AIP Conference Proceedings

A hybrid combination of symmetric and asymmetric encryption technique with graph labeling

Cite as: AIP Conference Proceedings **2516**, 120002 (2022); https://doi.org/10.1063/5.0108506
Published Online: 30 November 2022

V. N. Jaya Shruthy and V. Maheswari


View Online


Export Citation

ARTICLES YOU MAY BE INTERESTED IN

Fake news detection in social media using recurrent neural network
AIP Conference Proceedings **2516**, 100002 (2022); https://doi.org/10.1063/5.0108649

Integrating feature selection and mislaid data in thyroid classification using data mining algorithms
AIP Conference Proceedings **2516**, 100001 (2022); https://doi.org/10.1063/5.0109424

Security attacks on wireless sensor networks: Survey
AIP Conference Proceedings **2516**, 100005 (2022); https://doi.org/10.1063/5.0108553

AIP Publishing

© 2022 Author(s).

A Hybrid Combination of Symmetric and Asymmetric Encryption Technique with Graph Labeling

V. N. Jaya Shruthy[1, b)] and V. Maheswari[2, a)]

[1] *Research Scholar, Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies Chennai - 600117, India.*
[2]*Associate Professor, Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies Chennai - 600117, India.*
[a)] *Corresponding Author: maheswari.sbs@velsuniv.ac.in*
[b)]*jayashruthy12@gmail.com*

Abstract. Cryptography is the study of methodologies to promote secure communications by hiding or converting the original information to some unintelligible form. Graph Labeling is allocation of integers to edges and vertices of a graph following a set of conditions. Cryptography and graph theory are inextricably linked to each other since time immemorial. Here we implement cryptographic writing by combining the concepts of symmetric and asymmetric encryption techniques namely Pairwise Alternating Nested Caesar Cipher and RSA Algorithm with graph labeling. The former is an improved version of the popular symmetric encryption technique namely Caesar Cipher whereas the latter is an asymmetric cryptography algorithm widely used by modern computers to encrypt and decrypt messages. The plaintext undergoes hybrid encryption producing a Hybrid ciphertext which the sender passes to receiver as a Cryptographic writing comprising of Cipher Graph accompanied with a clue. We embrace Simply Sequential Additive labeling technique for ciphertext identification and the original plaintext is retrieved through corresponding decryption. The proposed methodology thus adopts the positive traits of both symmetric and asymmetric encryption ensuring double layer security of encrypted messages from adversaries, as knowledge of both Cryptography and Graph labeling is essential to proceed further.

KEYWORDS. Bistar, Pairwise Alternating Nested Caesar Cipher, RSA Algorithm, SSA labeling.
2010 Mathematical Subject Classification number: 05C78

INTRODUCTION

In our work we elaborate the encryption methodology of transporting secret messages with utmost care and security without the interference or disturbance from any adversary. To carry out this task we perform a hybrid design which is a blend of symmetric and asymmetric cryptography joining our hands together with Simply Sequentially Additive labeling technique. We term this type of hybrid as hetero hybrid whereas in our earlier work in [8] and [9] we have discussed homo hybrid, a combination of symmetric encryption methodology. In Symmetric key cryptography only a single key serves the purpose of both encryption and decryption whereas two different keys are employed in the case of asymmetric encryption. RSA Algorithm is deeply rooted in Number Theory concept and hence serves as the most efficient and secure algorithm till date. The plaintext from the sender undergoes encryption through hybrid combination generating a ciphertext which is disguised and presented to the receiver as a Cipher graph structure. From the Cipher graph the receiver perceives the hybrid text using Graph labeling technique and the ciphertext using trace keys whose corresponding decryption gives back the original plaintext. Certainly this hybrid methodology accompanied with SSA labeling technique ensures more safety in the transfer of secure communications in the current scenario.

LITERATURE REVIEW

All the graphs considered here are finite, simple and connected. J.A. Gallian in [1] provides an insight about various labeling techniques introduced. R.C. Read [2] highlights ideas on applications of Graph Theory

2nd International Conference on Mathematical Techniques and Applications
AIP Conf. Proc. 2516, 120002-1–120002-8; https://doi.org/10.1063/5.0108506
Published by AIP Publishing. 978-0-7354-4234-4/$30.00

associated with Cryptography. F. Harary [3] provides basic definitions and notations in Graph theory. Song Y. Yan [4] and Pawanveer Singh [5] details the role and importance of Number theory in Modern Cryptography. In [7] double encryption and decryption of secret messages using Enhanced Vigenere Cipher has been portrayed. In [6] we have discussed encryption using One-time Pad using Graph labeling. A great source of inspiration on hybrid encryption using graph labeling is derived from our work in [8]. Indeed our current work on combination of symmetric and asymmetric key cryptosystem is an extension of idea portrayed in it. K. Manimekalai, J. Baskar Babujee, K. Thirusangu [10] and D.W. Bonge and A.E. Barkauskas [11] discusses the simply sequentially additive labeling of trees and various graphs.

PRELIMINARIES

Definitions

Simply Sequentially Additive labeling

A k - Sequentially Additive labeling f of G (V, E) with vertex V and edge E is a bijection from V ∪ E to {k, k + 1, k + 2,.....…, k + |V ∪ E |-1} such that f (e) = f (u) + f (v) for u, v ∈ V. If k =1 then graph G (V, E) is said to be Simply Sequentially additive or 1- Sequentially additive abbreviated as SSA labeling

Bistar

A tree obtained by connecting the apex node of two copies of stars $K_{1,n}$ and $K_{1,m}$ with disjoint vertex sets is called a bistar graph denoted by $B_{m, n}$.

Cipher Graph

The Cipher text presented to the receiver as a graph structure called Cipher graph.

Cipher Clue

It is the key used for discovering the ciphertext sequence from the Cipher graph with the aid of graph labeling technique is called Cipher key and it is altered based on the trace key to be used.

Trace key

The keys used by the receiver for retrieving some data from the source key for easy decryption is called Trace Key for easy manipulation of plaintext from ciphertext.

PANC Cipher

A simple form of Substitution Cipher in which each plaintext letter is replaced by some letter by shifting to a certain number of positions along the alphabetical order is a Caesar Cipher. In [8] we have introduced Pairwise Alternating Nested Caesar Cipher abbreviated as PANC Cipher the message is split into pairs and Caesar Cipher is performed to the first word of each pair by shifting the letters forward and backward in an alternating fashion depending on the word length.

RSA Algorithm

RSA Algorithm is an asymmetric cryptography algorithm which uses two sets of keys viz a public key and a private key for secure transmission of information. It is an excellent and most widely adopted and celebrated Encryption algorithm as it enables movement of sensitive data over an insecure network base such as the internet where everyone can lay their hands upon. It was introduced by Ron Rivest, Adi Shamir and Leonard Adelman in

1978 and hence the nomenclature RSA Algorithm. The most striking feature of this algorithm is that it encrypts message without the need for exchanging secret keys. The computational difficulties in factorizing large integers that are product of two large prime numbers is practically very laborious or considered in-feasible due to heavy time consumption even with the advent of Supercomputers. The security of RSA Algorithm entirely confides on the above striking feature which makes it an expertise and pioneer among all other encryption algorithms.

Steps involved in RSA Algorithm

Step i. Select two large prime numbers p and q.
Step ii. Calculate m = p*q**.**
Step iii. Evaluate ϕ (m) = (p -1) (q -1).
Step iv. Choose an integer i, relatively prime to ϕ (m) with $1 \leq i \leq \phi$ (m) and the pair (m, i) serves as the public key.
Step v. The plaintext is converted into ciphertext by an integer P by using digit alphabet conversion table.
and the ciphertext C is obtained using $P^i \equiv C \pmod m$.
Step vi. Choose a secret recovery j corresponding to i satisfying the congruence relation
i. $j \equiv 1 \pmod{\phi(m)}$ where (m, j) acts as the private key.
Step vii. The plaintext is retrieved back from the Ciphertext using $C^j \equiv P \pmod m$.The last two steps are concerned with RSA decryption.

Hybrid Cryptographic Algorithm for encryption

The algorithm details the steps to be performed for encryption using hybrid combination. We deal with hetero hybrid and assume the parent encryption techniques to be Encryption technique I and Encryption technique II abbreviated as ET- I and ET - II and the resulting Hybrid Ciphertext as HC.
Step 1: Process the given Plaintext through ET - I. Here ET - I is our Symmetric Encryption technique namely PANC. The ciphertext obtained is Ciphertext - I.
Step 2: Process the Ciphertext – I obtained from ET - I through ET - II. Here ET - II is our asymmetric Encryption technique namely RSA Algorithm .The ciphertext obtained is Ciphertext - II.
Step 3: The Resulting hybrid ciphertext HC is obtained as a zig - zag combination of Ciphertext I elements $e_{i,k}$ and Ciphertext - II elements $d_{j,k}$ using the relation using the relation $e_{i,2n-1}\, d_{j,2n}$ where i = 1; j = 2 ; k = 1, 2,…..n recursively.
Step 4: Represent the resulting hybrid ciphertext HC as a Cipher graph with Cipher clue adopting the prescribed labeling to the receiver. Here we use SSA Labeling.
Step 5: The original cipher text is identified from hybrid ciphertext with the aid of trace key which in turn undergoes decryption yielding the required plaintext.

Plan of Work

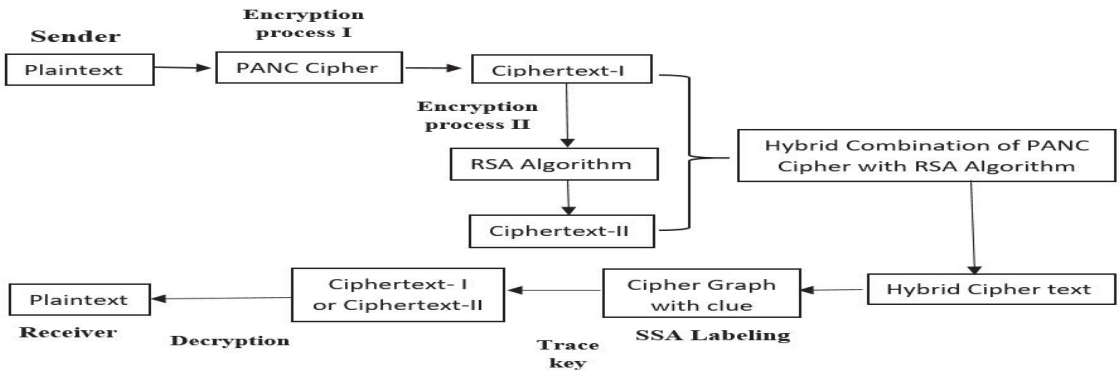

FIGURE 1. Plan of Work

Pre – Requisites of the Receiver

These are the keys handed over to the receiver well in advance
1. Cipher clue to perceive the Hybrid cipher text from the Cipher Graph.
2. Trace key to trace either of the ciphertext I or II from Hybrid ciphertext.
3. Decryption Key to decrypt ciphertext identified from hybrid text eventually yielding the required plaintext.
Further a knowledge of the implemented Graph labeling and Cryptography Technique is definitely required.

Numbering the alphabets

We convert the plaintext alphabets into double digits using Digit alphabet conversion table. We can also include numbers, signs and mathematical symbols as per the plaintext requirement. The numbering of alphabets can be done in any regular or random pattern suiting our needs and convenience.

TABLE 1. Digit Alphabet Conversion Table

Character	a	b	c	d	e	f	g	h	i	j	k	l	m
Digit Entry	26	01	25	02	24	03	23	04	22	05	21	06	20

n	o	p	q	r	s	t	u	v	w	x	y	z
07	19	08	18	09	17	10	16	11	15	12	14	13

ILLUSTRATION

Encryption Technique - I using PANC Cipher

Step 1: Let our plaintext I be the message: **stay in cave ten** and corresponding token (word) length is *4 2 4 3.*
We straightaway begin our PANC Encryption as we have detailed the steps involved in PANC Cipher Encryption in [8].

TABLE 2. PANC Cipher encryption

Pairs	I		II		III		IV
Paired statements	**stay in**		**in cave**		**cave ten**		**ten**
Token length	4	2	2	4	4	3	3
Token Considerations	Small		Large		Small		Large
Consideration value among the pair	2		4		3		3
Shift	Forward Shift +2		Backward Shift - 4		Forward Shift +3		Backward Shift - 3
Plaintext	**stay**		**in**		**cave**		**ten**
PANC Ciphertext	**uvca**		**ej**		**fdyh**		**qbk**

At the end of ET - I the **Cipher text - I** in blocks are: **uvca ej fdyh qbk** and the corresponding digit entry from "Table 1" is as follows **16 11 25 26 24 05 03 02 14 04 18 01 21.** As this method alternates its choice of token selection thereby shifting the letters in both the direction it definitely puzzles any eavesdropper.

Encryption Technique - II (ET - II) using RSA Algorithm

Step 2: Our Ciphertext - I from Encryption Technique - I (ET - I) using PANC Cipher becomes our Plaintext - II for Encryption Technique - II (ET - II) using RSA Algorithm.
For **Plaintext II**: **uvca ej fdyh qbk** corresponding digits are **16 11 25 26 24 05 03 02 14 04 18 01 21.**Now we perform RSA Algorithm as follows.
Step i: Select two prime numbers of our choice as **p = 13 and q = 2**. For illustration purpose and to facilitate the numbering of alphabets this selection is valid, but in real time execution each p and q should comprise of at least 100 digits.
Step ii: Next find **m = p. q** which is 13. 2 = **26.**
Step iii: Find **ϕ (m) = (p -1) (q -1) = 12. 1= 12.**
Step iv: Choose an integer **i = 5** such that *i* is co - prime with **ϕ (m)** (i.e., 5 is co - prime with 12).We break the plaintext digit and encrypt each block separately.
Step v: Each plaintext digit block is converted into Ciphertext using the relation $\mathbf{P^{i} \equiv C \pmod{m}}$ where P = Plaintext, C = Ciphertext, i = 3 and m = 493.

$(16)^5 \equiv C \pmod{26}$ which gives C = 22 $(11)^5 \equiv C \pmod{26} \rightarrow C = 07$
$(25)^5 \equiv C \pmod{26} \rightarrow C = 25$ $(26)^5 \equiv C \pmod{26} \rightarrow C = 0$
$(24)^5 \equiv C \pmod{26} \rightarrow C = 20$ $(05)^5 \equiv C \pmod{26} \rightarrow C = 05$
$(3)^5 \equiv C \pmod{26} \rightarrow C = 09$ $(02)^5 \equiv C \pmod{26} \rightarrow C = 06$
$(14)^5 \equiv C \pmod{26} \rightarrow C = 14$ $(04)^5 \equiv C \pmod{26} \rightarrow C = 10$
$(18)^5 \equiv C \pmod{26} \rightarrow C = 18$ $(01)^5 \equiv C \pmod{26} \rightarrow C = 01$
$(21)^5 \equiv C \pmod{26} \rightarrow C = 21$

The **ciphertext II** is obtained as **22 07 25 0 20 05 09 06 14 10 18 01 21**.

Designing the Hybrid Ciphertext

Step 3: The resulting Hybrid Ciphertext is obtained as a zig - zag combination of Ciphertext - I and Ciphertext-II using the relation $e_{i,2n-1}\, d_{j,2n}$ where i = 1; j = 2 ; n = 1, 2,…..13 recursively as depicted in "Table 3".

TABLE 3. Hybrid Ciphertext Formation

PANC Cipher ($e_{i,k}$)	16	11	25	26	24	05	03	02	14	04	18	01	02
RSA Algorithm ($d_{j,k}$)	22	07	25	0	20	05	09	06	14	10	18	01	21
Hybrid Ciphertext	16	07	25	0	24	05	03	06	14	10	18	01	02

The **Hybrid Ciphertext: 16 07 25 0 24 05 03 06 14 10 18 01 21** obtained is sent to the receiver as Cipher Graph structure whose edge labels are to be determined.

Message to the Receiver - Cipher graph

Step 4: As in [9], the receiver identifies the edge labels by applying SSA labeling and determines the Hybrid Ciphertext sequence by means of Cipher clue. The original Ciphertext I or II is discovered using Trace key whose corresponding decryption gets back our plaintext.

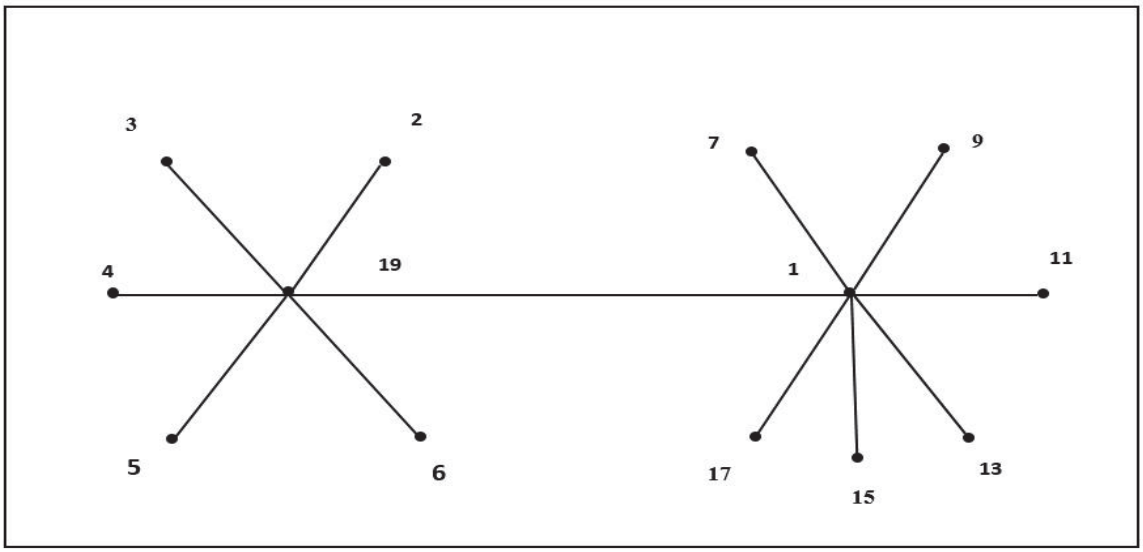

FIGURE 2. Cipher Graph to the receiver – Bistar B $_{5, 6}$

Requirements Handed to the receiver is Clue with Trace Key

We consider a bistar graph $B_{5, 6}$ for this purpose as shown in "Fig.2"

Cipher Clue: SSAL in the order [($e_{2, 5}$), ($v_{2, 1}$), ($e_{1, 5}$), v_2 -1)][($e_{1, 4}$), ($v_{1, 4}$)][($v_{1, 2}$), ($v_{1, 5}$), ($e_{2, 4}$), ($e_{2, 2}$)][($e_{2, 6}$) , v_2 , ($e_{1, 1}$)] where $e_{1, i}$ and $v_{1, i}$ denotes the i th edge labels and vertices of first star $k_{1, m}$ with $i \leq m$ and $e_{2, j}$ and $v_{2,j}$ denotes the j th edge labels of second star $k_{1,n}$ respectively with $j \leq n$ in the increasing order of disjoint vertices, v_1 and v_2 denotes the vertices in common connecting $k_{1,m}$ and $k_{1,n}$ .Also the square brackets indicates the necessary space required for PANC decryption to determine the token length and the need is justified as we combine two varied concepts together into one. The Cipher clue is altered based on the trace key to be used.

Using the clue *SSAL* which signifies Simply Sequentially Additive labeling we finds the edge labels using f (e) = f (u) + f (v) as depicted in "Fig. 3".

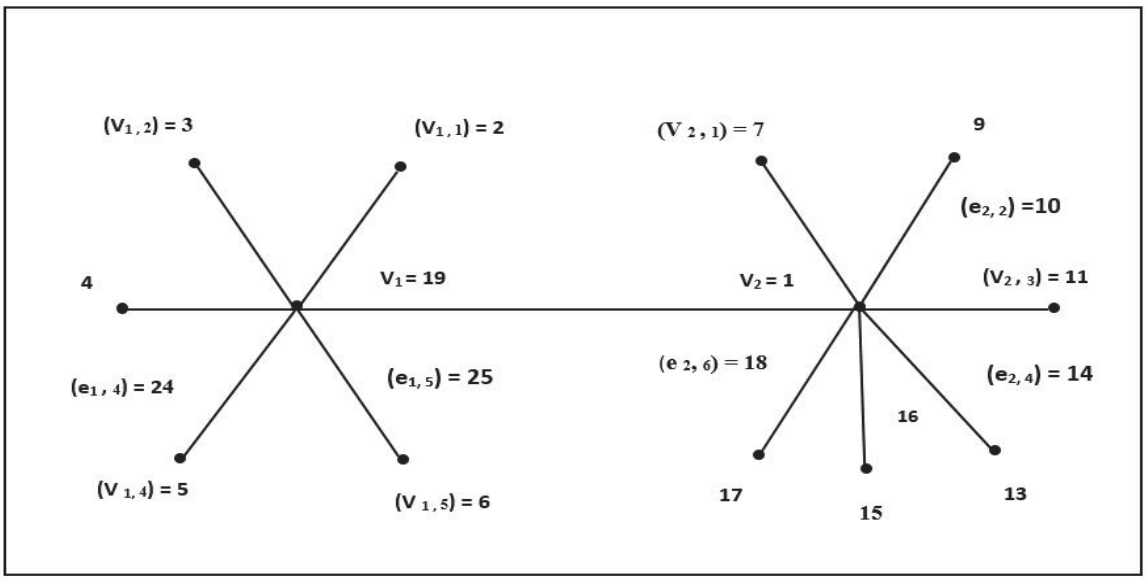

FIGURE 3. Edge Labels identified using Cipher Clue – Bistar B $_{5, 6}$

Our Cipher Graph adheres to SSA Labeling and not all the edge labels of the Cipher Graph are utilized but we only need to identify the specified labels in the given order thereby creating a certain confusion to any adversary other than the intended person. Using SSAL we identify the value for the edge labels as **16 07 25 0 - 24 05 - 03 06 14 10 - 18 01 21**. Here ($e_{2,5}$) denotes the 5 th edge label of second star $K_{2,6}$ which by SSAL is 15 + 1= 16,
($e_{1,5}$) denotes the 5 th edge label of first star $K_{1,5}$ which by SSAL is 19 + 6 = 25,
v_2 -1 denotes v_2 = 1 - 1= 0, ($v_{2,1}$) denotes the 1st vertex of second star $K_{2,6}$ which by SSAL is 7 and proceeding likewise we get the other edge labels.

Trace Key I:

Step 5: The trace keys is a key set provided to the receiver which traces certain data from the source - hybrid Ciphertext and retains the remaining data. It actually works like a trace paper and plays a vital role in hybrid combination process where two parent encryption techniques are combined in some random pattern. Trace key I traces Ciphertext I from Source (Hybrid ciphertext) whereas Trace key II traces Ciphertext II from Source.

TABLE 4. Ciphertext traced using Trace Key I

Hybrid Ciphertext HC	16	07	25	0	24	05	03	06	14	10	18	01	21
Trace key I	-	11	-	26	-	05	-	02	-	04	-	-	-
Ciphertext I	16	11	25	26	24	05	03	02	14	04	18	01	21

Here "-" indicates data traced from source and remaining values are reflected as it is [9].Using **Trace key I: - 11 - 26 - 05 - 02 - 04 - - -** technique as in [9] the PANC decryption yields the ciphertext I as 16 11 25 26 24 05 03 02 14 04 18 01 21 based on cipher clue. For more detailed explanation of trace key technique we refer [9]. As trace key and Cipher clue are interrelated the Ciphertext I now assumes the form **16 11 25 26 - 24 05 - 03 02 14 04 - 18 01 21** indicating the token length. The trace Key reduces the burden of long decryption process.
We can also make use of **Trace key II: 22 - 25 - 20 - 9 - 14 - 18 - 21** and corresponding decryption using RSA Algorithm decryption using $\mathbf{C^j \equiv P \pmod m}$ yields the required plaintext making use of step vi and vii.

Decryption of Ciphertext using PANC Cipher

TABLE 5. PANC Cipher decryption

Pairs	I	II	III	IV
Paired statements	**uvca ej**	**ej fdyh**	**fdyh qbk**	**qbk**
Token length	4 | 2	2 | 4	4 | 3	3
Token Considerations	Small	Large	Small	Large
Consideration value among the pair	2	4	3	3
Reverse Shift	Backward Shift -2	Forward Shift + 4	Backward Shift -3	Forward Shift +3
Plaintext	**uvca**	**ej**	**fdyh**	**qbk**
PANC Ciphertext	**stay**	**in**	**cave**	**ten**

We perform decryption of Ciphertext I: **16 11 25 26 - 24 05- 03 02 14 04 - 18 01 21** by converting the digits back to alphabets from "Table 1": **uvca ej fdyh qbk** and get our plaintext: **stay in cave ten.**

CONCLUSION

Thus a hybrid encryption methodology using PANC Cipher and RSA Algorithm along with graph labeling technique in two different ways has been presented here. Further studies can be carried on this versatile schema of encryption detailed above using other labeling techniques which certainly ensures confidentiality, non - repudiation, reliable and secure transfer of data which is the need of the hour.

REFERENCES

1. J. A. Gallian, *E - JC*, 18 (2016), #DS6.
2. R.C. Read, *Computer Math Application*, 34, (1997) ,pp.121- 127.
3. F. Harary, Graph Theory, *Addison - Wesley, Reading*, Massachusetts (1969).
4. Song Y. Yan, *Computational Number theory and Modern Cryptography*, Wiley, (2012).
5. Pawanveer Singh, Amanpreet Singh, Shola Jambs, *IJARSE*,6, Issue No. 01, Jan (2017).
6. V.N. Jaya Shruthy and V. Maheswari, *IJRTE*, 8, (2019), pp.76 - 81.
7. V.N. Jaya Shruthy and V. Maheswari, *JPCS*, 1362 (2019) 012023,(2019), pp, 1-7.
8. V.N. Jaya Shruthy and V. Maheswari, *TWMS J. of Appl. and Eng. Math*., 11, (2021),pp.154 -163.
9. K. Manimekalai, J.Baskar Babujee, K. Thirusangu, *Applied Mathematical Sciences*, 6, 131,(2012),6501-6514.
10. D.W.Bonge, A.E Barkauskas, P.J. Slater, Discrete Mathematics, 44, *North-Holland Publishing* (1983), pp.235 - 241.