International Journal of Mathematical Sciences © Serials Publications
Vol. 17, Nos. 3-4, July-December 2018, pp. 363-370 ISSN: 0972-754X

ENCRYPTION THROUGH GRAPH POLYNOMIALS

Anooja. I, Vinod. S and Biju. G. S

Abstract: Many researchers explored the concepts of graph theory that can be used in different areas of Cryptography. In this paper, we develop a cryptosytem using some graph polynomials.

Keywords: Chromatic polynomial, cryptosystem, matching, neighbourhood polynomial, private key, public key, vertex polynomial

2010 AMS subject classifications: 06C20, 94C15.

1. INTRODUCTION

Graph databases that store, manage, and query large graphs have received increased interest recently due to many large scale database applications that can be modeled as graph problems. Graph based public key algorithm was proposed in [1]. Some generalization of this method can found in [2] and [3]. Applications of algebraic graphs to cryptography started from symmetric algorithms based on explicit constructions of extremal graph theory and their directed analogs (see [4, 5, 6, 7]). The main idea is to convert an algebraic graph in finite automaton and use the preudorandom walks on the graph as encryption tools. This approach can be also used for the key exchange protocols. The idea to use arcs on graphs for encryption has been considered in [8] and [9].

In the process of developing a cryptosystem, first label all possible plaintext and ciphertext message units by mathematical objects from which functions can be easily constructed. To facilitate rapid enciphering and deciphering, it is convenient to have a rule for performing a rearrangement of N integers $0,1,2,...,N-1$ as enciphering transformation and use the operations addition and multiplication modulo N.

Here we discuss some new techniques for enciphering and deciphering using polynomials from graphs, which is more secure. In these methods, the sender and receiver must agree with the graph used for enciphering and deciphering before sending the message. In this paper we discuss a cryptosystem using some polynomials from graphs.

2. NEIGHBOURHOOD POLYNOMIAL METHOD

Most of the notations, definitions and results we mentioned here are standard and can be found in [11] and [12].

Let G be any graph. The neighbourhood complex N (G) of a graph G, whose vertices are the vertices of the graph G and whose faces are subsets of vertices that have a common neighbour. The neighbourhood polynomial of graph G is $neigh_G(x) = \sum_{U \in \mathcal{N}(G)} x^{|U|}$.

The vertex polynomial of G is defined as $V(G;x) = \sum_{k=0}^{\Delta(G)} v_k\, x^k$ where $\Delta(G) = \max\,\{\deg v \,/\, v \in G\}$ and v_k is the number of vertices of degree k.

Neighbourhood Polynomial Method

Suppose we have to send a message M consists of N alphabets. First, consider any graph G and form the neighbourhood polynomial $P(x)$ of the graph G. In order to enciphering the message, we use the following techniques.

Since we consider a polynomial, label each letter in our message by their numerical equivalents i.e., the message corresponds to its numerical equivalents $k_1, k_2, k_3, ..., k_n$ where each k_i represents each letter's numerical equivalent. Then the plaintext can be expressed as the form $M(x) = k_1 + k_2x + k_3x^2 + ... + k_nx^n$. This can be converted in to a ciphertext C by using the relation $C(x) = M(x)P(x)$, where $C(x) = l_1 + l_2x + l_3x^2 + ... + l_mx^m$, where each l_j is the additive modulo N of each numerical value obtained. Take all the coefficients from $C(x)$ and write down their corresponding alphabets to form the ciphertext C.

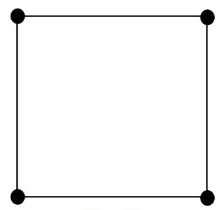
For deciphering, first we have to find the neighbourhood polynomial $P(x)$ of the same graph G. Then find $C(x)$ using C. Divide $C(x)$ by $P(x)$, we get $M(x)$ as $M(x) = k_1 + k_2x + k_3x^2 + ... + k_nx^n$. Take all the coefficients of and write down their corresponding alphabets, we get the original message M.

Illustration

Suppose, 'A' wants to send the following message to, 'B'.

$M =$ KILL HIM

For, consider $N = 27$ (label A to Z as 1 to 26 and space as 0) and choose $G = C_4$.



$G = C_4$

Figure 1

The neighbourhood polynomial of C_4 is $P(x) = 1 + 4x + 2x^2$.

The numerical equivalents of the message M are

11, 09, 12, 12, 00, 08, 09, 13

Now the polynomial corresponding to the plaintext is

$$M(x) = 11 + 9x + 12x^2 + 12x^3 + 0x^4 + 8x^5 + 9x^6 + 13x^7$$

Then find $C(x)$ by

$$C(x) = M(x)P(x)$$

$$= \left(11 + 9x + 12x^2 + 12x^3 + 0x^4 + 8x^5 + 9x^6 + 13x^7\right)\left(1 + 4x + 2x^2\right)$$

$$= 11 + 53x + 70x^2 + 78x^3 + 72x^4 + 32x^5 + 41x^6 + 65x^7 + 70x^8 + 26x^9$$

$$= 11 + 26x + 16x^2 + 24x^3 + 18x^4 + 5x^5 + 14x^6 + 11x^7 + 16x^8 + 26x^9$$

The coefficients of $C(x)$ are

11, 26, 16, 24, 18, 05, 14, 11, 16, 26

The corresponding ciphertext is C = KZPXRENKPZ.

Then send this to B. After receiving this message by B, B have to calculate the neighbourhood polynomial of $G = C_4$, $P(x) = 1 + 4x + 2x^2$.

Then write down the numerical equivalents of the alphabets in *C*. They are

11, 26, 16, 24, 18, 05, 14, 11, 16, 26

Find $C(x)$ as

$$C(x) = 11 + 26x + 16x^2 + 24x^3 + 18x^4 + 5x^5 + 14x^6 + 11x^7 + 16x^8 + 26x^9.$$

Now, divide $C(x)$ by $P(x)$, we get $M(x)$.

i.e., $M(x) = 11 + 9x + 12x^2 + 12x^3 + 0x^4 + 8x^5 + 9x^6 + 13x^7$

Take the coefficients of .

11, 09, 12, 12, 00, 08, 09, 13

Write down the corresponding alphabets, we get the original message *M*.

M = KILL HIM.

3. VERTEX POLYNOMIAL METHOD

Suppose we have to send a message M consists of N alphabets. First, consider any graph G and form the vertex polynomial $P(x)$ of the graph G.

In order to enciphering the message, we use the following techniques.

Since we consider a polynomial, label each letter in our message by their numerical equivalents. i.e., the message corresponds to its numerical equivalents $k_1, k_2, k_3, ..., k_n$ where each k_i represents each letter's numerical equivalent. Then the plaintext can be expressed as the form $M(x) = k_1 + k_2x + k_3x^2 + ... + k_nx^n$. This can be converted in to a ciphertext C by using the relation $C(x) = M(x)P(x)$, where $C(x) = l_1 + l_2x + l_3x^2 + ... + l_mx^m$, where each l_j is the additive modulo N of each numerical value obtained. Take all the coefficients from $C(x)$ and write down their corresponding alphabets to form the ciphertext C. For deciphering, first we have to find the vertex polynomial of the same graph G. Then find using C. Divide by, we get as. Take all the coefficients of and write down their corresponding alphabets, we get the original message M.

Illustration

Suppose, 'A' wants to send the following message to, 'B'.

M = KILL HIM

For, consider N = 27 (label A to Z as 1 to 26 and space as 0) and choose $G = C_4$.

The vertex polynomial of C_4 is $P(x) = 4x^2$.

The numerical equivalents of the message M are

11, 09, 12, 12, 00, 08, 09, 13

Now the polynomial corresponding to the plaintext is

$$M(x) = 11 + 9x + 12x^2 + 12x^3 + 0x^4 + 8x^5 + 9x^6 + 13x^7$$

Then find $C(x)$ by

$$\begin{aligned} C(x) &= M(x)P(x) \\ &= \left(11 + 9x + 12x^2 + 12x^3 + 0x^4 + 8x^5 + 9x^6 + 13x^7\right)\left(4x^2\right) \\ &= 0 + 0x + 44x^2 + 36x^3 + 48x^4 + 48x^5 + 0x^6 + 32x^7 + 36x^8 + 52x^9 \\ &= 0 + 0x + 17x^2 + 9x^3 + 21x^4 + 21x^5 + 0x^6 + 5x^7 + 9x^8 + 25x^9 \end{aligned}$$

The coefficients of $C(x)$ are

$$00, 00, 17, 09, 21, 21, 00, 05, 09, 25$$

The corresponding ciphertext is $C =$ QIUU EIY.

Then send this to B. After receiving this message by B, B have to calculate the neighbourhood polynomial of $G = C_4$, $P(x) = 1 + 4x + 2x^2$.

Then write down the numerical equivalents of the alphabets in C. They are

$$00, 00, 17, 09, 21, 21, 00, 05, 09, 25$$

Find $C(x)$ as

$$C(x) = 0 + 0x + 17x^2 + 9x^3 + 21x^4 + 21x^5 + 0x^6 + 5x^7 + 9x^8 + 25x^9.$$

Now, divide $C(x)$ by $P(x)$, we get $M(x)$.

i.e., $M(x) = 11 + 9x + 12x^2 + 12x^3 + 0x^4 + 8x^5 + 9x^6 + 13x^7$

Take the coefficients of $M(x)$.

$$11, 09, 12, 12, 00, 08, 09, 13$$

Write down the corresponding alphabets, we get the original message M.

$M =$ KILL HIM.

Analogous to this, we can use various polynomials obtained from a graph.

For,

1. Adjacency Polynomial

Consider any graph G and form the characteristic polynomial $P(x)$ of adjacency matrix of the graph G. This polynomial is the adjacency polynomial and proceed as in the above method.

Example

Consider the same graph and the same message M =KILL HIM given in the previous case.

The adjacency matrix of C_4 is $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$

The characteristic polynomial is $P(x) = x^4 - 4x^2$.

The numerical equivalents of the message M are

11, 09, 12, 12, 00, 08, 09, 13

Now the polynomial corresponding to the plaintext is

$$M(x) = 11 + 9x + 12x^2 + 12x^3 + 0x^4 + 8x^5 + 9x^6 + 13x^7$$

Then find $C(x)$ by

$$C(x) = M(x)P(x)$$

$$= (11 + 9x + 12x^2 + 12x^3 + 0x^4 + 8x^5 + 9x^6 + 13x^7)(x^4 - 4x^2)$$

$$= 0 + 0x - 44x^2 - 36x^3 - 37x^4 - 39x^5 + 12x^6 - 20x^7 - 36x^8 - 44x^9 + 9x^{10} + 13x^{11}$$

$$= 0 + 0x + 10x^2 + 18x^3 + 17x^4 + 15x^5 + 12x^6 + 7x^7 + 18x^8 + 10x^9 + 9x^{10} + 13x^{11}$$

The coefficients of $C(x)$ are

00, 00, 10, 18, 17, 15, 12, 07, 18, 10, 09, 13

The corresponding ciphertext is C = _ _ JRQOLGRJIM.

Then send this to B. After receiving this message by B, B have to calculate the characteristic polynomial of adjacency matrix of $G = C_4$, $P(x) = x^4 - 4x^2$.

Then write down the numerical equivalents of the alphabets in C. They are

00, 00, 10, 18, 17, 15, 12, 07, 18, 10, 09, 13

Find $C(x)$ as

$C(x) = 0 + 0x + 10x^2 + 18x^3 + 17x^4 + 15x^5 + 12x^6 + 7x^7 + 18x^8 + 10x^9 + 9x^{10} + 13x^{11}$.

Now, divide $C(x)$ by $P(x)$, we get $M(x)$.

i.e., $M(x) = 11 + 9x + 12x^2 + 12x^3 + 0x^4 + 8x^5 + 9x^6 + 13x^7$

Take the coefficients of $M(x)$.

11, 09, 12, 12, 00, 08, 09, 13

Write down the corresponding alphabets, we get the original message M.

M = KILL HIM.

2. Path Polynomial

Consider any graph G and take any path P from the graph G and form the path polynomial $P(x)$ of the path P. Then proceed as in the above method.

Example

The message KILL HIM can be coded as KTEQFEBCCVM using the path $v_1\, e_1\, v_2\, e_2\, v_3\, e_3\, v_4$ and the corresponding path polynomial as $P(x)=1+x+x^2+x^3$.

3. Matching Polynomial

Consider any graph G and take any matching from the graph G and form the matching polynomial $P(x)$. Then proceed as above.

Example

The message KILL HIM can be coded as KIWULTIUIM using the matching $\{e_1, e_3\}$ and the corresponding matching polynomial is $P(x)=1+x^2$.

4. CHROMATIC POLYNOMIAL

Consider any graph G and form the chromatic polynomial $P(x)$. Then proceed as above.

Example

The message KILL HIM can be coded as _ PXIHIV _ QTGM using the chromatic polynomial is $P(x)=x(x-1)^3=x^4-3x^3+3x^2-x$.

5. CONCLUSION

We have developed a cryptosystem using certain graph polynomials which will be used for data encryption and decryption with higher security.

REFERENCES

[1] V. A. Ustimenko, Maximality of affine group, and hidden graph cryptosystems, J. Algebra and Discrete Math., 10, 51-65, (2004).

[2] V. Ustimenko, On the extremal graph theory for directed graphs and its cryptographical applications In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko, Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, 3, 181-200 (2007).

[3] V. Ustimenko, On the graph based cryptography and symbolic computations, Serdica Journal of Computing, Proceedings of International Conference on Application of Computer Algebra, ACA-2006, Varna, N1 (2007).

[4] V. A. Ustimenko, Explicit constructions of extremal graphs and new multivariate

cryptosystems, Studia Scientiarum Mathematicarum Hungarica, Special issue "Proceedings of The Central European Conference, 2014, Budapest", 52, 185-204 (2015).

[5] V. A. Ustimenko, Graphs with Special Arcs and Cryptography, Acta Applicandae Mathematicae, 71, N2, 117-1530, (2002).

[6] V. Ustimenko, On the extremal graph theory for directed graphs and its cryptographical applications, In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko. Advances in Coding Theory and Cryptography. Series on Coding and Cryptology, 3, 2007, P. 181–200.

[7] V. A. Ustimenko, On the flag geometry of simple group of Lie type and Multivariate Cryptography, Algebra and Discrete Mathematics. 19(1), 130-144, (2015).

[8] V. A. Ustimenko, Random walks on special graphs and Cryptography, Amer. Math. Soc. Meeting, Loisville, March, 1988.

[9] V. A. Ustimenko, Coordinatization of regular tree and its quotients, In the volume "Voronoi's Impact in Modern Science": (Proceedings of Memorial Voronoi Conference, Kiev, 1998), Kiev, IM AN Ukraine, July, 1998, pp. 125 - 152.

[10] V. Ustimenko, A. Woldar, Extremal properties of regular and affine generalized polygons of tactical configurations, 2003, European Journal of Combinatorics, 2003, 24 , 99-111.

[11] N. Koblitz. Algebraic methods of cryptography, Berlin Heidelberg New York: Springer, 1998.

[12] A. J Menezes, Paul C Van Oorschot, and Scott A Vanstone, Handbook of Applied Cryptography. Discrete Mathematics and Its Applications. CRC press, New York, 1996.

Anooja. I
Department of Mathematics,
CMS College Kottayam (Autonomous),
Kottayam, Kerala, India

Vinod. S
Department of Mathematics,
Government College for Women,
Thiruvananthapuram, Kerala, India

Biju.G.S
Department of Mathematics,
College of Engineering,
Thiruvananthapuram, Kerala, India