THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Cryptographic Techniqueusing Linear Transformation on Vector Space R^nFor Text Data

R.K.Gupta
Lovley Professional University, Phagwara
rajesh.gupta@lpu.co.in

Abstract: In this paper a different cryptographic algorithm is developed by using linear transformation on vector space with dimension n. Each character of the message is converted to number and then transformed to another number. This transformation is different for each character of message depending upon the position of character in the sequence. Uniqueness of the transformation is that if any character appearing twice will have different encryption. Modular arithmetic is also applied to reduce big numbers to small numbers. Key K is symmetric and has two components $\left(k^{(1)}, k^{(2)}\right)$ $where$ $k^{(1)}$ consists the dimension n of vector space and coefficients of linear transformation,$k^{(2)}$ is the basis set in which all the n vectors are linearly independent and can generate the vector space. Since basis set in not unique and it will increases the security level of symmetric key. Afterwards linear transformation defined will be represented by the matrix relative to the basis set. This process can be iterated n number of times for encryption of text data.

Keywords: Encryption, Decryption, Linear Transformation, Basis, Dimension and Modular Arithmetic.

1. Introduction

The fundamental objective of cryptography is to enable two people, to hide the communicated text message over an insecure channel in such a way that an opponent cannot understand what is being said. Encryption is the process of obscuring information to make it unreadable without special knowledge. This is usually done for secrecy and typically for confidential communications. A cipher consist of an algorithm for performing encryption as well as decryption. The original information is known as plaintext, and the encrypted form as cipher text. The cipher text message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it[1]. Ciphers are usually parameterized by a piece of auxiliary information, called a key. The encrypting procedure is varied and depending on the key which

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

changes the detailed operation of an algorithm[2]. Without the key, the cipher cannot be used to encrypt, or more importantly, to decrypt. In this paper linear transformation form vector space R^n to itself is used to hide the text message form the unauthorized person. There are two components of the symmetric key K. First component consist of dimension n of the vector space and various coefficients of transformation. Second component is the basis set of the vector space which is not unique and will increase the security level. Moreover all the vectors of basis set are linearly independent and can generate the vector space. Square matrix of order n of linear transformation relative to basis is generated for encryption and its inverse will be used for decryption[3].

2. Definitions

Cryptosystem: It consists of 5 tuple setconsisting of(P, C, K, E, D) where

P = Set of characters used in message = {A, B, C… Z, space, comma, full stop etc.}

C = Set of characters used in cipher text = {A, B, C… Z, space, comma, full stop etc.}

K = Set of all keys.

E = Set of one-one Encryption functions from P → C = $\{ e_k(x) = y \mid k \epsilon K , x \epsilon P, y \epsilon C \}$

D = Set of one-one decryption functions from C→ P = $\{ d_k(y) = x \mid k \epsilon K , y \epsilon C , x \epsilon P \}$

A commutative ring R with identity and $|R| = |P|$, and bijections $\alpha: L \to R \; and \; f: R \to R$ also taken into consideration[4].

Vector Space: Set V which satisfy the closed,associative,existence of identity,existence of inverse and commutative properties under operation of vector addition, also satisfy five properties under the operation of scalar multiplication by the elements of field F is called vector space . It is denoted by V(F).

Basis and Dimension: A subset B of vector space V is called basis iff B is linearly independent set and it generates V. Dimension is the number of elements in basis set B. Basis set is not unique and it is increases security level.

Linear Transformation: If $V_1 \; and \; V_2$ are two vector spaces, then a mapping $T: V_1 \to V_2$ is said to linear transformation if it satisfy additive and homogeneous property of mapping T.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

3. Mathematical Formulation

Consider the vector space R^n with the dimension n and basis set $B = \{b^1, b^2, \dots, b^n\}$where $or\ b^i = \left(b^i{}_1, b^i{}_2, \dots, b^i{}_n\right)$ $,i = 1,2, \dots, n.$ Linear transformation $T: R^n \to R^n$ is defined as $T(X) = (a^1.X, a^2.X, \dots, a^n.X)\ where\ X = (x_1, x_2, \dots, x_n)\ and\ a^i = \left(a^i{}_1, a^i{}_2, \dots, a^i{}_n\right), i = 1,2, \dots, n.$

Transformation of the vectors $b^1, b^2, \dots, b^n$ is given by

$$T\left(b^i\right) = \left(a^1.b^i, a^2.b^i, \dots, a^n.b^i\right) = \left(\alpha^i{}_1, \alpha^i{}_2, \dots, \alpha^i{}_n\right)$$

Since $b^1, b^2, \dots, b^n$ are the basis vectors, so the vector $T\left(b^i\right)$ can be expressed as linear combination of the vectors $b^1, b^2, \dots, b^n$.

$$T\left(b^i\right) = \left(\alpha^i{}_1, \alpha^i{}_2, \dots, \alpha^i{}_n\right) = \beta^i{}_1 b^1 + \beta^i{}_2 b^2 + \cdots + \beta^i{}_n b^n\ , i = 1,2, \dots, n$$

Matrix representation of L.T. relative to basis set B is

$$A = \begin{bmatrix} \beta^1{}_1 & \beta^2{}_1 & \dots & \beta^n{}_1 \\ \beta^1{}_2 & \beta^2{}_2 & \dots & \beta^n{}_2 \\ \dots & \dots & \dots & \dots \\ \beta^1{}_n & \beta^2{}_n & \dots & \beta^n{}_n \end{bmatrix}_{n \times n}$$

Symmetric key is $= \left(k^{(1)}, k^{(2)}\right)\ where\ k^{(1)} = (n, a^1, a^2, \dots, a^n)\ and\ k^{(2)} = B = \{b^1, b^2, \dots, b^n\}.$

Key K is used to generate the key matrix A.

Let $M =< m_1, m_2, \dots \dots, m_l >$ be the text message of length l(multiple of n otherwise pad with dummy characters).$P = \ Set\ of\ characters\ used\ in\ message\ =$ $\{A, B, C \dots Z, space, comma, full\ stop\ etc.\}$and corresponding numeric codes are in set $Z_{|P|} = \{0,1,2,3, \dots \dots, |P| - 1\}.$

The bijection map$\alpha: P \to Z_{|P|}$ will assign the numeric codes to each character of message .

Numeric coding of message is $N =< n_1, n_2, \dots \dots, n_l > where\ n_i \in Z_{|P|}$Take $l = dn,$ For the encryption of the message M , consider matrix of plaintext

$$L = \begin{bmatrix} n_1 & n_{n+1} & \dots & n_{(d-1)n+1} \\ n_2 & n_{n+2} & \dots & n_{(d-1)n+2} \\ \dots & \dots & \dots & \dots \\ n_n & n_{2n} & \dots & n_{dn} \end{bmatrix}_{n \times d}$$

Encryption of the text message is

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

$$Q = A \times L = \begin{bmatrix} \beta^1{}_1 & \beta^2{}_1 & \cdots & \beta^n{}_1 \\ \beta^1{}_2 & \beta^2{}_2 & \cdots & \beta^n{}_2 \\ \cdots & \cdots & \cdots & \cdots \\ \beta^1{}_n & \beta^2{}_n & \cdots & \beta^n{}_n \end{bmatrix}_{n\times n} \times \begin{bmatrix} n_1 & n_{n+1} & \cdots & n_{(d-1)n+1} \\ n_2 & n_{n+2} & \cdots & n_{(d-1)n+2} \\ \cdots & \cdots & \cdots & \cdots \\ n_n & n_{2n} & \cdots & n_{dn} \end{bmatrix}_{n\times d}$$

$$Q = \begin{bmatrix} e_1 & e_{n+1} & \cdots & e_{(d-1)n+1} \\ e_2 & e_{n+2} & \cdots & e_{(d-1)n+2} \\ \cdots & \cdots & \cdots & \cdots \\ e_n & e_{2n} & \cdots & e_{dn} \end{bmatrix}_{n\times d} mod|P|$$

The bijection mapα^{-1}: $Z_{|P|} \to P$ will convert the numerals obtained in matrix C to the text characters as

$$C = \begin{bmatrix} c_1 & c_{n+1} & \cdots & c_{(d-1)n+1} \\ c_2 & c_{n+2} & \cdots & c_{(d-1)n+2} \\ \cdots & \cdots & \cdots & \cdots \\ c_n & c_{2n} & \cdots & c_{dn} \end{bmatrix}_{n\times d}$$

The cipertext or the encrypted message is $< c_1, c_2, \ldots\ldots, c_l >$

For the decryption of ciphertext find the value of $A^{-1} mod\ |P|$

$L = A^{-1} mod\ |P| \times Q\ mod\ |P|$and get the original message .

4. Illustrative Example

Let the matrix of transformation T is$A = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$

Message is ATTACK

M =< A,T,T,A,C,K> assign A-Z 0-25

N = <0,19,19,0,2,10>

$$L = \begin{bmatrix} 0 & 0 \\ 19 & 2 \\ 19 & 10 \end{bmatrix}$$

$$Q = A \times L = \begin{bmatrix} 24 & 12 \\ 0 & 6 \\ 9 & 22 \end{bmatrix} mod 26$$

Ciphertext message is < 24,0,9,12,6,22> i.e. < Y,A,J,M,G,W>i.e YAJMGW

For decryption , find $A^{-1} mod 26 = \begin{bmatrix} 11 & 22 & 14 \\ 7 & 9 & 21 \\ 17 & 0 & 3 \end{bmatrix}$

$$L = A^{-1} mod 26 \times Q = \begin{bmatrix} 0 & 0 \\ 19 & 2 \\ 19 & 10 \end{bmatrix}$$

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Conclusion : Cryptographic technique developed above is secure from the attack as it uses the linear transformation and the basis set of this transformation. Security of the message increases as the basis set and linear transformation is not unique for a vector space. Transformation is defined from vector space R^n to R^n. It can also be defined on two different vector spaces with different dimensions.

5. References

[1] Simion, E. (2015, January/February). The Relevance of Statistical Tests in Cryptography. *IEEE Security & Privacy*, *13*(1), 66:70.

[2] Stallings, W. (2006). *Cryptography and Network Security: Principles and Practice*, 4th ed. Englewood Cliffs, NJ: Prentice Hall.

[3] A.Ramesh, Dr.A.Suruliandi "Performance Analysis of Encryption Algorithms for Information Security", International Conference on Circuits, Power and Computing Technologies 2013 IEEE.

[4] Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. New York: John Wiley & Sons.