A NEW APPROACH FOR CRYPTOGRAPHY IN SYMMETRIC KEY GENERATION USING MATRIX METHOD

Tadavi Anjana

student, Computer Engineering(SNS), SVIT VASAD, Gujarat ,India

ABSTRACT

A cryptographic algorithm is very important in securing the confidential data while transmitting over the network. Modern cryptography is suggesting a variety of encryption schemes for protecting & securing the data. This paper focuses on developing a new method to generate the key & algorithm by using cryptographic techniques which will all together make an encryption scheme which is secure for generating the key. The proposed scheme does not require any specialized hardware or software, so basically it is low-cost & flexible for peer to peer networks & entity communication, which is based on the matrix. Finally, the paper concludes that simulation results are important for the feasibility of the algorithm.

Keyword : - *Secure communication, sheltered message passing communication, low budget algorithm.*

1.Introduction

Security of the data to be transferred is the crucial between the sender and receiver while communication. Information security is all times have set a fundamental part in each area associated with the communication of any confidential data. As the time is changing there is continuous requirement for a robust and powerful complex encryption technique. Presently, the superfluity for enciphering any plain text information subsists as well as encompasses accomplishment of the information protection to an immense level.

To maintain the equilibrium among the flexibility and robustness has always been a significant constraint of sustaining the altitude of security & encryption. Securing the data is the need for encryption. Generally the algorithm used to encrypt the data deals and aims at preserving the privacy of the data concealment & discretion of the data. Still while choosing any enciphering technique to be applied to the data the factors needs to be considered are how it performs, robustness, rapidity, dimension protection and complexity are the important aspects which need to be considered.

For enciphering any data there is a need for the key which can be generally classified as the" private key (symmetric)" and "public key (asymmetric)". symmetric as the name suggest is the algorithm where both the parties exchanging the information shares the same key where as asymmetric key there are different keys by the two parties. If any intruder any how can capture the information being send, this could lead to catastrophic bang for the

organization"s chaos. Consequently, proficient scheme which is emplaning the characteristic of marmalade the "Confidentiality, Integrity and Authenticity" are of more importance.

1.1 Confidentiality

The confidentiality is one of the essential parameter in security. Creating the documents or transaction transform when it is in the shipment state or stored in data canter is considered to as preserving the data-confidentiality.

1.2 Integrity

Integrity promises that the data being kept in the data-base or being transferred in the network is unchanged. Integrity can be reflected as the mixtures of two services as completeness plus correctness.

1.3Authenticity

Authenticity can be considers to the trust-worthiness of data-bases, communication via transmission-links, transactions, clients, data owners and the service provider. All the persons must be authorized for safeguarding the authenticity.

2. Proposed work

The new idea incorporates of the 3 steps which is form plain text key 1 is generated key 2 is generated from key 1 below is the mathematical proof of the system decipting the working of algorithm.

Encryption

1) Key 2 creation From Key 1:
a. select K1 = key 1
convert K1 to B(K1) which is binary
b. matrix A = binary counterpart by writing alongside the rows.
c. Transpose A to AT
d. B(AT)= binary of AT
The resultant binary number to hexadecimal.
HEX(B(AT)) = key 2
Key 2 is in the hexadecimal form
e. K1 todecimal number HEX(add decimal number)
f. Result= HEX(PT)-HEX(add decimal number)
g. S(txt)=Swap result digit among themselves
h. binary(S(txt)).
i. output=Inverse(2"s complement(binaryS(txt)))

2.Generation of key 3:
a. hex(output)
b. key 3= first and the last part hex(output)x2

3. Cipher Text Formulation
a. split (hex code) as follows.
b. output 1=The first block is Private Key shared with the receiver.
c. output 2=the second block is key with cipher text

Decryption
We get Cipher text as input.
Step1 partial cipher text extraction
a. Output 2 received = The block is Transport Cipher Key.
b. Output 1 received = The block is Private key shared .
c. Join (output1 ,output 2) convert to hex which is Key3.

Step 2.partial extraction of key 3:
d. We remove transport cipher key and append former 2 and the final 2 hex codes of cipher text.
e. We divide this new value from Key 3 to get Key 2.
f. Convert Key2 into it‟s binary equivalent.
g. We do the Inversion of this binary equivalent.
h. We do 2‟s complement of above Inversion.

Step 3. Plaintext Extraction
i. Convert the binary equivalent code into Hex code.
j. We swap the digits of above Hex code.
k. We add Hexadecimal equivalent to above Hex code.
l. Convert above Hex code into original Plaintext.

3. Mathematical proof of the proposed work

Plaintext : H E L L O
Key 1 = “SK”
Hexadecimal equivalent: 53 4B
Binary (SK)= "0101 0011 010 01011”
Matrix A = 0 1 0 1
0 0 1 1
0 1 0 0
1 0 1 1
Transpose AT = 0 0 0 1
1 0 1 0
0 1 0 1
1 1 0 1
Row form
0001 1010 0101 1101
Hexadecimal form
Key 2 1 A 5 D

Step 2 : After Key generation
Plaintext : H E L L O
Hexadecimal Form: 48 45 4C 4C 4F
Key 1 S K
Decimal Equivalent: 31223
3+1+2+2+3 = 11
Hexadecimal of 11 = 0B
Hexadecimal code after substracting 11
48 45 4C 4C 4F
- 11 - 11 - 11 -11 - 11
37 34 41 41 44
Hex code after swapping digits of each code:
73 43 14 14 44
Binary equivalent of each hexadecimal value
01110011 01000011 00010100 00010100 01000100
2‟s complement
1‟s complement : 10001100 10111100 11101011 11101011 10111011
2‟s complement: 10011101 11001101 11111100 11111100 11001100
Inversion

01100011 00110010 00000011 00000011 00110011
Hex Code: 62 32 03 03 33

Step 3: Key3 generation
Key2 = 1A5D
The first and last part of Hex code sequence are
62 32 03 33
62 33
Key2 1 A 5 D
Decimal 1 10 5 13
Ascii 62 32 03 33
Key3 63 42 08 46
Pre-shared private key : 63 42
Transport cipher key : 08 46
Cipher Text: 08 46 62 32 03 03 33

DECRYPTION
To convert the cipher text into original plain text,

Decryption
We get Cipher text as input.
private key shared : 63 42
The received cipher text:
Cipher Text: 08 46 62 32 03 03 33

1. Extracting key 3 from cipher text*:*
Key : 08 46
63 and 42 are previously shared the first two cipher text join them
key 3 = 63 42 08 46

2. Extracting Key2 :
Cipher text after removing first 2 values:
62 32 03 33
key 3 ÷ Cipher text after removing first 2 values = key 2
(63 42 08 46) ÷ (62 32 03 33) = 1 10 05 13
Therefore, Key 2 = 1 A 5 D

3. Key 1 Extraction :
Converting key 2 into binary value = 0001 1010 0101 1101
Writing it in the matrix form
Matrix B = 0 0 0 1
1 0 1 0
0 1 0 1
1 1 0 1
Row form: 0001 1010 0101 1101
Transpose Matrix T = 0 1 0 1
0 0 1 1
0 1 0 0
1 0 1 1
Binary equivalent = 0101 0011 0100 1011
Hexadecimal equivalent: 53 4B

ASCII of above binary number = SK
Key 1 = SK
Decimal (SK) = 21 3 23(3 is for space)
Sum of digits of above equivalent = 11
Hex equivalent of above sum = 0b
Adding 0b with each of the hex code in the sequence:
54 48 49 53 20 49 53 20 43 4f 4e 46 49 44 45 4e 54 49 41 4c
Hexadecimal code: 73 43 14 14 44
Swapping digits of each code: 37 34 41 41 44
Adding hexadecimal equivalent adding 0B
37 34 41 41 44
+11 + 11 +11 +11 + 11
48 45 4C 4C 4F
Plaintext: H E L L O

3.1.Result

For experiment java language figure 2 shows the output of the proposed approach which has the key size and the size of the memory in kb

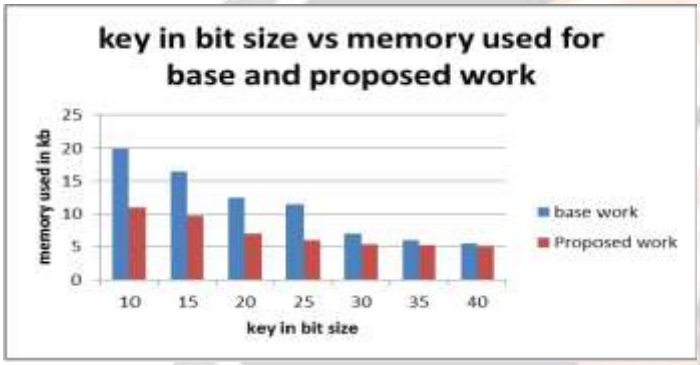

Chart 1 Comparison of the base and proposed work in terms of storage space

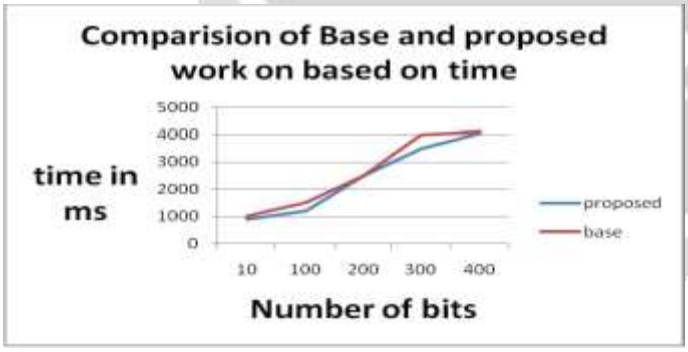

Chart 2 Comparison of base and proposed work on based on time

Proposed	Base
900	1000
1200	1500
2501	2500
3500	4000
4050	4100

4. CONCLUSIONS

A new advanced secure cryptographic approach has been projected which is resultant form the fundamental cryptographic algorithms and procedures are introduced and a new key generating process is presented,.

1. The key generation imposes randomized encryption
2. Key 3 are generated from the plain text which leads to the most complex form of the base algorithm

5. FUTURE EXTENSION

More secure algorithm other than RSA can be used for proposed system to provide more security. We will investigate encryption schemes that can resist such privacy vulnerabilities. We are also interested in exploring how to improve the proposed *a*lgorithm to minimize decryption time.

6. REFERENCES

[1] Robling Denning, Dorothy Elizabeth. Cryptography and data security. Addison-Wesley Longman Publishing Co., Inc., 1982.
[2] Davies, Donald Watts, and Wyn L. Price. Security for computer networks: and introduction to data security in teleprocessing and electronic funds transfer. John Wiley & Sons, Inc., 1989.
[3] Rivest, Ronald L. "The RC5 encryption algorithm." Fast Software Encryption. Springer Berlin Heidelberg, 1994.
[4] Wheeler, David J., and Roger M. Needham. "TEA, a tiny encryption algorithm." Fast Software Encryption. Springer Berlin Heidelberg, 1994.
[5] Matthews, Robert. "On the derivation of a "chaotic" encryption algorithm." Cryptologia 13.1 (1989): 29-42.
[6] Guan, Zhi-Hong, Fangjun Huang, and Wenjie Guan. "Chaos-based image encryption algorithm." Physics Letters A 346.1 (2005): 153-157.
[7] Gao, Tiegang, and Zengqiang Chen. "A new image encryption algorithm based on hyperchaos." Physics Letters A 372.4 (2008): 394-400.
[8] Pareek, N. K., Vinod Patidar, and K. K. Sud. "Discrete chaotic cryptography using an external key." Physics Letters A 309.1 (2003): 75-82.
[9] Camtepe, Seyit A., and Bülent Yener. "Key distribution mechanisms for wireless sensor networks: a survey." Rensselaer Polytechnic Institute, Troy, New York, Technical Report (2005): 05-07.
[10] 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.
[11] Kohda, Tohru, and Hirohi Fujisaki. "Jacobian elliptic Chebyshev rational maps." Physica D: Nonlinear Phenomena 148.3 (2001): 242-254.
[12] Blundo, Carlo, et al. "Efficient key management for enforcing access control in outsourced scenarios." Emerging Challenges for Security, Privacy, and Trust. Springer Berlin Heidelberg, 2009. 364-375.