Application of Graphs in Security

Debajit Sensarma, Samar Sen Sarma

Abstract**: *Now-a-days in the era of Big Data huge information is gathered in every second. Humans are now already interconnected via smart phones, gadgets, smart meters and other smart appliances. Also all these computing devices are fully connected to each other and this is known as "Internet of Things" which produces crucial information in every moment. These sensitive information needs to be protected. So, design of a good security mechanism is needed to provide protection against unauthorized attacks on this information. This article mainly takes cryptography and graph as a tool and concentrated on designing two public key encryption scheme based on graph where the first protocol is based on properties of matrices generated from graph. The aim is to protect the message graph generated from a given message. The second protocol is based on the properties of graphical codes.***

Keywords**: *Graph, Information Security, Cyber Security, Cryptography, Graphical Codes.***

I. INTRODUCTION

Security is about protection of assets from the various threats posed by certain inherent vulnerabilities. Security mechanisms deals with the countermeasures that have to be taken to reduce the risk arise from network vulnerabilities [1]. C.E. Shannon [2] defined secrecy system as a set of transformations of one space (the set of possible messages) into another space (the set of possible cryptograms). Each particular transformation corresponds to enciphering with a particular key. The transformation must be non singular, so that unique deciphering is possible when the key is known. There are three general types of secrecy systems i.e. i) concealment system, including such methods as invisible ink, concealing a message in an innocent text, or in a fake covering cryptogram, or other methods in which the existence of the message is concealed from the enemy, ii) privacy system, for example speech inversion, in which special equipment is required to recover the message and iii) the third type is the "true" secrecy systems where meaning of the message is hidden by cipher, code etc. This work mainly considers the third type of secrecy system. According to C.E. Shannon the security can be of different kind. a) *Unconditional security:* A cryptographic primitive is said to be unconditionally secure if one can prove that it cannot be broken even if attacker have infinite computational resources. This is the strongest kind of security we can achieve. Note that under this assumption attacker is allowed to do an *exhaustive key search*, i.e., exhaustively try all possible keys. b) *Computational security:* A cryptographic primitive is said to be computationally secure if one can prove that the best algorithm for breaking it requires at least t operations, where t is some large fixed number. It is a very rare event that a cryptosystem can be proved secure under this assumption. c) *Provable security:* A cryptographic primitive is said to be provably secure if its security can be reduced to some well-studied problem. This means that breaking the primitive implies that one can solve the well-studied problem. For example, a primitive might have been proved secure provided that an integer n cannot be factored. The security has then been reduced to the factoring problem. As long as we cannot factor large integers, the primitive is secure. d) *Heuristic security:* If there is no known method of breaking the primitive but we cannot prove the security in any sense. Actually, most ciphers used today have a security of this kind.

Providing Information Security is the practice of protecting information from unauthorized access, disclosure, disruption etc. According to [3] Information Security prevents confidentiality, integrity and availability of information where information can be in any form like written on a paper, stored electronically, transmitted by post or electronic medium etc. The international standard ISO/IEC 13335-1 (2004) [4] defines Information Communication Technology (ICT) security as all aspects relating to defining, achieving and maintaining the confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of information resources. Next, International Telecommunication Union (ITU) [5] defines Cyber Security as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Often the term Cyber Security and Information Security are used interchangeably. Actually they are not same but have some close relations between them and Cyber Security is the subset of Information Security. Fig. 1 depicts the possible overlap between Information Security, ICT security and Cyber Security. On the other hand, network security is also the subset of Cyber Security. It protects organizations IT infrastructure and network accessible resources from all kinds of cyber threats. This security mainly protects passwords, firewalls, internet access, encryption, backups etc.

Cryptography [6, 7] is an art to provide information security and authentication. It is a science which studies the techniques for secure communication in the presence of intruders or unauthenticated access. It is about constructing and analyzing protocols that overcome the influence of intruders.

Revised Manuscript Received on August 01, 2019

***** Correspondence Author

Debajit Sensarma, Assistant Professor, Dept. of Computer Science, Vivekananda Mission Mahavidyalaya, Vidyasagar University, India.

Samar Sen Sarma, Professor, Dept. of Computer Science & Engineering, University of Calcutta Kolkata, India.

Cryptography converts the original message in a non-readable format and sends the message over an insecure channel. The original message is called plain text. Disguising the plain text to hide its original contents is called encryption. The non readable format of the plain text after encryption is called cipher text. The process of reverting the cipher text to its corresponding plain text is called decryption process. For both encryption and decryption process key is used. It is used with plain text at the time of encryption and with the cipher text at the time of decryption.

Cryptography provides number of security goals to ensure the privacy of the data. The goals of the cryptography are Confidentiality, Integrity, Availability, Authenticity, Non Repudiation, Access control [3, 6, 7]. In cryptography the encryption algorithms can be classified into two broad categories- Symmetric key or private key cryptography and asymmetric key or public key cryptography. In Symmetric key cryptography the key used for encryption and decryption is same. Thus, the key must be distributed through the secure channel before transmission started. These types of algorithms are highly depended on the nature of the key. DES, Triple DES, AES, RC4, RC6, BLOWFISH etc are the example of symmetric key algorithms. In asymmetric key cryptography two different keys are used for encryption and decryption, they are private and public key. The public key is available to all in the network. The sender who wants to transmit message, encrypts the message with receiver's public key and only the authorized receiver can decrypt the message with its private key. RSA, SSH are the example of asymmetric key cryptography.

Many real world problems can be formulated in terms of graph by taking it as a mathematical tool such that solving the later problem can give a suitable solution to the former one. For instance, the psychologist Lewin proposed that the "life space" of a person can be modeled by a planar graph, in which the faces represent the different environments [8]. As observed by D.E. Knuth [9] graph theoretical terminology and graph theorist are numerically comparable at this time. The field graph theory started its journey from the problem of "Koinsberg bridge" in 1735.Graph algorithms can be treated as unified solution approach in many classical and modern application areas. The main concern is to design and adapt the art to various and numerous areas of real life industrial and engineering problems. This article mainly concentrated on designing two public key encryption scheme based on graph where the first protocol is based on properties of matrices generated from graph. The aim is to protect the message graph generated from a given message. The second protocol is based on the properties of graphical codes.

The paper is organized as follows: In section II contains some related works. In section III two proposed **Algorithm 1** has been described and **Algorithm 2** has been depicted in section IV. Section V contains illustrative examples related to both Algorithm 1 and Algorithm 2. Section VI contains security analysis of both the methods and section VII concludes the paper by giving some future scopes.

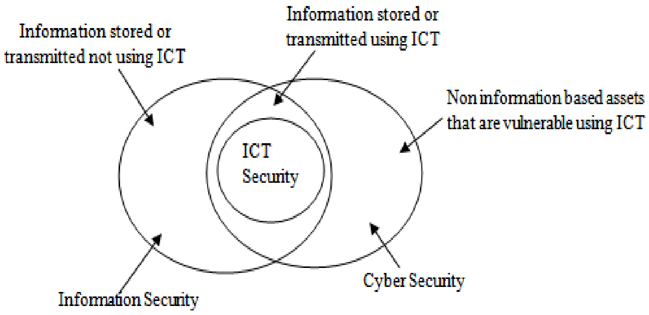
Information stored or transmitted not using ICT
Information stored or transmitted using ICT
Non information based assets that are vulnerable using ICT
ICT Security
Information Security
Cyber Security

Fig.1.Relationship between Information Security and Cyber Security [1].

II. RELATED WORKS

This section contains some encryption algorithms based on graphs and error correcting codes. Firstly [10] proposed an encryption algorithm based on cycle graph, complete graph and minimum spanning tree for generating a complex cipher text using a shared key. Next, authors of [11] proposed an encryption algorithm based on cipher block chaining method. They used degree sequence of graph constructed from any music note as key. In [12] authors proposed an encryption method using Hamiltonian path properties where encryption occurs in two steps. Once using Hamiltonian path and next using weighted adjacency matrix. Authors of [13] also used Hamiltonian circuit of graph for encryption of data. The authors of [14] have designed a secure cryptographic protocol taking advantages of two intractable problems namely Hamiltonian Path Problem and Graph Automorphis m problem. The algorithm is constrained based partial symmetric key algorithm. Classical Data Encryption Standard (DES) algorithm coupled with two above mentioned intractable problems are used to design the secure algorithm (GMDES). We have worked with a 4- cube graph and each vertex of that graph is encoded with 4 bit binary number. An arbitrary Hamiltonian Path of that graph represented by a sequence of binary symbols is used as the secret key and its 16 non -automorphic Hamiltonian Paths chosen randomly are used as the sub keys. The sub keys are stored in a secure mapping table of sender in an encrypted form. In [15] authors show how graph can be used to design Vignere cipher. Next authors of [16] uses algebraic graphs to design a symmetric key encryption algorithm. Authors of [17] designed an algorithm for encrypting a message graph to be transmitted securely. It is based on unconditional mapping, conjectured to be a trapdoor one-way function, designed for graphs. In [18] authors designed polyalphabetic subtraction cipher using paths between pair of graph vertices. Authors of [19] designed visual cryptography based on graph where every node and every edge are assigned arbitrary images. Besides this authors of [20, 21] designed encryption algorithm based on error correcting codes which is also termed as code based cryptography.

III. PROPOSED ALGORITHM 1

Theorem 1: All positive integer power of matrix M commute with all other positive integer powers of M [22].

Theorem 2: Scalar multiplication of matrices commutative [23].

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The proposed method contains four algorithms:
i) Receiver Side Key generation algorithm which produces a public and a private key (**Algorithm I**). Here two n x n matrices '**A**' and '**B**' has been taken and they are not multiplicative commutative to each other. Matrix C has been calculated by multiplying matrix A and B (i.e. C=ABA). Another n x n matrix '**P**' has been generated using theorem 1 and theorem 2 which is multiplicative commutative to matrix A (i.e. AP=PA). So, the public key is (C, B, P) and private key is A.
ii) Sender Side Graph Generation Algorithm algorithm (**Algorithm II**). Algorithm generates a message graph n x n adjacency matrix '**G**' which has to be sent.
iii) Sender Side Encryption Algorithm (**Algorithm III**): Sender generates another n x n matrix '**D**' using theorem 1 and theorem 2 which is multiplicative commutative to matrix P (i.e. PD=DP). A secret key matrix K has been generated by multiplying matrix D to matrix C (i.e. K= DCD). Another matrix E has been generated by multiplying matrix D to matrix B (i.e. E= DBD). Lastly a n x n matrix '**L**' has been produced by adding matrix G with matrix K and L along with E has been sent to the receiver.
iv) Receiver Side Decryption algorithm (**Algorithm IV**): Receiver knows 'n'. Receiver finds the secret key K by calculating K = AEA or K= ADBDA or K = DABAD (as AP=PA, PD=DP then AD = DA) or K=DCD. Then subtract K from L to get G and decrypt G.
The algorithms are depicted below:

Algorithm I: Receiver Side Key Generation Algorithm:

Step 1: Compute (n x n) adjacency matrices of two arbitrary graphs namely A and B with n vertices Where $AB \neq BA$.
Step 2: Multiply A, B and A to produce matrix C, i.e. C=ABA.
Step 3: Compute another (n x n) matrix P which is multiplicatively commutative with matrix A, i.e. AP=PA. The matrix P is generated by taking any power 'r' of matrix A and multiplying a scalar 's' with the resultant matrix, i.e. $P=s*A^r$.
Step 4: Receiver's public key is (C, B, P) and private key is A.

Algorithm II: Sender Side Graph Generation Algorithm:

Step 1: Let the vertex set be V= $\{v_1, v_2,...,v_n\}$, corresponding to the bit string $b_1,b_2,b_3,....b_n$.
Step 2: For each bit b_i
i) If b_i=1 then
a) Search the next two bits b_j and b_k such that b_j = 1 and b_k = 1 until i = j mod n or i = k mod n.
b) If no such b_j or b_k is found the go to (ii).
c) Else If only b_j is found add an edge (v_i,v_j) to E if edge (v_i,v_j) is not in E.
d) Else add egde (v_i,v_j) and (v_i,v_k) to E if edges (v_i,v_j) and (v_i,v_k) are not in E.
ii) If b_i=0 then
a) Search for the next bit b_m such that b_m = 1 until i=m mod n.
b) Add edge (v_i,v_m) to E if the edge is not present in graph G.

Algorithm III: Sender Side Encryption Algorithm:

Step 1: Compute an (n x n) matrix D which is multiplicatively commutative with matrix P, i.e. PD=DP. The matrix D is generated by taking any power 'r' of matrix P and multiplying a scalar 's' with the resultant matrix, i.e. $D=s*P^r$.
Step 2: Multiply D to C to produce the secret key matrix K (i.e. K=DCD) and also multiply D to B to produce a matrix E (i.e. E=DBD).
Step 3: Add G (produced from graph generation algorithm at sender side) to K to produce matrix L and send L along with matrix E to the receiver.

Algorithm IV: Receiver Side Decryption Algorithm:

Step 1: Compute key matrix K from K=AEA.
Step 2: Subtract K from L to produce matrix G.
Step 3: For each vertex v_i $\{v_1, v_2,...,v_n\}$ in G
If deg(vi) >= 2 then Store b_i=1.
Else store b_i=0.
Step 4: Return the bit string b $(b_1, b_2,.....,b_n)$.

IV. PROPOSED ALGORITHM 2

The algorithm is based on Graphical Codes. So, next sections describe Graphical Codes and the proposed algorithm.

A. *Graphical Codes*

In this section the concepts of Graphical Codes [24] are given in a nutshell. For general graph theory background reader can refer to [25]. Let, G (V, E) be a connected undirected graph with V = $\{v_1,...v_n\}$ vertices and E = $\{e_1, ...e_m\}$ edges. An Euler sub-graph of a graph G is a sub-graph g, in which every vertex has even degree. According to [9] Euler sub-graph is either a circuit or edge disjoint union of circuits. Every sub-graph g can be described using a binary characteristic vector g = $(g_1,..., g_m)$, where g_i = 1 if e_i is an edge of g and g_i = 0 otherwise ($1 \leq.i \leq m$). There are two subspaces associated with every graph. Circuit Space (W_Γ) or Cycle Space generated by all circuits or edge disjoint union of circuits of G and Cut-set Space or bond space (W_S) generated by every cut-sets or edge disjoint union of cut-sets. Let, t is a spanning tree of G. So, each edge not in t forms circuit with t and the characteristic vectors of these (m-n+1) circuits are linearly independent and this linearly independent row vectors forms a matrix of dimension W_Γ , is called Fundamental Circuit matrix. Similarly, each edge of t is associated with the cut-set of G and has (n-1) linearly independent cut-sets which also generates a matrix of dimension W_S, called Fundamental Cut-set matrix. It can be shown from [25] that, W_Γ and W_S are orthogonal to each other. So, from the above description, it is clear that the Circuit Space (also Cut-set Space) of G forms binary linear code C, with parameters [n, n-m+1, g] (also [n, n-1, g]), where g is the girth of G. The code C is termed as Graphical Code. Basically, in this paper Circuit code is considered and here Fundamental Circuit matrix acts as generator matrix and Fundamental Cut-set matrix acts as Parity Check matrix. The circuit code is denoted as C_E (G). These codes are firstly studied in [26].

The objective was to show that possibility of augmenting the Graphical Code (also called even graphical code [27]) to the larger dimension by keeping minimum distance unchanged and also to provide a decoding algorithm for these codes. Next, in [27, 28], authors shows an improvement over the decoding procedure using combinatorial optimization technique. T-join of the graph G, where $T \subseteq V$, is a subset of edges E, which has odd degree at every vertex in T and even degree in every other vertex. Necessarily T has even cardinality. The smallest possible cardinality of T-join will be denoted by τ (G, T). According to [14] the covering radius is equals the maximum vertex join number τ (G), where τ (G) = $\max_T$ (τ (G, T)), which is the largest size of the minimum T-join for any even vertex set T.

B. *Algorithm 2:*

The proposed method contains three algorithms:

Algorithm I: Receiver Side Key Generation Algorithm:

Step 1: Receiver selects binary (n, k) linear graph theoretic code which can correct t errors. A fundamental circuit matrix G is generated which is used as generator matrix.
Step 2: Receiver selects a k x k nonsingular matrix S.
Step 3: Receiver selects a random n x n permutation matrix P.
Step 4: Receiver computes a k x n matrix D = SGP.
Step 5: Receiver's public key is (D, t) and private key is (S, G, P, H). Here H is the fundamental cutset matrix which is used as parity check matrix.

Algorithm II: Sender Side Message Encryption Algorithm:

Let, sender wants to send message m with k bits to the receiver.
Step 1: Sender computes C = mD.
Step 2: A random n bit vector R has been generated which has exactly t ones.
Step 3: Sender computes the cipher text $C_F = C + R$.

Algorithm III: Receiver Side Decryption Algorithm:

Upon receipt of C, receiver decrypts the message using following steps.
Step 1: Receiver computes inverse of P (i.e. P^{-1}).
Step 2: Receiver computes $y= CP^{-1}$.
Step 3: Receiver uses decoding algorithm to decode y to L (where L=mS).
Step 4: Receiver computes $m= LS^{-1}$.

V. ILLUSTRATION WITH EXAMPLES

A. *Example 1 for **Algorithm 1**:*

At first key is generated at the receiver side using **Algorithm I**.

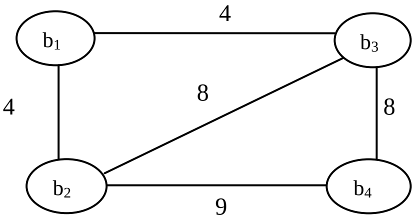

Fig.2. Arbitrary Weighted Graph

	b_1	b_2	b_3	b_4
b_1	0	4	4	0
b_2	4	0	8	9
b_3	4	8	0	8
b_4	0	9	8	0

Fig.3. Adjacency matrix (B) of a weighted graph

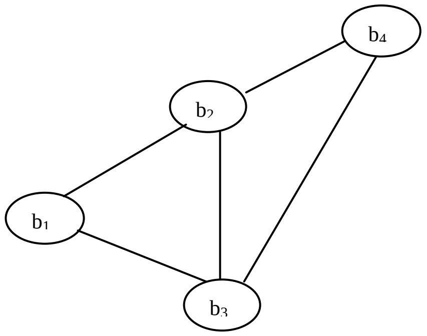

Fig.4. Arbitrary tree (**T**)

	b_1	b_2	b_3	b_4
b_1	0	1	1	0
b_2	1	0	1	1
b_3	1	1	0	1
b_4	0	1	1	0

Fig.5. Reduced incidence matrix (A) of an arbitrary tree T

16	33	33	16
33	24	33	33
33	33	26	33
16	33	33	16

Fig.6. Matrix C

216	348	348	216
348	384	396	348
348	396	384	348
216	348	348	216

Fig.7. Matrix P (Generated by s=12 and r=5)

Then, 4 x 4 adjacency matrix has been generated by sender using **Algorithm II**. The process is depicted below:

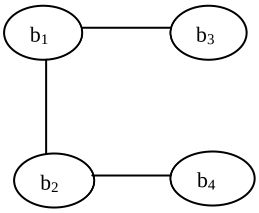

Fig.8. Desired message graph

	b_1	b_2	b_3	b_4
b_1	1	1	1	0
b_2	1	0	0	1
b_3	1	0	0	0
b_4	0	1	0	0

Fig.9. Adjacency matrix (G) of the graph

Next, sender computes matrix D, K, E using **Algorithm III**.

1006560	1265328	1265328	1006560
1265328	1639440	1639008	1265328
1265328	1639008	1639440	1265328
1006560	1265328	1265328	1006560

Fig.10. Matrix D (Generated by s=3 and r=2)

586802745713664	751250037567744	751251130811136	586802745713664
751250037567744	961741707706368	961743125488896	751250037567744
751251130811136	961743125488896	961744540285440	751251130811136
586802745713664	751250037567744	751251130811136	586802745713664

Fig.11. Matrix E

Fig.12. Matrix K

89298306745344	114462520250112	114462085416192	89298306745344
114462520250112	146701232303616	146700687174912	114462520250112
114462085416192	146700687174912	146700139060224	114462085416192
89298306745344	114462520250112	114462085416192	89298306745344

Fig.13. Matrix L

586802745713665	751250037567745	751251130811137	586802745713664
751250037567745	961741707706368	961743125488896	751250037567745
751251130811137	961743125488896	961744540285440	751251130811136
586802745713664	751250037567745	751251130811136	586802745713664

Receiver computes matrix K =AEA and subtract K from L to produce G. Then receiver decrypts G using **Algorithm IV**.

B. *Example 2 for Algorithm 2:*

Complete graph K_n gives rise to a binary linear code with parameters [${}^{n}C_2$, (n-1) (n-2)/2, 3] where number of edges = ${}^{n}C_2$, number of vertices =n and girth= 3[28]. We have constructed the example with n=5. For n=5, it is a code with covering radius = 2.

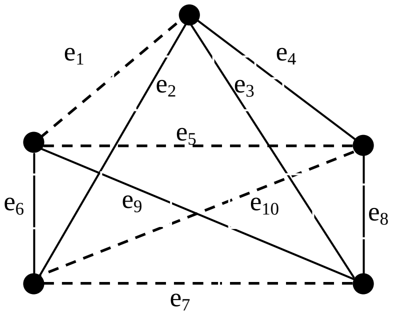

Fig.14. 5-vertex Complete Graph

Fig.15. Matrix G

e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}
1	1	0	0	1	0	0	0	0	1
1	0	1	0	1	0	1	0	0	1
1	0	0	1	1	0	0	0	0	0
0	0	0	0	1	1	0	0	0	1
0	0	0	0	0	0	1	1	0	1
0	0	0	0	1	0	1	0	1	1

Retrieval Number J11330881019/2019©BEIESP
DOI: 10.35940/ijitee.J1133.0881019

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}
1	1	1	1	0	0	0	0	0	0
0	1	1	1	1	1	0	0	1	0
0	1	1	0	0	1	0	1	1	1
0	0	1	0	0	0	1	1	1	0

Fig.16. Matrix H

0	1	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	1	0	0	0	0
0	0	0	1	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	1	0	0	0

Fig.17. Permutation matrix P

0	1	1	0	1	1
0	1	1	1	0	0
1	0	0	1	1	1
1	1	1	0	0	1
1	1	1	1	1	1
1	0	1	0	1	1

Fig.18. Nonsingular matrix S

1	0	0	0	1	1	1	1	1	1
1	0	0	1	1	1	0	1	0	0
0	1	1	1	0	1	0	0	1	1
1	1	1	0	1	0	1	0	0	1
1	1	1	1	1	1	1	1	1	1
0	0	1	0	1	1	1	0	1	1

Fig.19. Matrix D = SGP

Suppose, we want to send message m = 110001 (mG= 0110100011)

So, sender computes, C= mD = 0011110000.

Add random n bit error pattern R with one in the second position = 0100000000.

The final encrypted message is $C_F = C+R = 0111110000$.

Now, to decrypt the message receiver first compute $y= C_F P^{-1} = 1101110000$.

The error is now at the 1st position. When these are corrected with the error correcting algorithm, the receiver has found codeword L = 0101110000.

Now, from L receiver finds "mS" from the 2nd,3rd, 4th, 6th, 8th, 9th bit positions, i.e. mS= 101100.

Finally, the message m is recovered by multiplication with S^{-1}.

$$m = mSS^{-1}$$
$$= (101100).$$

1	1	1	0	0	0
0	1	1	0	0	1
0	1	0	0	1	1
0	1	1	0	1	0
0	1	1	1	0	0
1	1	0	1	1	0

Fig.20. Inverse of Matrix S

$$= 110001$$

VI. SECURITY ANALYSIS

This section contains security analysis of two proposed methods.

A. *Redundancy and efficiency:*

Redundancy = (Number of bits used to transfer the message) / (Actual number of bits in the message)

Efficiency =1/Redundancy.

Algorithm 1:

Redundancy = (n x n) / n = n
Efficiency = 1/n

Algorithm 2:

Redundancy = $(n \text{ x } (n-k)) / k = (n^2/k) - n$.
Efficiency = $1/(n^2/k) - n$.

B. *How secure the algorithms are?*

In case of **Algorithm 1**, attacker may try to utilize all the information provided in the public key to encrypt the message. So, first a known matrix M has been defined from C and P.

$$M = CPC^{-1} \quad \dots \text{(i)}$$

As C contains matrix B as a factor and P commute with A, so, $CP \neq PC$ and $M \neq P$.
Next, eliminate C from (i) to get,

$$M = (ABA)\, P\, (ABA)^{-1} \quad \dots \text{(ii)}$$

As, A and P must commute, swap P with A to get,

$$M = ABPAA^{-1}B^{-1}A^{-1} \quad \dots \text{(iii)}$$

Matrix A commutes with P but not matrix B. So, P does not commute with B. Then, suppose a known matrix N is defined as

$$N = BPB^{-1} \quad \dots \text{(iv)}$$

As, $BP \neq PB$, then $N \neq P$. So, from (iii) $M=ANA^{-1}$, N contains matrix B as a factor, so, $AN \neq NA$ and therefore $M \neq N$.
Nextly, P is obtained by power of matrix A and multiplication with any scalar. So, for large power it is very hard to generate P, also without knowing A and same it true for matrix D.

In case of **Algorithm 2**, attacker can at first try to guess generator matrix G but as G is generated arbitrarily from any graph for each transmission, it has very low chance to guess G correctly. Then attacker may try to guess matrix S and P. Matrix S is an nonsingular and invertible matrix of size k x k. So, the rows of the matrix S are linearly independent. Therefore, the total number of invertible binary matrices of size k x k are$\prod_{i=0}^{k-1}(2^k - 2^i)$.

Next, the number of possible permutation of size n x n is n!. So, the chance of guessing correctly matrix S is 1/$\prod_{i=0}^{k-1}(2^k - 2^i)$ and for finding permutation matrix the chance is 1/n!. So, for large k and n it is very hard to rightly guess matrix S and P. Besides this attacker may try to generate all possible 2^k codewords. But, as decoding general linear (n, k) codes in NP-Complete [20], it is very hard to guess the correct codeword.

VII. CONCLUSION

In this article two graph based public key cryptosystem has been proposed for protecting valuable information. The first method is purely based on properties of matrices. The second method is based on graphical code. Therefore, this is a candidate of code based cryptography. Security analysis of both the methods has been done. From the above exam 1 and 2 in section V it can be seen that for 6 bit message the efficiency of Algorithm 1 is 0.17 but the efficiency of Algorithm 2 is 0.15 which is slightly better than the former. Future works can be based on decreasing the key size by compressing the matrix or in other methods and designing Algorithm 2for post quantum cryptography which requires further study and analysis.

ACKNOWLEDGMENT

The authors would like to thank dept. of Computer science University Of Calcutta, West Bengal, India, Vivekananda Mission Mahavidyalaya, Vidyasagar University for supporting the work. The authors would also like to thank the reviewers for the comments which are very helpful and constructive.

REFERENCES

1. Von Solms, Rossouw, and Johan Van Niekerk. "From information security to cyber security." *computers & security*38 (2013): 97-102.
2. Shannon, Claude E. "Communication theory of secrecy systems." *Bell system technical journal* 28, no. 4 (1949): 656-715.
3. Sensarma, D., and S. Sen Sarma. "A Unified Framework for Security and Storage of Information A Unified Framework for Security and Storage of Information." *International Journal of Advance Engineering and Research Development* 2, no. 1 (2015).
4. ISO/IEC. ISO/IEC TR 13335-1:2004 information technology security techniques management of information and communications technology security part 1: concepts and models for information and communications technology security management. ISO/IEC, JTC 1, SC27, WG 1 2004.
5. International Telecommunications Union (ITU). ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity 2008.
6. Whitman, Michael E., and Herbert J. Mattord. "Principles of information security. Cengage Learning." *receives US patent for personal identification device.(2005). Wireless News*(2011): 1-1.
7. Kahate, Atul. *Cryptography and network security*. Tata McGraw-Hill Education, 2013.
8. Lewin, Kurt. *Principles of topological psychology*. Read Books Ltd, 2013.
9. Knuth, Donald E. *The Art of Computer Programming, Volume 4, Fascicle 6: Satisfiability*. Addison-Wesley Professional, 2015.
10. Al Etaiwi, Wael Mahmoud. "Encryption algorithm using graph theory." *Journal of Scientific Research & Reports* 3, no. 19 (2014): 2519-2527.
11. Yamuna, M., A. Sankar, Siddarth Ravichandran, and V. Harish. "Encryption of a Binary String using music notes and graph theory." *International Journal of Engineering and Technology* 5, no. 3 (2013): 2920-2925.
12. Yamuna M, Meenal Gogia, Ashish Sikka, Md. Jazib Hayat Khan. “Encryption using graph theory and linear algebra.” *International Journal of Computer Application*. ISSN:2250-1797; 2012.
13. Amudha A, Charles Sagayaraj A.C., Shantha Sheela A.C. “An Application of Graph Theory in Cryptography”, *International Journal of Pure and Applied Mathematics*, Vol.119 (13), 375-383, 2018.
14. Sensarma, Debajit, and Samar Sen Sarma. "Gmdes: a graph based modified data encryption standard algorithm with enhanced seurity." *Int J Res Eng Technol* 3, no. 3 (2014): 653-660.
15. Klima, Richard E., and Neil P. Sigmon. *Cryptology: classical and modern with maplets*. Chapman and Hall/CRC, 2012.
16. Ustimenko, Vasyl. "On graph-based cryptography and symbolic computations." *Serdica Journal of Computing* 1, no. 2 (2007): 131-156.
17. Akl, Selim G. "The graph is the message: design and analysis of an unconventional cryptographic function." *From Parallel to Emergent Computing, Adamatzky, A. et al., Eds., Taylor & Francis, CRC Press, Boca Raton, Florida* (2019).
18. Paszkiewicz, Andrzej, Anna Górska, Karol Górski, Zbigniew Kotulski, Kamil Kulesza, and Janusz Szczepański. "Proposals of graph based ciphers, theory and implementations." In *Proceedings of the Regional Conference on Military Communication and Information Systems. CIS Solutions for an Enlarged NATO, RCMIS*. 2001.
19. Lu, Steve, Daniel Manchala, and Rafail Ostrovsky. "Visual cryptography on graphs." *Journal of combinatorial optimization*21, no. 1 (2011): 47-66.
20. McEliece, Robert J. "A public-key cryptosystem based on algebraic." *Coding Thv* 4244 (1978): 114-116.
21. Sun, Hung-Min. "Cryptanalysis of a public-key cryptosystem based on generalized inverses of matrices." *IEEE communications letters* 5, no. 2 (2001): 61-63.
22. Hecker, David, and Stephen Andrilli. *Linear Methods: A General Education Course*. Chapman and Hall/CRC, 2018.
23. Eves, Howard Whitley. *Elementary matrix theory*. Courier Corporation, 1980.
24. Sensarma, Debajit, and Samar Sen Sarma. "Data Hiding using Graphical Code based Steganography Technique." *arXiv preprint arXiv:1509.08743* (2015).
25. Deo, Narsingh. "Graph theory with applications to engineering and computer science: PHI Learning Pvt." *Ltd India* (2004).
26. Hakimi, S., and J. Bredeson. "Graph theoretic error-correcting codes." *IEEE Transactions on Information Theory* 14, no. 4 (1968): 584-591.
27. Jungnickel, Dieter, and Scott A. Vanstone. "Graphical codes revisited." *IEEE Transactions on Information Theory* 43, no. 1 (1997): 136-146.
28. Jungnickel, Dieter, and D. Jungnickel. *Graphs, networks and algorithms*. Berlin: Springer, 2005.