Survey of symmetric key cryptography

Tadavi Anjana

Student,CE(SNS),Svit vasad,Gujarat,India

ABSTRACT

Cryptographic algorithm plays an important role to secure the confidential data while transmitting over the cloud. Modern cryptography offers a variety of encryption scheme for protecting the data. A key used for encrypting the plain text is another vital component on which the secrets depend. Advanced Encryption Standard (AES) algorithm is used in this research paper.This paper describes survey of symmetric key cryptography.

Keyword : - *Cryptography,plain text,Cipher text,symmetric key cryptography*

1. INTRODUCTION

Technology is advancing day-to-day. For a better and faster technology, information security is a must. This requires data authentication at the execution levels. Cryptography is a useful tool through which secure data independency can be established.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, *cryptanalysis* is the scienceof analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

2. SOME STATURE BASED PROTOCOLS

2.1 chaotic cryptography using external key

The paper has the discussion regarding 'dispositions' of trusting behavior, an external secret key of variable length maximum 128-bits and used in our algorithm. The encryption of each block of plaintext has been made dependent on the secret key and the cryptosystem is further made robust against any reasonable attack by using the feedback technique.

STEP 1:
The plaintext into blocks of 8-bits, i.e., each symbol of the plaintext/ciphertext corresponds to a single block. Plaintext and ciphertext of n blocks can be represented as:
P = P1P2P3P4 ···Pn (plaintext),
C = C1C2C3C4 ···Cn (ciphertext).

divided into blocks of 8-bits named as session keys.
K = K1K2K3K4 ···K16 (secret key)

STEP 2:
Xs= real number range 0 to 1

ASCII value of the nth session key

$$Xs=\frac{((K1)2 \oplus (K2)2 \oplus (K3)2 \oplus \cdots \oplus (K16)2)10}{256} \qquad (1)$$

Ns =(K1 + K2 + K3 +···+ K16) mod 256.

We choose a session key (Kr, 1 r 16) randomly and modify the seed values for the initial condition (Xs)

$$X=(Xs+\frac{Kr}{256})MOD1 \qquad (2)$$

N=Ns+K (3)

Kr = ASCII value of random session key

STEP 3:

Λ= system parameter

λi = (a ∗ Yi + c) mod m /200 + 3.57

a = multiplier,

m and c = constants,

λi=system parameter value of the

Yi= 0 for the encryption/decryption of the first block of plaintext/ciphertext

i = 1 while for the encryption/decryption of the remaining blocks of plaintext/ciphertext

(i = 2 to n) Yi is calculated using the standard LCG generator as defined below:

Yi=(a∗Yi−1+c)modm. (4)

ENCRYPTION:

Ci = (Pi + Xnew ∗ 256) mod 256 (5)

DECRYPTION:

Pi = (Ci + 256 − Xnew ∗ 256) mod 256

Xnew = the encryption/decryption of the next block of plaintext/ciphertext.

Ci−1 =ASCII value of the previously encrypted/decrypted ciphertext block are taken

X= seed values

Ns = number of iterations

put the symbols or we can say block to the ASCII values obtained in pervious (Ci/Pi) as the ciphertext/plaintext.Choose next block of plaintext/ciphertext and repeat the process from until the plaintext/ciphertext isexhausted.

2.1 Random Key Material Distribution

Node is pre-loaded with a subset of keys, known a key ring, randomly selected from a global pool of keys such that any pair of neighboring nodes can share at least one key with a certain probability.

After deployment, 2 neighboring nodes can have a shared key directly or an indirect key through a secure path, along which every pair of neighboring nodes has a direct shared key. The theoretical foundation of RKP is the random graph theory.

A random graph G(n, p) is a graph of n nodes for which the probability that a link exists between two nodes is p.

The graph does not have any edge if p = 0 or is fully connected if p = 1. There is a transition from the non-connected graph to the fully-connected graph when p increases. RKP exploits this property by setting p larger than a certain value such that the network is almost connected.

$Pc=\lim_{n\to\infty}Pr[G(n,p) is connected]= e^{e-c}$ (6)

p = ln(n) / n + c/n and c is any real constant.

p and d can be derived as= p ∗ (n − 1) for which the resulting graph is connected with desired probability Pc.

A major concern of RKP is node compromise. The random selection of a key ring for each node means the reuse of each key by multiple nodes. RKP can improve the resilience to node compromise when the number of compromised nodes is small. Unfortunately, it is not effective when the number is large. Spatial diversity is used to improve the resilience to node compromise.

There are some powerful anchor nodes that are assumed to be tamper proof. A global key is shared by all the anchor nodes and normal nodes, and each normal node is preloaded with a key ring following RKP. Each anchor node uses the global key to broadcast several rounds of random nonces at different power levels in its neighborhood.
Each sensor node uses the received nonces to rebuild its key ring. Later, all the nodes can follow RKP to establish shared keys with their neighbors. Finally, each node deletes its original key ring and the global key. The introduced spatial diversity by anchor nodes results in the derived key rings being very different for two nodes that are far away from each other, while making neighboring nodes have more common keys in their derived key rings.

2.3 Security of Public Key Cryptosystems based on Chebyshev Polynomials

Key Generation Algorithm. Key Generation takes place in three steps
Alice, in order to generate the keys, does the following:
1. Generates a large integer s.
2. Selects a random number $x \in [-1 , 1]$ and computes $Ts(x)$. 3. Alice sets her public key to $(x, Ts(x))$ and her private key to s.
Encryption Algorithm. Encryption requires five steps: Bob, in order to encrypt a message, does the following:
1. Obtains Alice's authentic public key $(x, Ts(x))$.
2. Represents the message as a number $M \in [-1\ 1]$.
3. Generates a large integer r.
4. Computes $Tr(x)$, $Tr{\cdot}s(x) = Tr(Ts(x))$ and $X = M \cdot Tr{\cdot}s(x)$.
5. Sends the ciphertext $C = (Tr(x), X)$ to Alice.

Decryption algorithm:
Decryption requires two steps: Alice, to recover the plaintext M from the ciphertext C, does the following:
1. Uses her private key s to compute $Ts{\cdot}r(x) = Ts(Tr(x))$.
2. Recovers M by computing $M = X/Ts{\cdot}r(x)$.

2.4 Jacobian Elliptic Chebyshev Rational Maps

Key Generation Algorithm. Key Generation takes place in three steps: Alice, in order to generate the keys, does the following:
1. Generates a large integer s
2. Selects two random numbers $\omega \in [-1 , 1]$ and $k \in [0, 1]$, and computes $Rs(\omega, k)$.
3. Alice sets her public key to $(\omega, k, Rs(\omega, k))$ and her private key to s.

Encryption Algorithm. Encryption requires five steps: Bob, in order to encrypt a message, does the following:
1. Obtains Alice's authentic public key $(\omega, k, Rs(\omega, k))$.
2. Represents the message as a number $M \in [-1 , 1]$.
3. Generates a large integer r.
4. Computes $Rr(\omega, k)$, $Rr{\cdot}s(\omega, k) = Rr(Rs(\omega, k), k)$, and $X = M \cdot Rr{\cdot}s(\omega, k)$.
5. Sends the ciphertext $C = (Rr(\omega, k), X)$ to Alice.

Decryption Algorithm.
Decryption requires two steps: 11 Alice, to recover the plaintext M from the ciphertext C, does the following:
1. Uses her private key s to compute $Rs{\cdot}r(\omega, k) = Rs(Rr(\omega, k), k)$.
2. Recovers M by computing $M = X/Rs{\cdot}r(\omega, k)$. Notice that, the value of k, which defines the form of the map, could be the same for all users of the system

2.5 A Cryptography Using Advanced Substitution Technique and Symmetric Key Generating Algorithm

Encryption algorithm is used to maintain the secrecy of the data whereas performance, speed, size and security are the key factors to be considered while deciding an encryption algorithm. A key is used to encrypt the plaintext which is categorized into private key (symmetric) and public key (asymmetric). Symmetric key algorithm is considered to be the effective and secured one while comparing with asymmetric key. In this research, a new substitution method is introduced and key generating method is enhanced to encrypt the text message .

Symmetric key encryption scheme or secret key encryption scheme has the following five ingredients
Plain Text- This is the original text message or data is fed into the substitution technique as input.
Encryption algorithm- The encryption algorithm performs various substitutions on the plaintext.
Secret key- The secret key is also input to the encryption algorithm .The key is a value independent of the plaintext. The algorithm will produce a different output depending on the specific key being used at the time .the exact substitutions and transformations performed by the algorithm depend on the key.
Cipher text-This is the scrambled message produced asoutput .It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data and, as it stands is unintelligible.
Decryption Algorithm- This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

PROPOSED WORK

A. Proposed Framework

To make the plain text into more secured cipher text, the proposed framework is divided into three phases which is depicted in Figure 1.
1) Phase I – Substitution Phase: The initial phase which gets the plain text as input. The input text is then converted into first form of cipher text with Advanced Substitution method .
2) Phase II – Key generation phase: The cipher text which is generated in the phase I is given as input to the phase II. The cipher text is further encrypted with the symmetric key (Private key). This key is similar to one-time pad keywhich can be used once for encryption and decrytpion, but the implemented concept is different.
3) Phase III- Algorithm phase: In this phase the strongly encrypted message is further more encrypted using a symmetric key algorithm. In this method, Advanced encryption Standard algorithm is used.

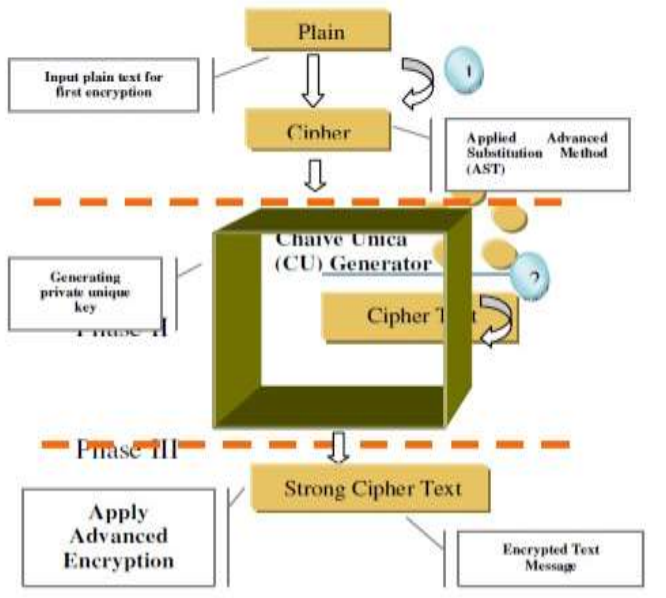
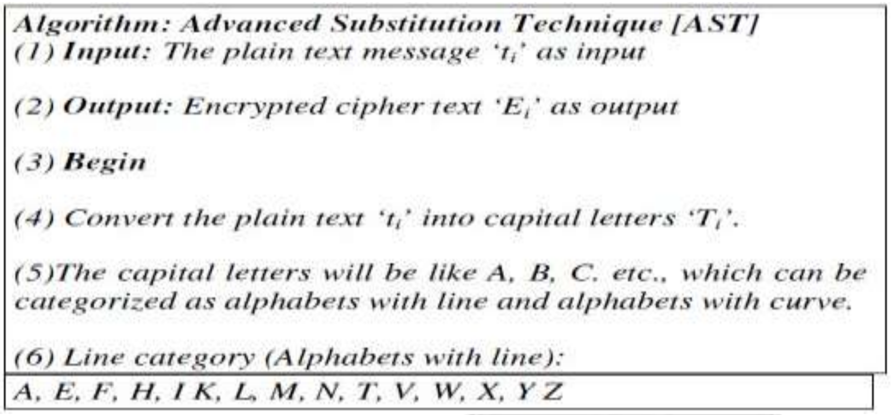

Plain
Input plain text for first encryption
1
Cinher
Applied Advanced Substitution Method (AST)
Chaive Unica (CU) Generator
2
Generating private unique key
Phase II
Cipher Text
Phase III
Strong Cipher Text
Apply Advanced Encryption
Encrypted Text Message

Figure. 1 Proposed Framework for Encryption

The main features of AES are
Symmetric and parallel structure- A lot of flexibility which protects against cryptanalysis attacks.
Adapted to modern processors- Algorithm works with modern processors like Pentium, RISC, parallel.
Suited to Smart cards- Work well with the smart cards.
Algorithm for Advanced Substitution Method (AST)-
AST is specifically designed to encrypt the plain text with highly secured way. The algorithm is as follows



Algorithm: Advanced Substitution Technique [AST]

(1) ***Input:*** *The plain text message 't_i' as input*

(2) ***Output:*** *Encrypted cipher text 'E_i' as output*

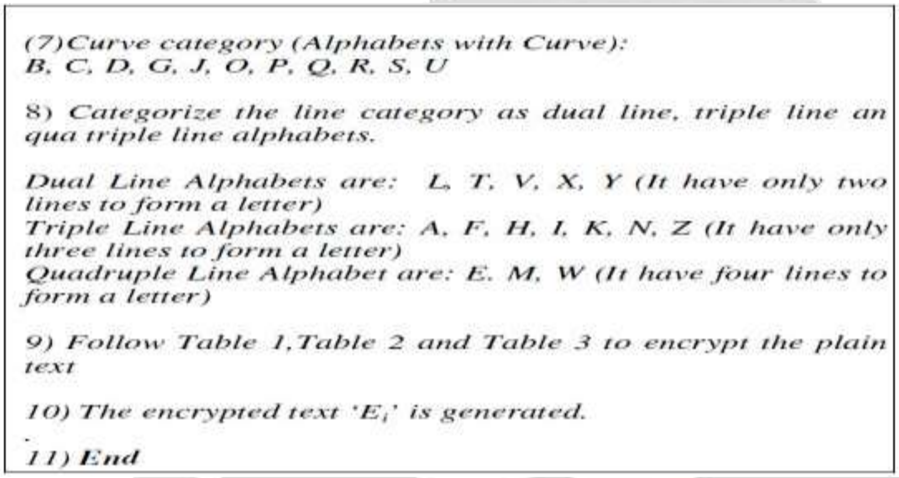
(3) ***Begin***

(4) Convert the plain text 't_i' into capital letters 'T_i'.

(5)The capital letters will be like A, B, C. etc., which can be categorized as alphabets with line and alphabets with curve.

(6) Line category (Alphabets with line):

A, E, F, H, I K, L, M, N, T, V, W, X, Y Z



(7)Curve category (Alphabets with Curve):
B, C, D, G, J, O, P, Q, R, S, U

8) Categorize the line category as dual line, triple line an qua triple line alphabets.

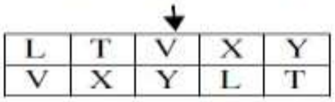
Dual Line Alphabets are: L, T, V, X, Y (It have only two lines to form a letter)
Triple Line Alphabets are: A, F, H, I, K, N, Z (It have only three lines to form a letter)
Quadruple Line Alphabet are: E. M, W (It have four lines to form a letter)

9) Follow Table 1,Table 2 and Table 3 to encrypt the plain text

10) The encrypted text 'E_i' is generated.

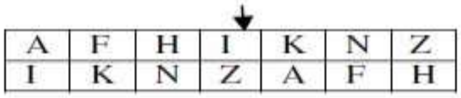
11) End

DOUBLE LINE ALPHABET



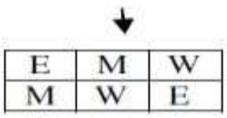
L	T	V	X	Y
V	X	Y	L	T

DOUBLE LINE ALPHABET



A	F	H	I	K	N	Z
I	K	N	Z	A	F	H

QUADRUPLE LINE ALPHABET



E	M	W
M	W	E

1 Plain Text : h e l l o
2 Convert as capital letters : H E L L O
3 Categorize the line and curve Alphabet: H E L L is line category and O is curve category.

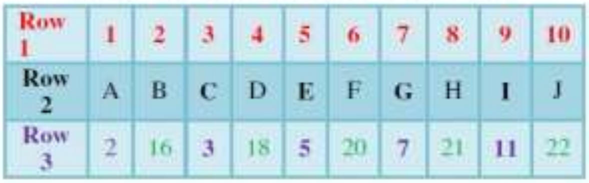
4 Further categorize dual line, Triple line and
quadruple line alphabet: Dual Line : L L
Triple Lne: H
Quadruple Line: E

5 Find the alphabet corresponding to the letter from Table I, II, III
and IV: H => N
E => M
L => V
L => V
O => S

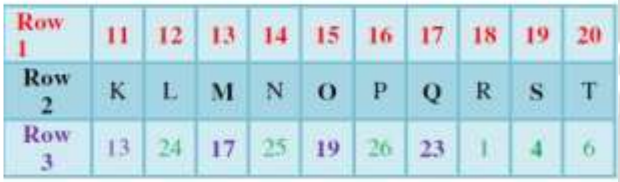
6 The Encrypted text using AST is : N M V V S for
H E L L O

Algorithm:Chaive Unica Generator[CUG]
(1)Input:the encrypted message 'Ei'.
(2)output:strong encrypted cipher text 'SEi' as output
(3)Begin
(4)select the unique key from the code key sheet based on the encrypted letter
For eg., if the Ei is 5 letter word then select key with 5 letters
(5)number each odd positioned alphabrt with increasing prime numbers till 23 as given in table V and number the consequent alphabets.
(6)check the Ei with corresponding numbers in the third row.
(7)a new SEi is generated.
(8)End

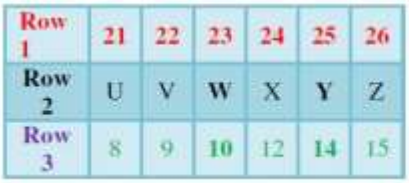
ALPHABETS WITH ORIGINAL AND PRIME NUMBERING



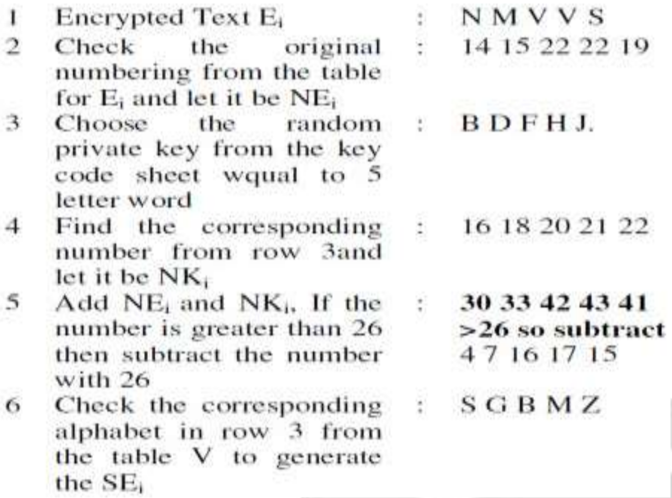
Row 1	1	2	3	4	5	6	7	8	9	10
Row 2	A	B	C	D	E	F	G	H	I	J
Row 3	2	16	3	18	5	20	7	21	11	22



Row 1	11	12	13	14	15	16	17	18	19	20
Row 2	K	L	M	N	O	P	Q	R	S	T
Row 3	13	24	17	25	19	26	23	1	4	6



Row 1	21	22	23	24	25	26
Row 2	U	V	W	X	Y	Z
Row 3	8	9	10	12	14	15

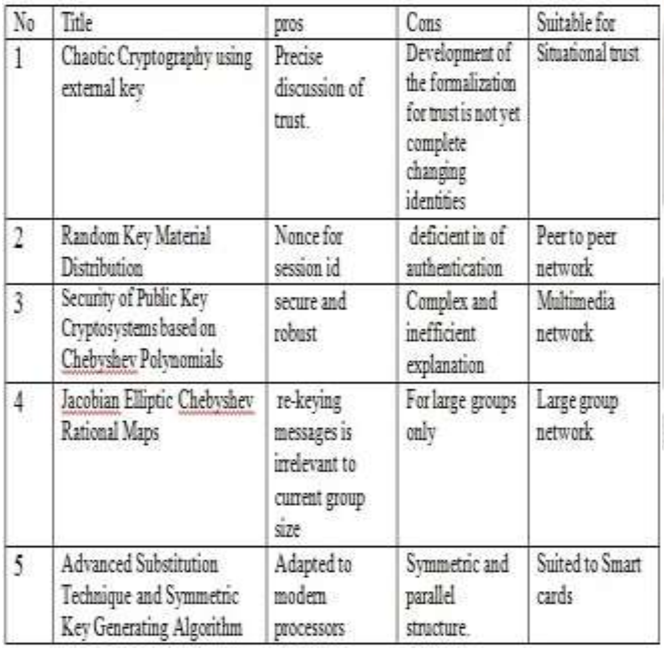


1	Encrypted Text E_i	:	N M V V S
2	Check the original numbering from the table for E_i and let it be NE_i	:	14 15 22 22 19
3	Choose the random private key from the key code sheet wqual to 5 letter word	:	B D F H J.
4	Find the corresponding number from row 3and let it be NK_i	:	16 18 20 21 22
5	Add NE_i and NK_i. If the number is greater than 26 then subtract the number with 26	:	**30 33 42 43 41** **>26 so subtract** 4 7 16 17 15
6	Check the corresponding alphabet in row 3 from the table V to generate the SE_i	:	S G B M Z

Algorithm: Advanced Encryption Standard (AES)

(1) Expand the 16-byte key to get the actual key block to be used
(2) Do one time initialization of the 16-byte plain text block (State)
(3) XOR the state with key block
(4) Apply S-box to each of the strong encrypted text SEi
(5) Rotate row k of the strong encrypted text SEi by k bytes
(6)Perform the mix coloumns operation
(7) XOR the state with the key block
(8) End

3.result



No	Title	pros	Cons	Suitable for
1	Chaotic Cryptography using external key	Precise discussion of trust.	Development of the formalization for trust is not yet complete changing identities	Situational trust
2	Random Key Material Distribution	Nonce for session id	deficient in of authentication	Peer to peer network
3	Security of Public Key Cryptosystems based on Chebyshev Polynomials	secure and robust	Complex and inefficient explanation	Multimedia network
4	Jacobian Elliptic Chebyshev Rational Maps	re-keying messages is irrelevant to current group size	For large groups only	Large group network
5	Advanced Substitution Technique and Symmetric Key Generating Algorithm	Adapted to modern processors	Symmetric and parallel structure.	Suited to Smart cards

Comparison of various Key generating scheme

4. CONCLUSIONS

This paper has surveyed the literatures on reputation models across diverse disciplines. The centralized as well as decentralized different aggregation methods for peer to peer network. Disadvantage of each of the protocol has been pointed out. We have attempted to integrate our understanding across the surveyed literatures any tried to find out the on system proving the privacy and with strong cryptography building blocks.

5. REFERENCES

[1]Gomathi, S. "A cryptography using advanced substitution technique and symmetric key generating algorithm." *Intelligent Systems and Control (ISCO), 2014 IEEE 8th International Conference on*. IEEE, 2014.

[2] Bergamo, Pina, et al. "Security of public-key cryptosystems based on Chebyshev polynomials." *Circuits and Systems I: Regular Papers, IEEE Transactions on* 52.7 (2005): 1382-1393.

[3]. Diaa Salama, Abdul Elminaam, Hatem Mohamed Abdul Kader And Mohie Mohamedhadhound & Performance Evaluation Of Symmetric Encryption Algorithm &, Ijcsns, 2008.Deven N.Shah:"Information Security: Principles Andpractice".

[4]. Matthews, Robert. "On the derivation of a "chaotic" encryption algorithm." Cryptologia 13.1 (1989): 29-42.

[5] Kohda, Tohru, and Hirohi Fujisaki. "Jacobian elliptic Chebyshev rational maps." Physica D: Nonlinear Phenomena 148.3 (2001): 242-254.

[6] Encryption Algorithm &, Ijcsns, 2008.Deven N. Shah:"Information Security: Principles And Practice".