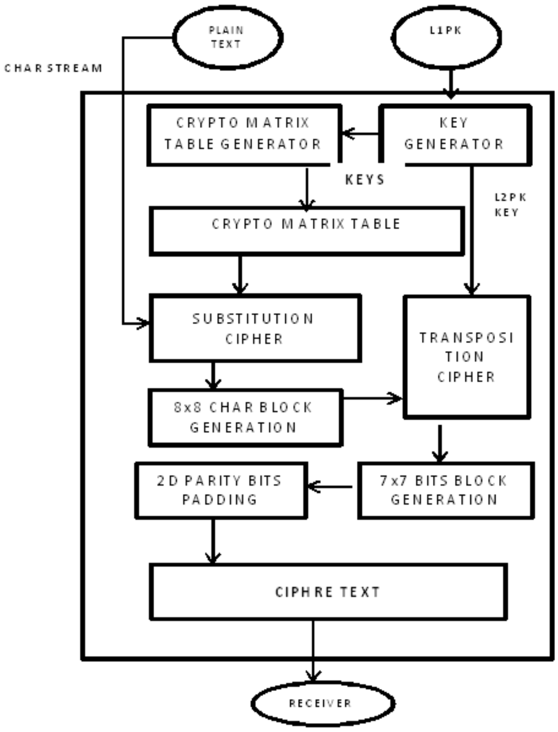

Figure 1.2: Key Generation & Encryption at Source

Level 1: Here Encryption performed by using CRYPTO MATRIX Table each character of plaintext is replaced with two column & row ID characters.

PC-> (CC, RC)
Where CC- Column ID,
RC- Row ID, PC-Plain Text Character.

Example:
Plain text: I am here
E(Pc1)→ (Cc,Rc) so I→ (^ ,&) → ^&
Level 1 Cipher text: ^&^=-#&^ %= *+ ^%

Level 2: Splitting up of character stream generated at step 1 in to 64bit fixed size blocks as 8X8 matrix. The last block may contain less than 64 bits. Transposition cipher method is applied on rows & columns of this 8X8matrix. Each row & columns will be shifted to L2pk times to generate cipher text.

Level 3: Applying Two Dimensional Parity Bit method to help destination device to find out integrity violation in data. Character stream of cipher text generated level 2 are converted into bit stream. This bit stream is grouped into blocks of 7X7 matrix and two dimensional parity bits are added. By this cipher text will be ready to transport to destination.

Algorithm 3: Generating Symmetric keys &Decryption of Cipher Text.
Generation keys and preparing crypto matrix table starts after receiving L1pk by sender. using PGK which is a pre negotiated key used for key generation, L2pk and L3pk is calculated. Using these two keys crypto matrix table is prepared.

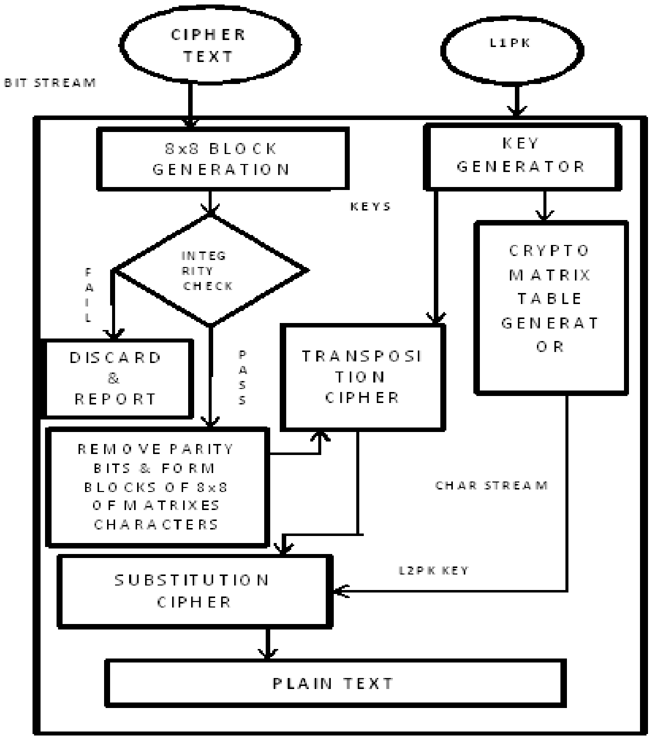

Figure 1.3: Key Generation & Decryption at Destination

Decryption of Cipher Text is in the reverse hierarchy of encryption process.

Step 1: Grouping cipher text bits into 8X8 blocks and checking integrity of the data by analyzing parity bits.
Step 2: If no violation of the data integrity is found, Then parity bits are removed and characters of cipher text are grouped in to 8X8 matrix.

Step 3: Reversal of transposition is performed on matrix against the transposition performed during encryption using L2pk.

Step 4: Each characters of cipher text after transposition are substituted with appropriate character of crypto matrix table.

Example:
Cipher text : ^& ^=-# &^ %= *+ ^%
{^&→(^ ,&))→ (Cc,Rc)}
Plain text: I am here

@	#	$	%	^	&	*	-	=
#		1	2	3	4	5	6	7
$	9		0	@	#	$	%	^
%	*	-		=	+	Q	W	E
^	T	Y	U		I	O	P	A
&	D	F	G	H		J	K	L
*	‘	“	:	Z	X		V	B
-	M	C	.	/	<	>		,
=	~	8	&	R	S	;	N	+

Figure 1.4: Crypto Matrix table at Destination

III.CONCLUSION

This new Cryptography package will provides 3 level of security. In first the key L1pk shared to destination is not the actual key which can be used for Decryption. Two private keys L2pk and L3pk have to be generated from the L1pk with the help of PGK which is pre negotiated. So even if L1pk is hacked by intruder they are not aware of PGK and process of generating L2pk and L3p. All these key contributes in encryption and Decryption so unavailability of even one key leads to failure of decryption.
The second thing that encryption process takes place in many levels includes both byte cipher and bit Cipher and Both transposition and substitution cipher methods are used. At the end parity bits are added to check for the active attack on data being transmitted.

Compare to other well-known cryptographic techniques this will takes less time to Develop & Implement. By Simple coding using any programming languages .It can be developed as application software. Like PGP package it can be made as open source application so that anyone can freely download and use this to secure their sensitive administrative data of their organization.

To enhance the Strength of this encryption operation different simple encryption algorithms can be added to make chain encryption.

REFERENCES

[1] William Stallings. 2013. Cryptography and Network Security, Principal and practice, 5th Edition, Pearson Education, Inc.
[2] AtulKahate. 2011 “Cryptography and network security, 2rd Edition.”, Tata McGraw Hill Edition Private Limited.
[3] Whitfield Diffie. pp 2010.Applied cryptography, 2nd Edition, Bruce Schneider Press.

[4] V.K.Pachaghare. 2009. Cryptography and Information Security. 1st Edition, PHI Learning Private Ltd.

[5] BehrouzA.Forouzan.2004,"Data Communication and Networking,4th Edition. Tata McGraw-Hill Publication.

[6] Vinay S &Shivamurthaiah M. p 2014, "Private C- Multi Key S-Matrix Block Cipher" , ISBN: 978-81-207-8818-3. National conference on Convergence in Operational and Computational Technology-COCT 2k14.28 march 2014)

[7] Vinay S &Shivamurthaiah M. P 2013, 'A plain key Compliment XOR Cipher Method',ISBN: 978-81-92820309.National conference on Software and information management. 27 Sept 2013

[8] Lin Yi Hui, P 2009, Cryptography and Network security an overview. 'International Journal of Computer Science and Security', vol. 1, no. 1.