Adripathi Cipher

Rachana B. Nair

Independent Researcher

***Abstract*— The proposed algorithm deals with the determination of enciphered data using the concepts of substitution as one of the key ingredients. Secret key is generated which hides the plain text from the knowledge of adversaries. The key is kept secret. Each plain text alphabet has its own key to create the corresponding cipher text. The algorithm is based on symmetric key cryptographic system where the same key is used for both encryption and decryption. Underlying statistics of cipher text is hidden since same alphabet is not enciphered by the same key .The cryptanalysis is hard.**

***Keywords*— Adripathi cipher, cipher text, cryptography, decryption , encryption, plain text.**

I. INTRODUCTION

The goal of cryptographic algorithm system is to ensure the security of information from the adversaries. The information should be hidden and kept secure from unauthorized attackers [1]. Alteration or modification of data should be prevented at any cost. The availability of data /resources to authorized and authentic users should be ensured [2]. During transit as well as storage of information the data should not be maligned or accessed by unauthentic entities. In case of electronic transactions and e-commerce applications, the confidentiality and integrity are important requisites which should be attained by the incorporation of cryptographic techniques to the existing scenario. The cryptographic algorithm's strength lies on the secrecy of key (a secret component used for creating the cipher text) and also high level computation infeasibility for the crypt analyst to generate the key should be achieved by the algorithm. The randomness is the key property used in the algorithm. The properties of the algorithm should be well hidden from the cryptanalyst. The strength of the algorithm lies in the difficulty to determine the frequency of letters in the cipher text in comparison with the frequency of letters in English language , resulting in the failure to obtain any information regarding the message.

II. PROPOSED ALGORITHM- ADRIPATHI CIPHER

Step a) : Compute $y = k_z \bmod 26$

k_z value can be chosen by the communicating entities.

Step b): Generate a 3*3 matrix , A in the following manner.

$A_{mn} = y^* i \bmod 26$, elements of the matrix; where $0 \leq i \leq y+1$.

Step c): Compute determinant of A matrix , denoted as g and (g mod 26)= j , key.

Step d): Encryption:

$(p + j) \bmod 26 = c$

Decryption:

$(c - j) \bmod 26 = p$

Plain text letter is represented as 'p' and associated cipher text letter is denoted as 'c'.

y, k_z , matrix A ,g and j (key) are kept secret.

For the next letter of the plain text ,

$k_z' = (k_z + 1) \bmod 26$

then $y' = k_z' \bmod 26$.

The above mentioned algorithm is repeated again and again until all the alphabets of the plain text is exhausted, in other words until the entire plain text is transformed to an unintelligible form.

III. CONCLUSIONS

The algorithm hides the frequency of letters. It provides protection against cipher text only attacks.

Even known plain text attack is thwarted as each alphabet of plain text has its own key which would generate a different cipher text for the same letter.

In this algorithm, the influence of plain text on the structure of the cipher text is reduced. It also masks the frequency of letter. It also exhibits a feature of randomness.

ACKNOWLEDGMENT

I would like to thank my parents, teachers and almighty god for inculcating a strong belief in my capabilities and nurturing my inner strength to achieve any milestones.

REFERENCES

[1] A. J. Menezes, P.C. van Oorschot, S. Vanstone. "Handbook of Applied Cryptography," CRC Press Boca Raton FL USA. 1996.

[2] W. Stallings, "Cryptography and Network Security: Principles and Practice", Prentice-Hall Upper Saddle River, USA, 1999.