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 latency 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

\[ P(n) = \frac{1}{2^{\mu}} \]

Where \( q = 2^{\mu} \)

where \( \mu \) is length of the datable Framework.

Assume the value of \( \mu \) 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 \times 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 \times 10^{16} and chance to obtain the output is 1.387778781 \times 10^{-17}.

Hence the final equation is given as

\[ n = 2^{\mu}; \quad P(n) = \frac{1}{(2^{\mu})} = \frac{1}{n} \]

The above equation is a derived form of Poisson distribution.

Where \( q \) is number of logical operation and \( \mu \) is number of message bits.
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, \(X = [X_1, X_2, \ldots, X_M]\). 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 \(K = [K_1, K_2, \ldots, K_J]\) 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 an encrypted ASCII code.

For the defined adversary function

\[
S = f_n^k [\text{data}, Ke] \quad \text{S is output crypt data}
\]

\[
S^1 = \text{mod}[f_n^k [X(n), Ke] = \text{mod}[f_n^k [X(n), \text{DTE \_ REJ \_ RSA}(g(x))]]]
\]

\[
S^I = \text{mod}[f_n^k [ \sum_{j=0}^{n-1} M_j, \text{DTE \_ REJ \_ RSA}(g(x))]]
\]

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 \(P, Q, E (2e-1, 2e)\).

The rejection criterion for either \(P\) or \(Q\) distribution of primer uniform the range of \(e^{-1} \text{mod } (P-1) (Q-1)\) 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 \( P_m \) is uniform over primes in \([2^{e-1}, 2^e]\) for some \( e \geq 2 \) and RSA – REJ – DTE be scheme described above.

Then adversary \( (A) \leq \left(1 - \frac{1}{3^e}\right)^{-1} \) 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.

\[
\text{MeE M} = \frac{1}{n} = \frac{1}{2^e}
\]

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

6. Methodology Overview
logical diagram flow chart and programming algorithm with program output.

<table>
<thead>
<tr>
<th>Key Transfer Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Diagram of Key Transfer Technology]</td>
</tr>
</tbody>
</table>

This article can be downloaded from http://www.ijerst.com/currentissue.php
Logical Block Diagram for A² Encryption/Decryption Algorithm

```
<table>
<thead>
<tr>
<th>Input</th>
<th>ASCII Gen.</th>
<th>ASCII Code</th>
<th>Switch</th>
<th>Logical operator</th>
<th>Encrypted ASCII</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Encryption Key</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Flow Chart for A² Encryption/Decryption Algorithm

```
start -> Get the code -> ASCII Generation

switch

Key(Ka,Ka) -> Logical operation encryption key(Ke)

ASCII Generation

get the encrypted code -> stop
```

This article can be downloaded from http://www.ijerst.com/currentissue.php
Programming Output for Encryption Decryption Algorithm

<table>
<thead>
<tr>
<th>Encryption:</th>
<th>Decryption:</th>
</tr>
</thead>
<tbody>
<tr>
<td>enter the character</td>
<td>enter the character</td>
</tr>
<tr>
<td>enter the key</td>
<td>enter the key</td>
</tr>
<tr>
<td>the ascii value of A is 65</td>
<td>the ascii value of J is 74</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>1. And</td>
<td>1. And</td>
</tr>
<tr>
<td>2. Or</td>
<td>2. Or</td>
</tr>
<tr>
<td>3. Xor</td>
<td>3. Xor</td>
</tr>
<tr>
<td>enter the operation</td>
<td>enter the operation</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>74</td>
<td>65</td>
</tr>
<tr>
<td>Encrypted data is J_</td>
<td>decrypted data is A_</td>
</tr>
</tbody>
</table>

**PROGRAM LOGIC**

**Encryption Algorithm of a² 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.

**A²E 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 $7.450580597 \times 10^{-9}$. 

This article can be downloaded from http://www.ijerst.com/currentissue.php
A²E 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 $P_{ke}$ is over the prime in $[2^{l-1}, 2^e]$ in adversary. In hold that then

$$\text{Adv} = \text{A²E for secure data transfer:}$$

Since the above statement is meant for smaller data.A²E 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 A² 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 A² 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.
5. IJETCAS12-210, Sanjeev Dhawan, Alisha Saini, International Journal of Emerging
6. JVELS and RISTEN PART, University Of Wiscon Sin, IJCES, Jan 29, 2003, version 1.1.


