International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 5, No. 1
February 2016

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 5, No. 1, February 2016

Research Paper

A² ENCRYPTION/DECRYPTION ALGORITHM

Arulanantham Kandhappan[1]* and Anandh Arul[1]

*Corresponding Author: ***Arulanantham Kandhappan*** ✉ arulananthamk95@gmail.com

We introduce A² encryption a simple, secure encryption technique using low min-entropy. It is a symmetric type encryption algorithm which is working on the basis of dual stage encryption. Here the first stage is switch to operation and the second stage is encryption key.The bit wise operating algorithm will provide the more security.It is basically operated at TCP/IP layer hence it provide higher order security. Due to low latancy and low memory requirement it is preferable to embedded and device based applications.

Keywords: Low min-entropy,Symmetry type encryption,Dual stage encryption,Logical operations,Encryption key

INTRODUCTION

- In the modern world the rapidized development of network field, the security of the individual is important . The existing system is strong but not enough for the current view.
- Many real world systems rely for encryption on low-entropy or weak secret, most commonly user chosen password.
- However the current technique is improved by dual stage of encryption.

Therefore the number of chances to get the message from code is given by equation

$$P(n) = \frac{1}{2^{3\mu}}$$

Where $q = 2^{3\mu}$

where μ is length of the datable Framework.

Assume the value of μ is 3 then the resultant number of output will be 16777216 combinations of ASCII codes and chance to obtain the right data is 5.960464478 x 10-8.

Since 3 is value of only three logical operations then it can increased up to 7.

So the number of output chances is 7.2055759404 x 1016 and chance to obtain the output is 1.387778781 x 10-17.

Hence the final equation is given as

$n = 2qxu$; $P(n) = 1/(2qxu) = 1/n$

The above equation is a derived form of Poisson distribution.

Where q is number of logical operation and μ is number of message bits.

[1] Department of Electronics and communication Engineering , PRIST UNIVERSITY, Puducherry, India.
[2] Department of Computer Science Engineering, PRIST UNIVERSITY , Puducherry, India.

METHODS

1. Symmetric Encryption

A form of crypto system where encryption and decryption are performed using the same key. Let us take a closer look at the essential elements of a symmetric encryption scheme. A source produces a message in plaintext, X=[X1, X2,…,XM]. M elements of X are letters in some finite alphabet. Traditionally, the alphabet usually consist of the 26 capital letters. Nowadays, the binary alphabet {0, 1} is typically used. For encryption, a key of the form K = [K1, K2,…, KJ] is generated. If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel. Alternatively, a third party could generate the key and securely deliver it to both source and destination.

2. Encoding methodology

Here we use a simple logical operation for given data which is converted in to ASCII code and perform it with key data to encryption. At first we generate ASCII code for given data input. We can switch the logical operation by Switch key.

Then the logical operation is performed with the encryption key hence the output is obtained as a encrypted ASCII code.

x(n) message sequence

where (n) = {m-$_0$, m_1, m_2,…….,m_{n-1}}

X[N]=x(n)$_{ASCII}$

(ie) $x(n) \xrightarrow[ASCII]{\Delta} X[n]$

Then X[n]= {M-$_0$, M_1, M_2,……., M_{n-1}}

The g(x) is a key generation function then the key term is Ke.

Ke = DTE_REJ_RSA [g(x)]

For the defined adversary function

S is output crypt data

$$S = f_n^k[data, Ke]$$

$$S^1 = \text{mod}[\, f_n^k[X(n), Ke]$$

$$= \text{mod}[\, f_n^k[X(n), DTE\_REJ\_RSA(g(x))]]$$

$$S^1 = \text{mod}[\, f_n^k[\sum_{n=0}^{n-1} M_N, DTE\_REJ\_RSA(g(x))]$$

For defined Adversary

Where f_n^k is the operating logical function

DTE – Distribution Transformation Encoding

Assume [A] is a data to be encrypted.

The final key transfer is done in the form for (K_s, K_e) where the switch is first stage of encryption the encryption data is at the operational level.

3. Switching Key (k_s)

This is simple key where it perform the operation hence it is limited which has maximum value of 7 only. But it is hard core and perform encryption. To perform the operations of higher stage the *combinational logical circuits* are use which is more and more effective.

4. Encryption Key (k_e)

To generate this key we use distribution transforming encoders (DTE). We turn to building a DTE for RSA secret keys. A key can generated of bit length 2 via rejection sampling of random variables P,Q, E (2^{e-1}, 2^e).

The rejection criterion for either P or Q distribution of primer uniform the range of e^{-1} mod (P–1) (Q–1) for some fixed e typically (65537) yield.

One straw man approach is just to Unicode the input P, Q as a part of (l-2)-bit strings C the leading 'l' bit Left implicit J, but it gives a poor DTE.

However the encryption key is generated by theorem of DTE. Which is Pm is uniform over primes in $[2^{e-1}, 2^e]$ for some $e \geq 2$ and RSA – REJ –DTE be scheme described above.

Then adverdite (A) $\leq \left(1-\frac{1}{3^e}\right)^{t-1}$ RSA – REJ – DTE

For any adversary A.

5. Key Transfer

Knowledge about the number and length of messages between nodes may enable an opponent to determine who is talking to whom. This can have obvious implications in a military conflict. Even in commercial applications, traffic analysis, may yield information that the traffic generators would like to conceal. [MUFT89] lists the following types of information that can be derived from a traffic analysis attack:

- Identities of partners
- How frequently the partners are communicating
- Message pattern, message length, or quantity of messages that suggest important information is being exchanged
- The events that correlate with special conversations between particular partners

Another concern related to traffic is the use of traffic patterns to create a covert channel. A covert channel is a means of communication in a fashion unintended by the designers of the communication facility. Typically, the channel is used to transfer information in a way that violates a security policy. For example, an employee may wish to communicate information to an outsider in a way that is not detected by management and that requires simple eves dropping on the part of the outsider. The two participants could set up a code in which an apparently legitimate message of a less than a certain length represents binary zero, whereas a longer message represents a binary one. Other such schemes are possible.

The final key transfer is done in the form for (K_s, K_e) where the switch is first stage of encryption the encryption data is at the operational level.

6. Decoding messages

Since it is symmetric encryption the decryption is also the same methodology of encryption since the key is also identified. decoding a message data is quite simple.

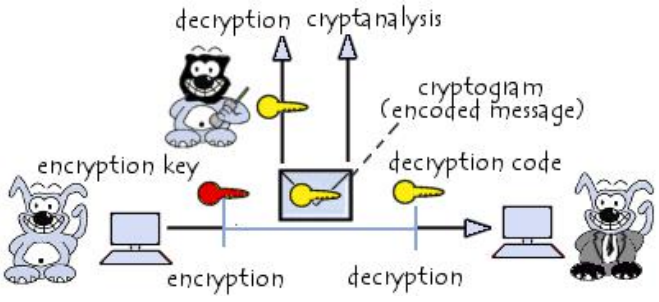
MeE M $= \frac{1}{n} = \frac{1}{2^q}$

Let us decode the previous encrypted data [J] okay here is the key of (XOR, 11) then performing (74) EXOR with [11] we obtain [65] where it is ASCII code of [A].

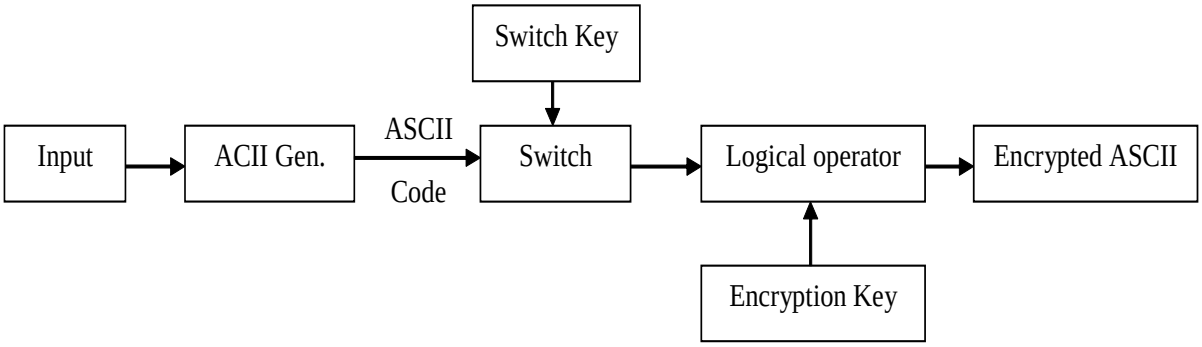
6. Methodology Overview

logical diagram flow chart and programming algorithm with program output.

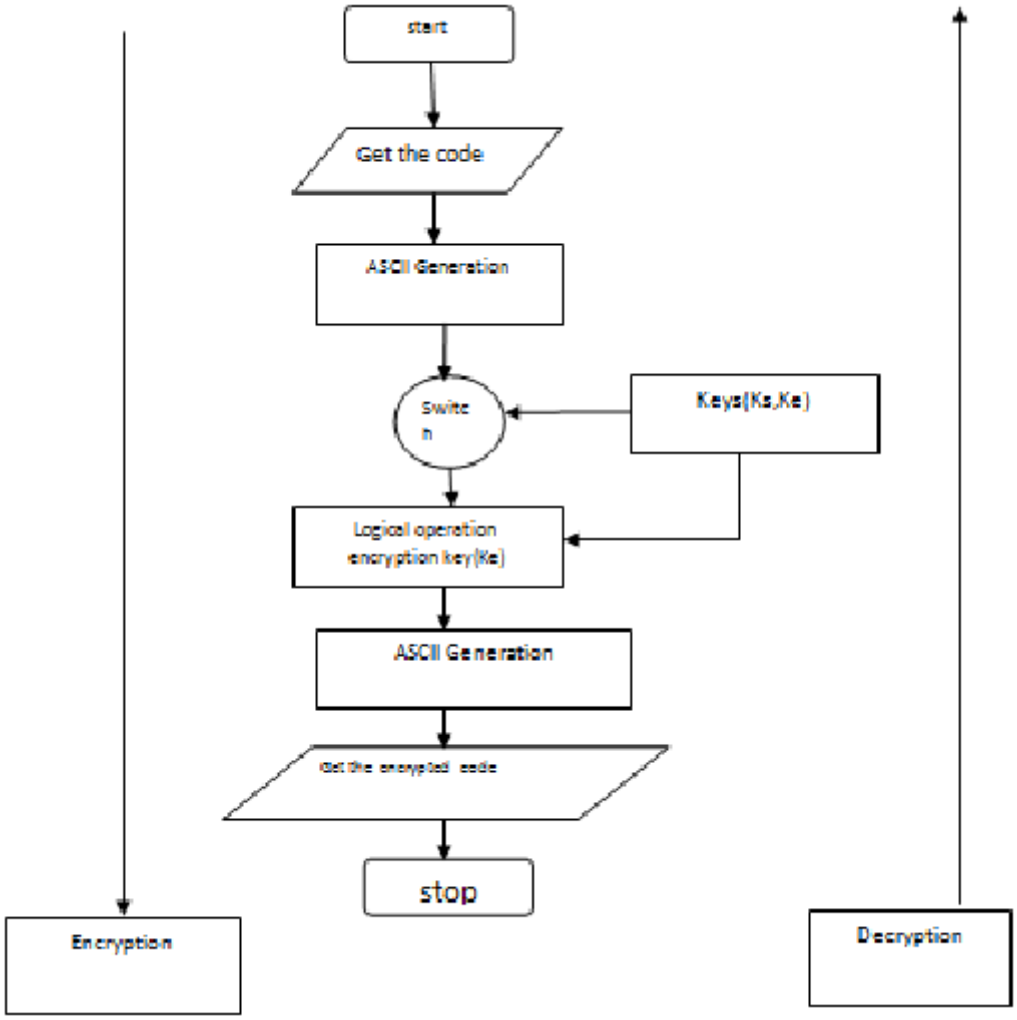
Key Transfer Technology



Logical Block Diagram for A² Encryption / Decryption Algorithm



Flow Chart for A² Encryption / Decryption Algorithm



Programming Output for Encryption Decryption Algorithm

```
encryption                          decryption
enter the character                 enter the character
A                                   J
the ascii value of Ais 65           the ascii value of Jis 74
enter the key                       enter the key
11                                  11

1.And                               1.And
2.Or                                2.Or
3.Xor                               3.Xor
enter the operation                 enter the operation
3                                   3
74                                  65
Encrypted data is J_                decrypted data is A_
```

PROGRAM LOGIC

Encryption Algorithm of a^2 Algorithm

We are presenting the steps of the encryption algorithm of the A2 Algorithm steps are:

Step 1: Input the character and the key.

Step 2: Convert the previous character to ASCII code.

Step 3: It under goes switch parameter in bitwise operation.

Step 4: Obtain the ASCII code put it as one character.

Step 5: Return encrypted text.

Decryption Algorithm of A2 Algorithm

We are presenting the steps of the decryption algorithm of the A2 Algorithm steps are:

Step 1: Input the character and the key.

Step 2: Convert the previous character to ASCII code.

Step 3: It under goes switch parameter in bitwise operation.

Step 4: Obtain the ASCII code and put it as one character.

Step 5: Return decrypted text.

DISCUSSION

We now draw all of the results of previous section together in a several real time example.

A^2E for Credit Card Numbers, PIN and CVV's

A Credit card number known technically as Primary Account Number (PAN), consist of 16 decimal digits. Although structure vary somewhat, commonly nine digit constitute the card holder account number.

Here in this case the message data length is 9 then the number of output for K_S = 3 is 134217728 where the chance to get correct pin is $7.450580597 \times 10^{-9}$.

A^2E for Authentication

We now show how to apply HE to RSA secret key by using the DTE introduced for authentication.

In some settings RSA is use to make the user's key readily available to attackers in such authorized access to a remote service using HTTPS or SSH. The client store RSA key to corresponding remote service.

Consider Theorem 5 of RSA – REJ – DTE

Then P_{Ks}, P_{Ke} are over the prime in $[2^{l-1}, 2^e]$ in adversary. In hold that then

Adv=

A^2E for secure data transfer:

Since the above statement is meant for smaller data.A^2E algorithm is also meant for large amount of data transfer regarding. Since it has low min-entropy the encryption rate is high and secured.

CONCLUSION

In this paper, we designed an A^2 encryption/ decryption which will provide more security form of algorithms which are in existence still now. Apart from providing double layer security with complexity of low latency and low min entropy and cryptography computer difficulties we can say this algorithm will provided two fold computing as well. Due to this reason A^2 encryption/ decryption algorithm possess high confidential strength. The presentation of this algorithm is illustrated with the help of small example using Turbo C for user interface. The cost of encryption will be comparatively lower than others which exist in real time. The future work of analysis the performance of the algorithm designed to withstand various cryptanalytic attacks.The embedded interfacing applications in order to use the memory efficiently in the device memory without compensation of the security and it is more suitable for real time application due to low latency.

ACKNOWLEDGMENT

Our sincere thanks to Dr. Dhanushkodi, Ph.D, Associative Dean ,PRIST UNIVERSITY, Puducherry. Mr. Mohan Kumar, M.E, Assistant Professor, Department of Electronics and Communication Engineering, PRIST UNIVERSITY, Puducherry. Mr. Udhaya Kumar,M.Tech ,Assistant Professor, Department of Computer Science Engineering, PRIST UNIVERSITY, Puducherry. Mis. Bharathi, M.Tech, Assistant Professor, Department of Computer Science Engineering, PRIST UNIVERSITY, Puducherry. Mr. Manoj, B.Tech Student, Department of Electrical and Electronics Engineering, PRIST UNIVERSITY, Puducherry.

REFERENCES

1. Basics of cryptography from Kioskea.net for encryption and decryption techniques.
2. Cormen T H, Leiserson C E, Rivestand R L and Stevn C (2009), *Introduction to Algorithm*, pp. 428–436, Press, Third Edition.
3. Cryptography & Neetwork security, Willian Stallings, Pearson Edu. inc.
4. Doonum M R and Soy Jaudah K M S (2010), "Analytical Comparison of Cryptographic Techniques for Resource – Constrained Wireless Security", *International Journal of Network Security,* Vol. 10, No. 3, pp. 213-219.
5. IJETCAS12-210, Sanjeev Dhawan, Alisha Saini, *International Journal of Emerging*

Technologies in Computational and Applied Science (IJETCAS).

6. JVELS and RISTEN PART, University Of Wiscon Sin, IJCES, Jan 29, 2003, version 1.1.
7. Nidhi Singhal and Raina J P S (2011), "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", *International Journal of Computer Trends and Technology*, July to Aug Issue 2011.
8. Programming Reference from Programming Simplified and C Programmer Blogspot for "ASCII GENERATOR".
9. Shannon C E Comm (1948), "Theory of Secrecy Systems", *Bell System Technical Journal,* Vol. 28, No. 4, pp. 656-715.
10. Yashant Kanetakar, Let us C for resource of C programming implementation.

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com