Iranian Journal of Fuzzy Systems

Volume 23, Number 5, (2026), pp. 67-86

Original paper

University of Sistan and Baluchestan

Polynomial-driven fuzzy network cryptosystem based on multi-prime RSA encryption

A. Meenakshi [1], S. Dhanushiya [2], H. Rashmanlou [3], B. Pourhassan [4] and F. Mofidnakhaei [5]

[1] *Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi, Chennai–600062, Tamil Nadu, India*

[2] *Department of Mathematics, Rajalakshmi Institute of Technology, Chennai–600124, Tamil Nadu, India*

[3] *School of Physics, Damghan University, Damghan, Iran*

[3] *Canadian Quantum Research Center, 106–460 Doyle Ave, Kelowna, British Columbia V1Y 0C2, Canada*

[4] *School of Physics, Damghan University, P. O. Box 3671641167, Damghan, Iran*

[4] *Center for Theoretical Physics, Khazar University, 41 Mehseti Street, AZ1096 Baku, Azerbaijan*

[5] *Department of Physics, Sar.C., Islamic Azad University, Sari, Iran*

drameenakshi@veltech.edu.in, sdhanushiya488@gmail.com, h.rashmanlou@du.ac.ir, b.pourhassan@du.ac.ir, farshid.mofidnakhaei@gmail.com

Abstract

In the modern digital era, the level of security is much dependent on the factors of reliability and robustness. Domination theory provides a powerful mathematical tool for the purpose of controlling and monitoring access among nodes in a fuzzy network. Network models in the form of fuzzy graphs have become important in recent times in view of providing significant development related to lightweight cryptographic systems as they can handle issues related to uncertainty and partial membership effectively. Polynomials are fundamental in cryptography because they are the basis of many algebraic systems that are used in encryption and, most importantly, decryption techniques. Polynomials are employed explicitly or implicitly in all cryptosystems, creating a solid platform upon which communication occurs. This study aims to develop a fuzzy graph network, describing an encrypted version of secret information. Mathematical modeling of the fuzzy graph network is derived based on a multi-prime RSA system. Considering the given text, it creates a polynomial as part of the main key of a cryptosystem. Algorithms for encryption and decryption are developed and explained to show the effectiveness of the proposed method. Also, the security level of the developed fuzzy graph network is improved with the incorporation of the domination parameters and the polynomial transformations.

Keywords: Fuzzy graph, domination, cryptography, polynomial, security.

1 Introduction

Fuzzy Graph Theory is an extension of conventional graph theory, and it accommodates uncertainties by assigning numerical values to graph edges and vertices. Fuzzy graph theory has its foundation in definitions, significant numbers of hybrid versions of fuzzy graph theory, and applications in diverse areas of communication networks, decision-making systems, image processing techniques, etc.

In a fuzzy graph, vertices as well as edges have corresponding membership degrees, which describe incomplete connections between objects. Key concepts in a fuzzy graph, such as degree, order, size, path strength, as well as connectivity, have corresponding analogues in fuzzy graphs as an extension of corresponding classical concepts. A fuzzy graph can be rigorously defined as an ordered pair of a fuzzy set of vertices and a fuzzy relation over this fuzzy set, whereas level graphs can be used to obtain corresponding crisp graphs. Domination is an important structural parameter that regulates the optimal control or coverage of vertices within a given graph network. Efficient domination

Corresponding Author: A. Meenakshi

Received: February 2026; Revised: July 2026; Accepted: July 2026.

https://doi.org/10.22111/ijfs.2026.54859.9721

refers to the determination of a minimum dominating set, that is, the smallest number of vertices required to dominate (or cover) all other vertices in the prescribed graph network.

The study of fuzzy graph theory is a generalization of the study of graphs. Graph theory is an expansion of fuzzy sets. The fuzzy graph theory has various foundations, extensions, and applications. The fuzzy graph theory is used to describe uncertain relationships between nodes and arcs. The most common definitions of fuzzy graph formalism describe a fuzzy graph as a pair. The latter two components of the pair represent a fuzzy subset of the nodes and a fuzzy relation on the subset, respectively. The results obtained using the level set of a fuzzy graph have a direct effect on the traditional treatment of graph theory. A fuzzy network enables partial trust, partial connectivity, and uncertain relationships between nodes to be modeled. This is important in cryptography because trust between the nodes in a communication process is not absolute the reliability of the communication channel may be variable, and the probability of an attack is not binary (safe or dangerous) but gradual. Therefore, fuzzy modeling enhances the representation of security. Domination is a parameter used to determine the maximum utilization of nodes in a specified graph network. Efficient domination is defined as the minimum number of nodes required to dominate a specified graph network.

The phenomenon of uncertainty in real-world scenarios using fuzzy set theory has been proposed by Zadeh in 1965 [25]. It results in the membership values of the vertices and their edges lying in $[0, 1]$. The concept of fuzzy graphs was proposed by Rosen field in 1975 [21]. The concept of dominating sets in graphs was introduced by Ore in 1960[18]. The concept of total domination in graphs was formally proposed by Cockayne et al. [9] in 1980. Biggs studied efficiently the structure of perfect codes, which resulted in initiating efficient domination by Bange et al. in 1988 [4]. Kulli and Patwari [11] studied the concept of total efficient domination in graphs. Graph network is one of the types of graph neural network, which is an entity or system of representation of structural relationships between entities, often depicted as boxes drawn as nodes, and connections as edges or lines. Baagyere et al. proposed a multi-layered concept of data encryption/decryption using a genetic algorithm in combination with residual numbers [3]. Yu G., et al proposed how to make subgraphs using expanders.

Cryptography is the science of protecting information by converting it into a form that unauthorized users cannot understand. It guarantees that communication is confidential, authentic, and tamper-proof. Chen (2009) and Alghafis etal. (2020), suggested a viable approach for the encryption of images [1, 2, 6]. Graph neural network for cryptographic analysis is done by Wang et al. (2023) [23] using graph-based deep learning. The author discussed the creation of traffic graphs in his research. Mahardika (2024) and Triayudi [13] suggested comparative analysis for the performance of the encryption and decryption of cryptography. Kychak et al. (2025) suggested the joint key permutation for the significant dimension of the cryptographic protocol [12].

The security of messages in contemporary cryptography has been significantly maintained by developing integrations of adaptive and uncertainty-oriented security systems and combinatorial and structural methods. The deniable encryption technique was proposed by Chu et al. in [8]. This algorithm was adopted in modulation-based storage systems. The security of the messages was further enhanced in this approach. Wu and Lu [24] proposed a secure framework of hypergraph structure for multilayer and multi-domain smart intelligent optical networks, addressing the security issues of these complex networks. The secret key generation mechanism was explored by Zhou and Chan [26] in the context of minimally connected fuzzy hypergraphical sources, ascertaining the security of uncertain network conditions. Cheng et al. in [7] further explored the hypergraph-based abstract models in duplicated storage systems. Meenakshi et al. [16] explored the studies on fuzzy hypergraph-based framework for secure encryption and decryption of sensitive messages. Shariatzadeh et al. [22] studied the adaptive image encryption scheme by fuzzy models. Despite these significant contributions, the integration of fuzzy logic with network architecture remains a relatively underexplored direction in cryptographic research. In particular, the transformation of secret information into structured fuzzy graph networks has not been systematically developed within existing cryptographic frameworks.

Data communication security has been gaining a lot of interest in the past few years. To improve the encryption strength and resistance against cryptanalytic attacks, Belazi et al. in 2017 [5] proposed an efficient cryptosystem that is based on substitution–permutation networks and S-box design. In 2023, Kaushik et al. [10] provided a comprehensive overview of the different encryption and decryption methods and their importance in securing sensitive information. Data encryption and decryption are two critical topics in cryptography, which Masud et al. [14] addressed in 2022 with a new cryptographic approach for securing data and enhancing its confidentiality. In 2023, Meenakshi et al. [15] studied graph networks using the concept of total magic labeling and showed its applications in the efficient communication structure. Pius and Kirubaharan [19] proposed the use of fuzzy graph theory in cryptography in 2021 to improve data privacy and secure information transmission through fuzzy relationships. In 2024, Razaq et al. [20] introduced a fuzzy logic-driven substitution box to enhance security in telemedicine applications for medical image encryption. In addition, Mehta and Rana [17] investigated the safest number of primes in the modulus of the RSA and suggested an approximated generalized multi-moduli RSA to enhance cryptographic security and computational efficiency in 2025. The present work reflects the increasing blending of graph theoretic methods, fuzzy systems and advanced cryptographic

methods in the development of secure and efficient communication networks.

Based on the identified gap in literature review as mentioned in this section, this study aims to develop a novel approach to cryptography methodology in which the output of the encryption process is represented by a fuzzy graph network structure. In the proposed approach to cryptography methodology, a systematic approach to constructing a polynomial using the plaintext (secret message) is developed, and this polynomial constructed from the multi-prime RSA approach in cryptography. The plaintext is algebraically encoded in polynomial form in addition, the output of the encryption process in polynomial form is encoded within a fuzzy graph network. The polynomial modeling provides an algebraic layer of transformation, the fuzzy graphs bring uncertainty in the form of membership values, and the domination theory helps to determine the critical control nodes in the network. The integration generates several interconnected layers, which further add complexity in unauthorized reconstruction, thus strengthening the security of the proposed communication framework.

By incorporating polynomial modeling, fuzzy graph architecture, and multi-prime RSA algorithms together into the proposed system, it can improve structural security, resistance to cryptanalysis, and computational efficiency. This overall theoretical model can be used as a strong mathematical solution for secure communication. The research gap of this work is shown in the following table. The novelty of this research focuses on (i) Plaintext to polynomial key generation: The original text is converted to a polynomial, which serves as a fundamental key component, introducing a new algebraic encoding scheme. (ii) Integration of Domination as a Security Parameter: Instead of domination, as a parameter of graphs, it is utilized as an instrument of security management, regulating the level of influence as well as coverage. (iii)Hybridization with Multi-prime RSA: The system incorporates fuzzy graph modeling along with multi-prime RSA, enhancing its computational efficiency. (iv) Structural and Algebraic Security Combination: The proposed framework includes algebraic hardness (Multi-prime RSA-based), structural complexity (fuzzy network topology) and control Optimization (Domination Theory).

Section 1 deals with the introduction, preliminaries, motivation and novelty of the research being proposed. Section 2 explores the main framework of the proposed crypto model. In Section 3, the process of encryption and decryption is discussed. Section 4 presents an illustrative example to facilitate a better understanding of the proposed methodology. The flowchart of the algorithm is presented in Section 5. Finally, the paper concludes along with the possible directions for future research. The following Table 2 gives the abbreviations of the symbols used in this research.

2 Main framework of the research

Let the numerical plain text be P_{Num} be " $a_{11}a_{12}a_{13}\ldots a_{1r_1}/\ a_{21}a_{22}a_{23}\ldots a_{2r_2}/\ a_{31}a_{32}a_{33}\ldots a_{3r_3}/\ \ldots/a_{k1}a_{k2}a_{k3}\ldots a_{1r_k}$".

The ciphertext transformed into a polynomial form is to give an algebraic structure which can be readily combined with the proposed fuzzy graph network. The direct numerical ciphertext cannot be modeled using the graph-based framework used here. The polynomial degree is based on how many partitions of the ciphertext are used in encryption. The higher the polynomial degree, the more complex the representation and reconstruction and the more secure the cryptographic security, but the security is not guaranteed solely by the polynomial degree. While the primary security is based on the multi-prime RSA system, the polynomial transformation provides an extra obfuscation and network-modeling layer.

Let $P_{Num_1} = a_{11}a_{12}a_{13}\ldots a_{1r_1}, P_{Num_2} = a_{21}a_{22}a_{23}\ldots a_{2r_2}, P_{Num_3} = a_{31}a_{32}a_{33}\ldots a_{3r_3}, \ldots, P_{Num_k} = a_{k1}a_{k2}a_{k3}\ldots a_{1r_k}$. Frame the first fuzzy sub-network F_{SN_1}, from $a_{11}a_{12}a_{13}\ldots a_{1r_1}$. The corresponding plain text polynomial is $P_{Poly_1}(x) = a_{11} + \ a_{12} * \ x + \ a_{13} \ * \ x^2 + \cdots + a_{1r_1} * x^{(r_1-1)}$.

Using the Multi-prime RSA algorithm, generate the public key $PU_{\text{key}}(e, N)$ and the private key $PR_{\text{key}}(d, N)$. Let the prime numbers be $P_1 = N_1$, $P_2 = N_2$, $P_3 = N_3$, ..., $P_k = N_k$. Then, $N = P_1 \times P_2 \times P_3 \times \cdots \times P_k$. Euler's totient function is given by $\varphi(N) = (P_1 - 1)(P_2 - 1)\cdots(P_k - 1)$. Choose an integer e such that $\gcd(e, \varphi(N)) = 1$. Next, determine d satisfying $ed \equiv 1 \pmod{\varphi(N)}$. Finally, the public and private keys are obtained as

$$PU_{\text{key}} = (e, N), \qquad PR_{\text{key}} = (d, N).$$

From $a_{21}a_{22}a_{23}\ldots a_{2r_2}$, frame F_{SN_2}. Corresponding plain text polynomial be $P_{Poly_2}(x) = a_{21} + \ a_{22} * \ x + \ a_{23} \ * \ x^2 + \cdots + a_{2r_2} * x^{(r_2-1)}$. From $a_{31}a_{32}a_{33}\ldots a_{3r_3}$ frame F_{SN_3}. Corresponding plain text polynomial is $P_{Poly_3}(x) = a_{31} + \ a_{32} * \ x + \ a_{33} \ * \ x^2 + \cdots + a_{3r_3} * x^{(r_3-1)}$. Proceeding, from $a_{k1}a_{k2}a_{k3}\ldots a_{1r_k}$ frame F_{SN_k}. Corresponding plain text polynomial be $P_{Poly_k}(x) = a_{k1} + \ a_{k2} * \ x + \ a_{k3} \ * \ x^2 + \cdots + a_{1r_k} * x^{(r_1-1)}$.

The $P_{Poly_1}(x) = \sum_{i=1}^{r_1} a_{1i} * \ x^{(i-1)}$ is converted to encrypted polynomial $En(P_1(x)) = \sum_{i=1}^{r_1} ({a_{1i}}^e \ mod \ N) \ * \ x^{(i-1)}$ using RSA. $En(P_1(x)) = \sum_{i=1}^{r_1} ({a_{1i}}^e \ mod \ N) \ * \ x^{(i-1)} = \sum_{i=1}^{r_1} b_{1i} \ * \ x^{(i-1)}$, where $({a_{1i}}^e \ mod \ N) = \ b_{1i}, \ i = 1 \ to \ r_1$. Using normalization, convert the coefficient of $x^{(i-1)}$ into a fuzzy number by (Coefficient of $x^{(i-1)}$)/10000. Choose the value of $x, \ 1 \le x \le 3$, let the value be $x = 1, \ 2$ or 3 throughout $x^{(i-1)}$. $b_{1r_1} \ * \ x^{(r_1-1)} = \left(\frac{b1r_1}{10000}\right) * \ 2^{(r_1-1)} = \ n_{2_{r1}}$,

Table 1: Research gap

Factor	Pius (2021) & Kirubakaran [15]	Masud et al. (2022) [10]	Meenakshi et al.(2023) [12]	Kaushik et al. (2023) [9]	Razaq et al. (2024) [16]	Proposed Work
Research Domain	Fuzzy Graph Cryptography	General Cryptography	Graph Network Optimization	Encryption Review	Image Encryption	Multilayer Mathematical Cryptography
Type of Study	Applied Research	Conference Proposal	Mathematical Modeling	Survey Paper	Applied Encryption	Theoretical Applied Hybrid Model
Fuzzy Logic Usage	Structural (Fuzzy Graph)	Not Used	Not Used	Not Used	S-box Design	Structural Security Layer
Graph Theory Usage	Yes	No	Yes	No	No	Yes (Domination-Based Control)
Efficient Domination Concept	No	No	No	No	No	Yes
RSA Integration	No	No	No	No	No	Yes (Multiprime RSA)
Polynomial Framework	No	Limited	No	No	No	Algebraic Mapping Layer
Applications	Data Privacy	General Data Security	Network Efficiency	Literature Survey	Telemedicine Images	Secure Multilayer Data Transmission
Security Architecture	Single-layer	Single-layer	Non-cryptographic	Descriptive	Single-layer	Multilayer Architecture
Level of Mathematical Integration	Moderate	Basic	Moderate	Low	Moderate	High (Number Theory, Fuzzy logic, Graph Theory)

$b_{12}(r_1-1) * x^{(r_1-2)} = \left(\frac{b_{1r_1}}{10000}\right) * 2^{(r_1-1)} = n_1(r_1-1)$ (here the value of x is 2), Proceeding this, $b_{12} * x^1 = \left(\frac{b_{12}}{10000}\right) * 3 = n_{12}$, (here the value of x is 3), and $b_{11} * x^0 = \left(\frac{b_{11}}{10000}\right) = n_{11}$. Each $n_{1i},\ i = 1$ to r_1 as $V_{mem.v}$ of F_{SN_1}.

Construct the F_{SN_1} from P_{Num_1}. Let the vertices of F_{SN_1} be o_1 as the middle vertex and its neighbors are $f_{1_i},\ i = 1$ to r_1. The $V_{mem.v}(f_{1_i}) = n_{1i},\ i = 1$ to r_1 respectively and let $V_{mem.v}(o_1) = o_1$. $\mathcal{E}_{mem}v(o_1 f_{1_i}) = \min(o_1, n_{1i})$, $i = 1$ to r_1, which is shown in Figure 1. The first subnetwork, F_{SN_1} illustrates the initial fuzzy graph structure used in the proposed encryption framework for secure information representation. The $P_{Poly_2}(x) = \sum_{i=1}^{r_1} a_{2i} * x^{(i-1)}$ is converted to encrypted polynomial $En(P_2(x)) = \sum_{i=1}^{r_2} ({a_{2i}}^e \ mod\ N) * x^{(i-1)}$ using RSA.

$$En(P_2(x)) = \sum_{i=1}^{r_2} ({a_{2i}}^e \ modN) * x^{(i-1)} = \sum_{i=1}^{r_2} b_{2i} * x,$$

where $({a_{2i}}^e \ mod\ N) = b_{2i},\ i = 1$ to r_2. Choose the value of $x,\ 1 \le x \le 3$, let the value be $x = 1$ or 2 or 3 throughout $x^{(i-1)}$. $b_{2_{r2}} * x^{(r_2-1)} = \left(\frac{b_{2r_2}}{10000}\right) * 2^{(r_2-1)} = n_{2_{r2}}$, $b_2(r_2-1) * x^{(r_2-2)} = \left(\frac{b_{2r_3}}{10000}\right) * 2^{(r_2-1)} = n_2(r_2-1)$, Proceeding

Table 2: Abbreviations of the symbols used

Symbols	Abbreviation
P_{Num}	Numerical Plaintext
$PU_{key}(e,N)$	Public key
$PR_{key}(d,N)$	Private key
GCD	Greatest Common divisor
$P_{Poly}(x)$	Plaintext polynomial in x
F_{SN}	Fuzzy sub network
$En(P(x))$	Encrypted polynomial in x
$V_{mem.v}$	Vertex membership value
$E_{mem.v}$	Edge membership value
F_{GN}	Fuzzy Graph Network
$F_{GN_{min}}$	Fuzzy Graph Network with minimum number of edges
$F_{GN_{Avg}}$	Fuzzy Graph Network with average number of edges
$F_{GN_{max}}$	Fuzzy Graph Network with maximum number of edges
L	Illustration

this, $b_{22} * x^1 = \left(\frac{b_{22}}{10000}\right) * 3 = n_{22}$, $b_{21} * x^0 = \left(\frac{b21}{10000}\right) = n_{21}$. Each $n_{2i},\ i = 1\ to\ r_2$ as the vertex membership values ($V_{mem.v}$) of F_{SN_2}.

Construct F_{SN_2} from P_{Num_2}. Let the vertices of F_{SN_2} be o_2 as middle vertex and its neighbors are $f_{2i},\ i = 1$ to r_2. The $V_{mem.v}(f_{2i}) = n_{2i},\ i = 1$ to r_2 respectively and let $V_{mem.v}(o_2) = o_2$. $\mathcal{E}_{mem}v(o_2 f_{2i}) = \min(o_2, n_{2i})$, $i = 1$ to r_2, which is shown in Figure 2. The second subnetwork, F_{SN_2} illustrates the fuzzy graph structure used in the proposed encryption framework for secure information representation.

The $P_{Num_3}(x) = \sum_{i=1}^{r_3} a_{3i} * x^{(i-1)}$ is converted to encrypted polynomial $En(P_3(x)) = \sum_{i=1}^{r_3} ({a_{3i}}^e\ mod\ N) * x^{(i-1)}$ using RSA. $En(P_3(x)) = \sum_{i=1}^{r_3} ({a_{3i}}^e\ mod\ N) * x^{(i-1)} = \sum_{i=1}^{r_3} b_{3i} * x^{(i-1)}$, where $({a_{3i}}^e\ mod\ N) = b_{3i},\ i = 1$ to r_3. Choose $1 \leq x \leq 3$; let $x = 1,\ 2$ or 3 throughout $x^{(i-1)}$. $b_{3_{r3}} * x^{(r_3-1)} = \left(\frac{b_{3_{r3}}}{10000}\right) * 2^{(r_3-1)} = n_{3_{r3}}$, $b_3(r_3-1) * x^{(r_3-2)} = \left(\frac{b_{3_{r3}}}{10000}\right) * 2^{(r_3-1)} = n_3(r_3-1)$, Proceeding this, $b_{32} * x^1 = \left(\frac{b32}{10000}\right) * 3 = n_{32}$, $b_{31} * x^0 = \left(\frac{b31}{10000}\right) = n_{31}$. Each $n_{3i},\ i = 1$ to r_3 as the $V_{mem.v}$ of F_{SN_3}.

Construct F_{SN_3} from P_{Num_3}. Let the vertices of F_{SN_3} be o_3 as the middle vertex and its neighbors are $f_{3i},\ i = 1$ to r_3. The $V_{mem.v}(f_{3i}) = 3_i,\ i = 1$ to r_3 respectively and let $V_{mem.v}(o_3) = o_3$. $\mathcal{E}_{mem}v(o_3 f_{3i}) = \min(o_3, n_{3i})$, $i = 1$ to r_3, which is shown in Figure 3. Proceeding, the $P_{Poly_k}(x) = \sum_{i=1}^{r_k} aki * x^{(i-1)}$ is converted to encrypted polynomial $En(P_k(x)) = \sum_{i=1}^{r_k} ({a_{ki}}^e\ modN) * x^{(i-1)}$ using RSA.
$En(P_k(x)) = \sum_{i=1}^{r_k} ({a_{ki}}^e\ mod\ N) * x^{(i-1)} = \sum_{i=1}^{r_k} b_{k_i} * x^{(i-1)}$, where $({a_{ki}}^e\ mod\ N) = b_{ki},\ i = 1$ to r_k. Choose $1 \leq x \leq 3$ let the value be $x = 1,\ 2$ or 3 throughout $x^{(i-1)}$. $b_{k_{rk}} * x^{(r_k-1)} = \left(\frac{bkr_k}{10000}\right) * 2^{(r_k-1)} = n_{k_{rk}}$, $b_3(r_k-1) * x^{(r_k-2)} = \left(\frac{bkr_k}{10000}\right) * 2^{(r_k-1)} = b_k(r_k-1)$, Proceeding this, $b_{k_2} * x^1 = \left(\frac{bk2}{10000}\right) * 3 = n_{k_2}$, $b_{31} * x^0 = \left(\frac{bk1}{10000}\right) = n_{k_1}$.

Each $n_{k_i},\ i = 1$ to r_k as the $V_{mem.v}$ of F_{SN_k}. Construct F_{SN_k} from P_{Num_k}. Let the vertices of F_{SN_k} be $\mathcal{O}_k$ as the middle vertex and its neighbors are $f_{ki},\ i = 1$ to r_k. The $V_{mem.v}(f_{ki}) = n_{ki},\ i = 1$ to r_k respectively and let $\mathcal{V}_{mem}v(\mathcal{O}_k) = o_k$. $\mathcal{E}_{mem}v(o_k f_{ki}) = \min(o_k, n_{ki})$, $i = 1$ to r_k, which is shown in Figure 3. The third subnetwork, F_{SN_2}, representing the fuzzy graph network constructed as a component of the proposed framework.

Using F_{SN_1}, F_{SN_2}, F_{SN_3},..., F_{SN_k}, frame three types of fuzzy graph networks based on the number of edges (i) Fuzzy graph network with minimum number of edges ($F_{GN_{min}}$) (ii) Fuzzy graph network with an average number of edges ($F_{GN_{Avg}}$) (iii) Fuzzy graph network with maximum number of edges ($F_{GN_{Max}}$)

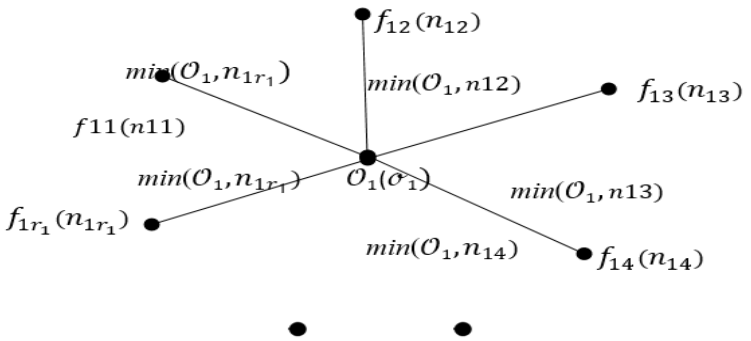

Figure 1: F_{SN_1}

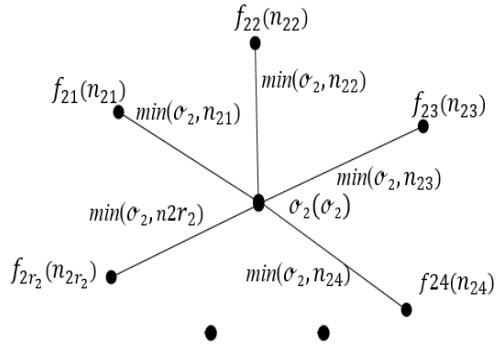

Figure 2: F_{SN_2}

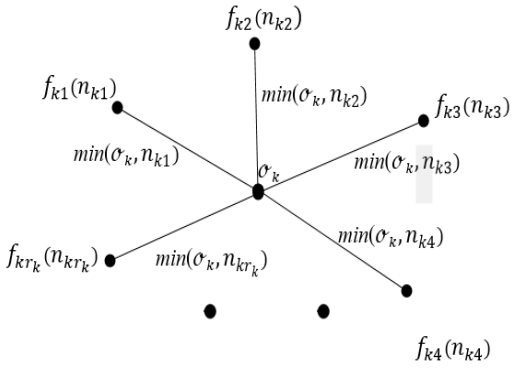

Figure 3: F_{SN_3}

(i)$F_{GN_{min}}$: This fuzzy graph is framed based on the efficient dominating members $\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3, \ldots, \mathcal{O}_k$. Join F_{SN_1}, F_{SN_2}, F_{SN_3},..., $F_{SN_{(k-1)}}$ by edges that do not violate the efficient dominating set. The number of edges in $F_{GN_{min}}$ are $\{\mathcal{O}_1 f_{1i}, (i = 1 \text{ to } r_1)\} \cup \{\mathcal{O}_2 f_{2i} (i = 1 \text{ to } r_2)\} \cup \{\mathcal{O}_3 f_{3i}, (i = 1 \text{ to } r_3)\} \cup \ldots \cup \{\mathcal{O}_k f_{ki} (i = 1 \text{ to } r_k)\} \cup \{ f_{1i} f_{2i}$ (for only one i)$\} \cup \{f_{2i} f_{3i}$ (for only one i)$\} \cup \{f_{3i} f_{4i}$ (for only one i)$\} \cup \cdots \cup \{f_{(k-2)i} f_{(k-1)i}$ (for only one i)$\} \cup \{f_{(k-1)i} f_{ki}$ (for only one i)$\} = r_1 + r_2 + r_3 + \cdots + r_k + (k-1)$.The number of vertices present is $r_1 + r_2 + r_3 + \cdots + r_k + k$, which is shown in Figure 4. It is the minimum fuzzy graph network, $F_{GN_{min}}$ constructed by connecting the subnetworks through efficient dominating vertices using the minimum number of inter-subnetwork edges while preserving the efficient dominating set.
(ii) $F_{GN_{Avg}}$: The number of edges present in $F_{GN_{Min}}$ is $r_1 + r_2 + r_3 + \cdots + r_k + (k-1)$. Along with these edges, $\mathcal{E}_{1i} \cup \mathcal{E}_{2i} \cup \mathcal{E}_{3i} \cup \cdots \cup \mathcal{E}_{ki} \cup \{f_{1i} f_{2j};\ i = 1 \text{ to } r_1,\ j = 1 \text{ to } r_2\} \cup \{f_{2i} f_{3j};\ i = 1 \text{ to } r_2,\ j = 1 \text{ to } r_3\} \cup \ldots$

$\cup\{f_{(k-1)i}f_{kj};\ i\ =\ 1\ to\ r_{(k-1)},\ j=\ 1\ to\ r_k\}\cup\{f_{ki}f_{1j};\ i=\ 1\ \text{to}\ r_k,\ j=\ 1\ \text{to}\ r_1\}$ (not all , some of the edges may be included) where $\mathcal{E}_{1i}=\ \{\ f_{1i}f_{1(i+1)i}=\ 1\ \text{to}\ r_1-1\}\cup\{f_{1r_1}f_{11}\}$ (not all , some of the edges may be included), $\mathcal{E}_{2i}=\{f_{2i}f_{2(i+1)i},\ i=\ 1\ \text{to}\ r_2-1\}\cup\{f_{2r_2}f_{21}\}$ (not all , some of the edges may be included) $\mathcal{E}_{3i}=\{\ f_{3i}f_{3(i+1)i},\ i=\ 1\ to\ r_3-1\}\cup\{f_{3r_3}f_{31}\}$ (not all, some of the edges may be included). Proceeding, $\mathcal{E}_{ki}=\{\ f_{ki}f_{k(i+1)i},\ i=\ 1\ \text{to}\ r_k-1\}\cup\{f_{kr_k}f_{k1}\}$ (not all, some of the edges may be included). The number of edges which are not exceeding the $F_{GN_{Max}}$, which is shown in Figure 5. It is the average fuzzy graph network, $F_{GN_{Avg}}$ illustrating the subnetworks interconnected with an intermediate number of intra- and inter-subnetwork edges, representing a balanced network structure between $F_{GN_{min}}$ and $F_{GN_{Max}}$.

(iii) $F_{GN_{\text{Max}}}$: The number of edges present in $F_{GN_{\text{Avg}}}$ is

$$n\binom{r_1+r_2+\cdots+r_k+(k-1)}{2}-\{\mathcal{O}_1f_{2i}:i=1,\ldots,r_2\}-\{\mathcal{O}_2f_{3i}:i=1,\ldots,r_3\}-\{\mathcal{O}_3f_{4i}:i=1,\ldots,r_4\}$$
$$-\cdots-\{\mathcal{O}_{k-1}f_{ki}:i=1,\ldots,r_k\}-\{\mathcal{O}_kf_{1i}:i=1,\ldots,r_1\}-\{\mathcal{O}_1\mathcal{O}_2,\mathcal{O}_2\mathcal{O}_3,\mathcal{O}_3\mathcal{O}_4,\ldots,\mathcal{O}_{k-1}\mathcal{O}_k,\mathcal{O}_k\mathcal{O}_1\}.$$

3 Encryption and decryption algorithm for the proposed work

3.1 Encryption algorithm

Input: P_{Num}
Output: F_{GN}

Step 1: Let the numerical plaintext be denoted by P_{Num}, given by

$$P_{\text{Num}}=\text{“}a_{11}a_{12}a_{13}\cdots a_{1r_1}/a_{21}a_{22}a_{23}\cdots a_{2r_2}/a_{31}a_{32}a_{33}\cdots a_{3r_3}/\cdots/a_{k1}a_{k2}a_{k3}\cdots a_{kr_k}.''$$

Step 2: Determine the Public key $PU_{key}(e,N)$ and the private key $PR_{key}(d,N)$. Let $P_1=N_1$,$P_2=N_2$,$P_3=N_3$,...,, $P_k=N_k$ then $N=\ P_1*\ P_2*P_3*\cdots*P_k$. The Euler pi function is given by $\varphi(N)=\ (P_1-1)*\ (P_2-1)*\cdots*\ (P_k-1)$. Choose e such that the GCD($e,\ \varphi(N)=1$. Find d such that $e*d=1\,(mod\ \varphi(N))$. Using e and d, find the public key $PU_{key}(e,N)$ and the private key $PR_{key}(d,N)$.

Step 3: Let $P_{Num_1}=a_{11}a_{12}a_{13}\ldots a_{1r_1}$. The corresponding plain text polynomial be $P_{Poly_1}(x)=a_{11}+\ a_{12}*\ x+a_{13}\ *\ x^2+\cdots+a_{1r_1}*x^{(r_1-1)}$.

The $P_{Poly_1}(x)=\sum_{i=1}^{r_1}a_{1i}*\ x^{(i-1)}$ is converted to encrypted polynomial $En(P_1(x))=\sum_{i=1}^{r_1}(a_{1i}{}^e\ mod\ N)\ *\ x^{(i-1)}$ using RSA. $En(P_1(x))=\sum_{i=1}^{r_1}(a_{1i}{}^e\ mod\ N)\ *\ x^{(i-1)}=\sum_{i=1}^{r_1}b_{1i}\ *\ x^{(i-1)}$, where $(a_{1i}{}^e\ mod\ N)=\ b_{1i},\ i=1\ to\ r_1$.

Using normalization, convert the coefficient of $x^{(i-1)}$ into a fuzzy number by (Coefficient of $x^{(i-1)}$)/10000. Choose the value of $x,\ 1\le x\le 3$; let the value be $x=1,\ 2$ or$\dot{3}$ throughout $x^{(i-1)}$. $b_{1r_1}\ *\ x^{(r_1-1)}=\left(\frac{b1r_1}{10000}\right)*\ 2^{(r_1-1)}=\ n_{2_{r1}}$, $b_{12}(r_1-1)\ *\ x^{(r_1-2)}=\left(\frac{b_{1r_1}}{10000}\right)*\ 2^{(r_1-1)}=\ n_1(r_1-1)$ (here the value of x is 2), Proceeding this, $b_{12}\ *\ x^1=\left(\frac{b_{12}}{10000}\right)*\ 3=\ n_{12}$, (here the value of x is 3), and $b_{11}\ *\ x^0=\left(\frac{b_{11}}{10000}\right)=\ n_{11}$.

Each $n_{1i},\ i=1$ to r_1 as $V_{mem.v}$ of F_{SN_1}. Construct the F_{SN_1} from P_{Num_1}. Let the vertices of the F_{SN_1} are o_1 as middle vertex and its neighbors are $f_{1_i},\ i=\ 1$ to r_1. The $V_{mem.v}(f_{1_i})=\ n_{1i},\ i=1$ to r_1 respectively and let $V_{mem.v}(o_1)=o_1$. $\mathcal{E}_{mem}v(o_1f_{1_i})=\min(\ o_1,n_{1i})\},\ i=1$ to r_1.

Step 4: Let $P_{Num_2}=a_{21}a_{22}a_{23}\ldots a_{2r_2}$. The corresponding plain text polynomial be $P_{Poly_2}(x)=a_{21}+\ a_{22}*\ x+a_{23}\ *\ x^2+\cdots+a_{2r_2}*x^{(r_2-1)}$. The $P_{Poly_2}(x)=\ \sum_{i=1}^{r_1}a_{2i}*\ x^{(i-1)}$ is converted to encrypted polynomial using RSA $En(P_2(x))=\ \sum_{i=1}^{r_2}(a_{2i}{}^e\ mod\ N)\ *\ x^{(i-1)}$.
$En(P_2(x))=\ \sum_{i=1}^{r_2}(a_{2i}{}^e\ mod\ N)\ *\ x^{(i-1)}=\sum_{i=1}^{r_2}b_{2i}\ *\ x$, where $(a_{2i}{}^e\ mod\ N)=b_{2i},\ i=1$ to r_2.

Choose the value of $x,\ 1\le x\le 3$, let the value be $x=1$ or 2 or 3 throughout $x^{(i-1)}$. $b_{2_{r2}}*x^{(r_2-1)}=\left(\frac{b_{2r_2}}{10000}\right)*2^{(r_2-1)}=$ $n_{2_{r2}}$, $b_2(r_2-1)\ *\ x^{(r_2-2)}=\left(\frac{b_{2r_3}}{10000}\right)*\ 2^{(r_2-1)}=\ n_2(r_2-1)$, Proceeding this, $b_{22}\ *\ x^1=\left(\frac{b_{22}}{10000}\right)*\ 3=\ n_{22}$, $b_{21}\ *\ x^0=\left(\frac{b21}{10000}\right)=\ n_{21}$. Each $n_{2i},\ i=1\ to\ r_2$ as the vertex membership values ($V_{mem.v}$) of F_{SN_2}. Construct

F_{SN_2} from P_{Num_2}. Let the vertices of F_{SN_2} be o_2 as the middle vertex and its neighbors are $f_{2i},\ i=1$ to r_2. The $V_{mem.v}(f_{2i}) = n_{2i},\ i=1$ to r_2 respectively and let $V_{mem.v}(o_2) = o_2$. $\mathcal{E}_{mem}v(o_2f_{2i}) = \min(o_2, n_{2i})\ ,\ i=1$ to r_2.

Step 5: Let $P_{Num_3} = a_{31}a_{32}a_{33}\ldots a_{3r_3}$. The corresponding plain text polynomial be $P_{Poly_3}(x) = a_{31} + a_{32} * x + a_{33} * x^2 + \cdots + a_{3r_3} * x^{(r_3-1)}$.The $P_{Num_3}(x) = \sum_{i=1}^{r_3} a_{3i} * x^{(i-1)}$ is converted to encrypted polynomial
$En(P_3(x)) = \sum_{i=1}^{r_3} ({a_{3i}}^e \ mod\ N) * x^{(i-1)}$ using multi-prime RSA.
$En(P_3(x)) = \sum_{i=1}^{r_3} (a3i^e \ mod\ N) * x^{(i-1)}$ where $({a_{3i}}^e \ mod\ N) = b_{3i},\ i=1$ to r_3.

$1 \le x \le 3$, let $x=1,\ 2$ or 3 throughout $x^{(i-1)}$. $b_{3_{r3}} * x^{(r_3-1)} = \left(\frac{b_{3_{r3}}}{10000}\right) * 2^{(r_3-1)} = n_{3_{r3}}$, $b_3(r_3-1) * x^{(r_3-2)} = \left(\frac{b_{3_{r3}}}{10000}\right) * 2^{(r_3-1)} = n_3(r_3-1)$, Proceeding this, $b_{32} * x^1 = \left(\frac{b_{32}}{10000}\right) * 3 = n_{32}$, $b_{31} * x^0 = \left(\frac{b_{31}}{10000}\right) = n_{31}$. Each $n_{3i},\ i=1$ to r_3 as the $V_{mem.v}$ of F_{SN_3}. Construct F_{SN_3} from P_{Num_3}. Let the vertices of F_{SN_3} are o_3 as middle vertex and its neighbors are $f_{3i},\ i=1$ to r_3. The $V_{mem.v}(f_{3i}) = 3i,\ i=1$ to r_3 respectively and let $V_{mem.v}(o_3) = o_3$. $\mathcal{E}_{mem}v(o_3f_{3i}) = \min(o_3, n_{3i})\ ,\ i=1$ to r_3.

Step 6: Proceeding this, let$P_{Num_k} = a_{k1}a_{k2}a_{k3}\ldots a_{kr_k}$. The corresponding plain text polynomial is $P_{Poly_k}(x) = a_{k1} + a_{k2} * x + a_{k3} * x^2 + \cdots + a_{kr_k} * x^{(r_1-1)}$. The $P_{Poly_k}(x) = \sum_{i=1}^{r_k} a_{ki} * x^{(i-1)}$ is converted to encrypted polynomial $En(P_k(x)) = \sum_{i=1}^{r_k} ({a_{ki}}^e \ modN) * x^{(i-1)}$ using RSA. $En(P_k(x)) = \sum_{i=1}^{r_k} ({a_{ki}}^e \ mod\ N) * x^{(i-1)} = \sum_{i=1}^{r_k} b_{k_i} * x^{(i-1)}$, where $({a_{ki}}^e \ mod\ N) = b_{ki},\ i=1$ to r_k.

$1 \le x \le 3$, let $x=1,\ 2$ or 3 throughout $x^{(i-1)}$. $b_{k_{rk}} * x^{(r_k-1)} = \left(\frac{bkr_k}{10000}\right) * 2^{(r_k-1)} = n_{k_{rk}}$, $b_3(r_k-1) * x^{(r_k-2)} = \left(\frac{bkr_k}{10000}\right) * 2^{(r_k-1)} = b_k(r_k-1)$, Proceeding this, $b_{k_2} * x^1 = \left(\frac{bk2}{10000}\right) * 3 = n_{k_2}$, $b_{31} * x^0 = \left(\frac{bk1}{10000}\right) = n_{k_1}$. Each $n_{k_i},\ i=1$ to r_k as the $V_{mem.v}$ of F_{SN_k}. Construct F_{SN_k} from P_{Num_k}. Let the vertices of F_{SN_k} be $\mathcal{O}_k$ as the middle vertex and its neighbors are $f_{ki},\ i=1$ to r_k. The $V_{mem.v}(f_{ki}) = n_{ki},\ i=1$ to r_k respectively and let $\mathcal{V}_{mem}v(\mathcal{O}_k) = o_k$. $\mathcal{E}_{mem}v(o_kf_{ki}) = \min(o_k, n_{ki})\ ,\ i=1$ to r_k.

Step 7: Using the F_{SN_1}, F_{SN_2}, F_{SN_3},..., F_{SN_k}, frame three types of fuzzy graph networks based on the number of edges (i) $F_{GN_{Min}}$(ii) $F_{GN_{Avg}}$ (iii) $F_{GN_{Max}}$, FGN is the encrypted fuzzy network; its construction procedure is given in Section 3.

3.2 Decryption algorithm for the proposed work

The final encrypted ciphertext generated by the proposed multi-layer encryption framework is used to reconstruct the original plaintext by the proposed decryption algorithm. The algorithm's input consists of the final ciphertext and the decryption parameters, such as the cryptographic keys and parameters for decrypting each layer. The result of the algorithm is the recovered plaintext, which is the same as the original message before encryption. The decryption is done by reversing the encryption process one by one in reverse order to that of the encryption process. The detailed steps of the proposed decryption algorithm are given below.

Algorithm 1 Algorithm for the proposed work

Input: F_{GN}

1: **Output:** P_{Num}
2: **Step 1:** Find the efficient dominating members of F_{GN}, which are $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_k$. The neighbors of $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_k$ are $f_{1i},\ i=1$ to r_1, $f_{2i},\ i=1$ to r_2,..., $f_{ki},\ i=1$ to r_k respectively.
3: **Step 2:** The $\mathcal{V}_{mem}v(f_{1i}) = n_{1i},\ i=1$ to r_1, , $\mathcal{V}_{mem}v(f_{2i}) = n_{2i},\ i=1$ to r_2,..., $\mathcal{V}_{mem}v(f_{ki}) = n_{ki},\ i=1$ to r_k.
4: **Step 3:** Find b_{1i} from $n_{1i}\ ,\ i=1$ to r_1; b_{2i} from $i=1$ to r_2;...; b_{ki} from $i=1$ to r_k.
5: **Step 4:** Find $b_{1i} = {a_{1i}}^e \ mod\ N;\ i=1$ to r_1, $b_{2i} = {a_{2i}}^e \ mod\ N;\ i=1$ to r_2,..., $b_{ki} = {a_{ki}}^e \ mod\ N;\ i=1$ to r_k. Find $a_{1i};\ i=1$ to r_1, $a_{2i}; i=1$ to r_2, $\ldots, a_{ki}; i=1$ to r_k. using ${b_{1i}}^d \ mod\ N(\ i=1$ to $r_1)$, ${b_{2i}}^d \ mod\ N\,(i=1$ to $r_2), \ldots, {b_{ki}}^d \ mod\ N(i=1$ to $r_k)$.
6: **Step 5:** From $a_{1i};\ i=1$ to r_1 , we get $P_{Num_1} = a_{11}a_{12}a_{13}\ldots a_{1r_1}$, from $a_{2i}; i=1$ to r_2, we get $P_{Num_2} = a_{21}a_{22}a_{23}\ldots a_{2r_2}$, from $a_{3i}; i=1$ to r_3 we get $P_{Num_3} = a_{31}a_{32}a_{33}\ldots a_{3r_3}$, proceeding this from $a_{ki}; i=1$ to r_k we get $P_{Num_k} = a_{k1}a_{k2}a_{k3}\ldots a_{kr_k}$.
7: Finally, the plaintext is $P_{Num} =$ " $a_{11}a_{12}a_{13}\ldots a_{1r_1}/\ a_{21}a_{22}a_{23}\ldots a_{2r_2}/\ a_{31}a_{32}a_{33}\ldots a_{3r_3}/\ \ldots/a_{k1}a_{k2}a_{k3}\ldots a_{kr_k}$".

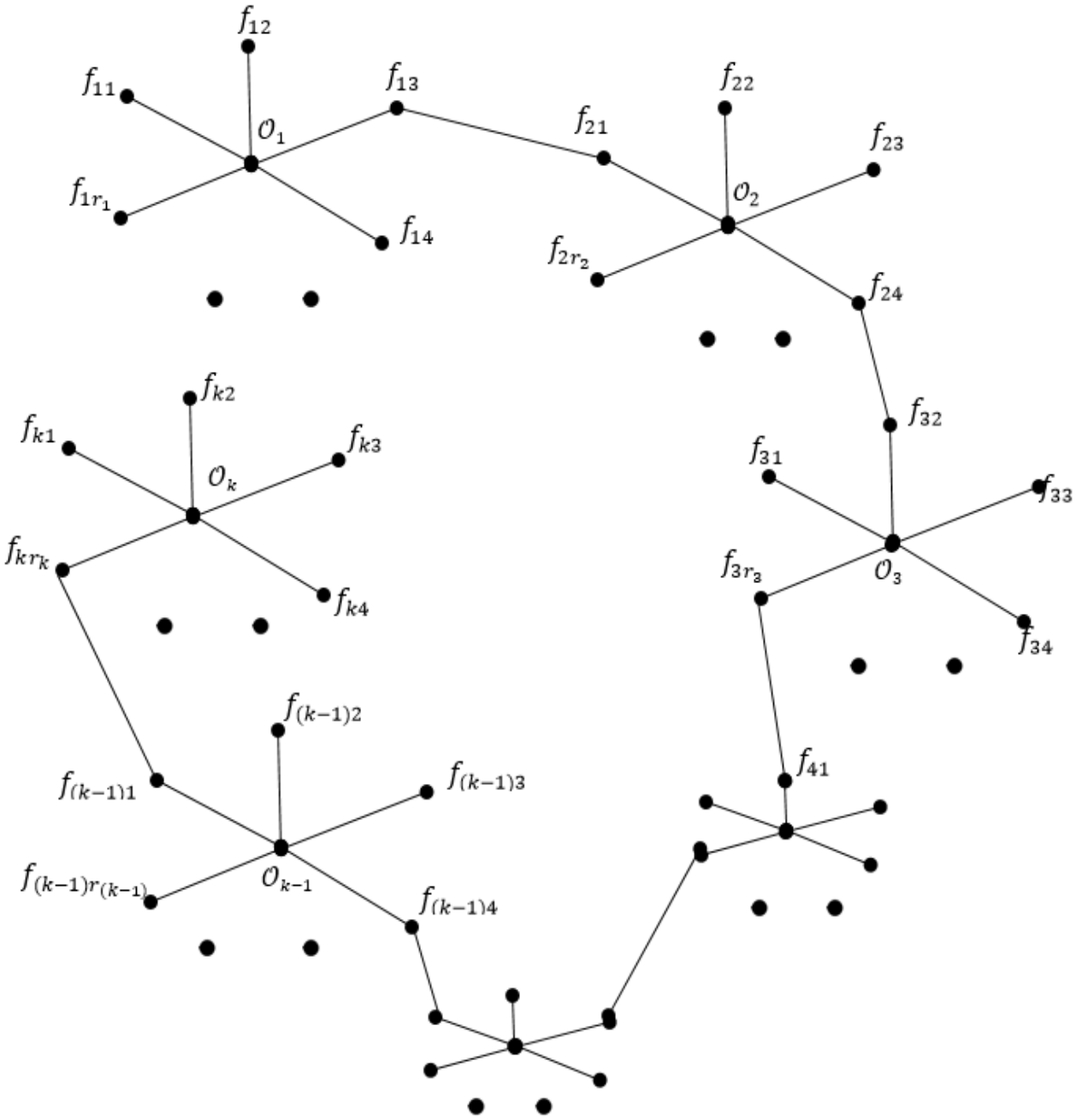

Figure 4: $F_{GN_{Min}}$

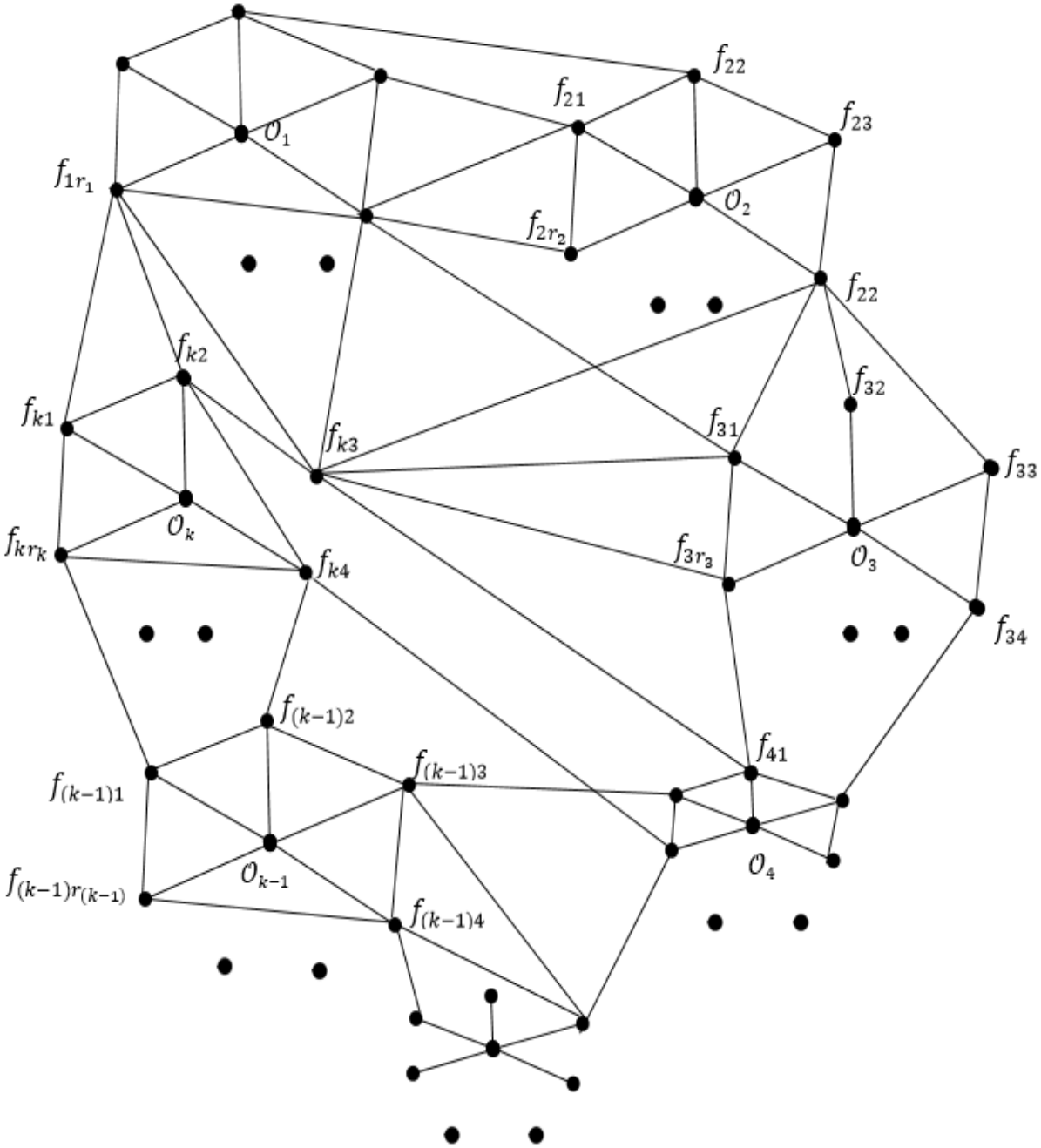

Figure 5: $L - F_{GN_{Avg}}$

4 An example of the proposed method

The plaintext is P_{Num} =22132145773314/153205421013/3344556677/425663721437 /5865729. Using multi-prime RSA algorithm first to find the $PU_{key}(e, N)$ and $PR_{key}(d, N)$. Let $P_1 = 3, P_2 = 5$ and $P_3 = 11$ then $N = P_1 * P_2 * P_3 = 165$. The Euler phi function is given by $\varphi(N) = (P_1 - 1) * (P_2 - 1) * (P_3 - 1) = 80$. Choose $e = 7$ such that the GCD$(e, \varphi(N) = 1$. Find d such that $e * d = 1 (mod\, \varphi(N))$. Using e and d, find the public key $PU_{key}(e, N) = PU_{key}(7, 165)$ and private key $PR_{key}(23, 165)$. For all the sub-networks retain the same $PU_{key}(e, N)$ and $PR_{key}(d, N)$.

4.1 Encryption algorithm

Input: $L - P_{Num}$
Output: $L - P_{Num}$
Step 1: Let the numerical plaintext be denoted by

$$L\text{-}P_{\text{Num}} = \text{“22132145773314/153205421013/3344556677/425663721437/58657299”}.$$

Let $L - P_{Num_1} = a_{11}a_{12}a_{13}\ a_{14}a_{15}a_{16}\ a_{17}$ =22132145773314; $a_{11} = 22$; $a_{12} = 13$; $a_{13} = 21$; $a_{14} = 45$; $a_{15} = 77$; $a_{16} = 33$; $a_{17} = 14$.(here $L - P_{Num_1}$ is partitioned into 2 digits, one's wish may partitioned into 2 or more digits). Let $L - P_{Num_2} = a_{21}a_{22}a_{23}a_{24}a_{25}a_{26}$ =1532054210, $a_{21} = 15$; $a_{22} = 32$; $a_{23} = 05$; $a_{24} = 42$; $a_{25} = 10$;$a_{26} = 13$. Let $L - P_{Num_3} = a_{31}a_{32}a_{33}a_{34}a_{35}$ =3344556677 $a_{31} = 33$; $a_{32} = 44$; $a_{33} = 55$; $a_{34} = 66$;$a_{35} = 77$. Let $L - P_{Num_4} = a_{41}a_{42}a_{43}a_{44}a_{45}a_{46} = 425663721437$. $a_{41} = 42$; $a_{42} = 56$; $a_{43} = 63$; $a_{44} = 72$; $a_{45} = 14$; $a_{46} = 37$. Let $L - P_{Num_5} = a_{51}a_{52}a_{53}a_{54} = 58657299$. $a_{51} = 58$; $a_{52} = 65$; $a_{53} = 72$; $a_{54} = 99$.

Step 2: Let $L - P_{Num_1} = a_{11}a_{12}a_{13}a_{14}a_{15}a_{16}a_{17}$ =22132145773314 where $a_{11} = 22$; $a_{12} = 13$; $a_{13} = 21$; $a_{14} = 45$; $a_{15} = 77$; $a_{16} = 33$; $a_{17} = 14$. The corresponding plain text polynomial is $L - P_{Poly_1}(x) = a_{11} + a_{12} * x + a_{13} * x^2 + a_{14} * x^3 + a_{15} * x^4 + a_{16} * x^5 + a_{17} * x^6 = 22 + 13 * x + 21 * x^2 + 45 * x^3 + 77 * x^4 + 33 * x^5 + 14 * x^6$. The $L - P_{Poly_1}(x) = \sum_{i=1}^{7} a_{1i} * x^{(i-1)}$ is converted to encrypted polynomial $L - En(P_1(x)) = \sum_{i=1}^{7} ({a_{1i}}^e \ mod\ 165) * x^{(i-1)}$ using multi-prime RSA.

$En(P_1(x)) = \sum_{i=1}^{r_1} ({a_{1i}}^e \ mod\ 165) * x^{(i-1)} = \sum_{i=1}^{7} b_{1i} * x^{(i-1)}$, where $({a_{1i}}^e \ mod\ 165) = b_{1i}$, $i = 1$ to 7, $b_{11} = 119$, $b_{12} = 132$, $b_{13} = 143$, $b_{14} = 45$, $b_{15} = 21$ $b_{16} = 7$ $b_{17} = 88$. Using normalization, convert the coefficient of $x^{(i-1)}$ into fuzzy number by (Coefficient of $x^{(i-1)}$)/10000.
Choose the value of x, $1 \le x \le 3$, let the value be $x = 1$ or 2 or 3 throughout $x^{(i-1)}$. $\left(\frac{b_{17}}{10000}\right) * x^{(6)} = \left(\frac{88}{10000}\right) * 2^6 = 0.5632 = n_{17}$, $\left(\frac{b_{16}}{10000}\right) * 2^5 = \left(\frac{7}{10000}\right) * 2^{(5)} = 0.0224 = n_{16}$ (here the value of x is 2), $\left(\frac{b_{15}}{10000}\right) * 2^4 = \left(\frac{21}{10000}\right) * 2^4 = 0.0336 = n_{15}$. $\left(\frac{b_{14}}{10000}\right) * 2^3 = \left(\frac{45}{10000}\right) * 2^3 = 0.036 = n_{14}$. $\left(\frac{b_{13}}{10000}\right) * 2^4 = \left(\frac{143}{10000}\right) * 2^2 = 0.0572 = n_{13}$. $\left(\frac{b_{12}}{10000}\right) * 3 = \left(\frac{132}{10000}\right) * 3 = 0.0396 = n_{12}$. $\left(\frac{b_{11}}{10000}\right) = \left(\frac{119}{10000}\right) = 0.0119 = n_{11}$.
Corresponding n_{1i} values are $n_{11} = 0.0119$; $n_{12} = 0.0396$; $n_{13} = 0.0572$; $n_{14} = 0.036$; $n_{15} = 0.0336$; $n_{16} = 0.0224$ and $n_{17} = 0.5632$. Each n_{1i}, $i = 1$ to 7 as the vertex membership value ($\mathcal{V}_{mem}v$) of the first network $L - F_{SN_1}$. Construct the F_{SN_1} from P_{Poly_1}.
Let the vertices of $L - F_{SN_1}$ be $\mathcal{O}_1$ as the middle vertex, and its neighbors are f_{1i}, $i =$ 1 to 7. Then $\mathcal{V}_{mem}v(f_{1i}) = n_{1i}$, $i = 1$ to 7 are respectively 0.0119; 0.0396; 0.0572; = 0.036; 0.0336; 0.0224 and 0.5632. Let $\mathcal{V}_{mem}v(\mathcal{O}_1) = o_1 = 0.1$. $\mathcal{E}_{mem}v(\mathcal{O}_1 f_{1i}) = \min(o_1, n_{1i})$, $i = 1$ to 7, $\mathcal{E}_{mem}v(\mathcal{O}_1 f_{11}) = \min(\mathcal{O}_1, n_{11}) = \min(0.1, 0.0119) = 0.0119$; $\mathcal{E}_{mem}v(\mathcal{O}_1 f_{12}) = \min(o_1, n_{12}) = \min(0.1, 0.0396) = 0.0396$;$\mathcal{E}_{mem}v(\mathcal{O}_1 f_{13}) = \min(o_1, n_{13}) = \min(0.1, 0.0572) = 0.0572$; $\mathcal{E}_{mem}v(\mathcal{O}_1 f_{14}) = \min(o_1, n_{14}) = \min(0.1, 0.036) = 0.036$; $\mathcal{E}_{mem}v(\mathcal{O}_1 f_{15}) = \min(\mathcal{O}_1, n_{15}) = \min(0.1, 0.0336) = 0.0336$;$\mathcal{E}_{mem}v(\mathcal{O}_1 f_{16}) = \min(o_1, n_{16}) = \min(0.1, 0.0224) = 0.0224$ and $\mathcal{E}_{mem}v(\mathcal{O}_1 f_{17}) = \min(\mathcal{O}_1, n_{17}) = \min(0.1, 0.5632.) = 0.1$, see Figure 6.

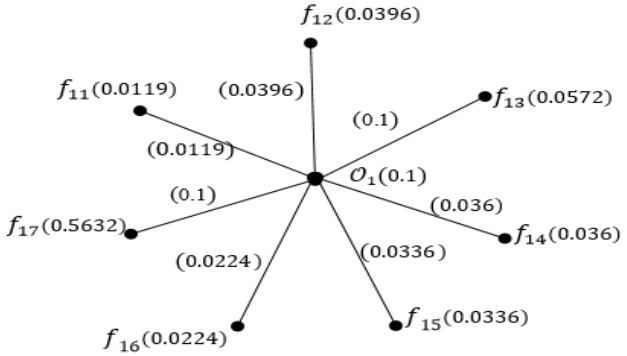

Figure 6: $L - F_{SN_1}$

Step 3: Let $P_{Poly_2} = a_{21}a_{22}a_{23}a_{24}a_{25}a_{26}$ =153205421013, where $a_{21} = 15$; $a_{22} = 32$; $a_{23} = 05$; $a_{24} = 42$; $a_{25} = 10$ and $a_{26} = 13$. The corresponding plain text polynomial is $P_{Poly_2}(x) = a_{21} + a_{22} * x + a_{23} * x^2 + a_{24} * x^3 + a_{25} * x^4 + a_{26} * x^5 = 15 + 32 * x + 05 * x^2 + 42 * x^3 + 10 * x^4 + 13 * x^5$.

$P_{Poly_2}(x) = \sum_{i=1}^{6} a_{2i} * x^{(i-1)}$ is converted to encrypted polynomial $En(P_2(x)) = \sum_{i=1}^{6} (a_{2i}{}^e \ mod\ 165) * x^{(i-1)}$ using RSA. $L - En(P_2(x)) = \sum_{i=1}^{6} (a_{2i}{}^e \ mod\ 165) * x^{(i-1)} = \sum_{i=1}^{6} b_{2i} * x^{(i-1)}$, where $(a_{2i}{}^e \ mod\ 165) = b_{2i},\ i = 1$ to 6. b_{21} =7, $b_{22} = 10$, $b_{23} = 48$, $b_{24} = 80$, $b_{25} = 98$, $b_{26} = 60$.
Using normalization, convert the coefficient of $x^{(i-1)}$ into a fuzzy number by (Coefficient of $x^{(i-1)}$)/10000. Choose the value of x, $1 \le x \le 3$, let the value be $x = 1$ or 2 or 3 throughout $x^{(i-1)}$. $\left(\frac{b_{26}}{10000}\right) * 2^5 = 0.192 = n_{26}$, $\left(\frac{b_{25}}{10000}\right) * 2^4 = 0.1568 = n_{25}$, $\left(\frac{b_{24}}{10000}\right) * 2^3 = 0.064 = n_{24}$. $\left(\frac{b_{23}}{10000}\right) * 2^2 = 0.0432 = n_{23}$. $\left(\frac{b_{22}}{10000}\right) * 3 = 0.003 = n_{22}$, $\left(\frac{b_{21}}{10000}\right) = 0.0007 = n_{21}$.
Corresponding n_{2i} values are $n_{21} = 0.0007$; $n_{22} = 0.003$, $n_{23} = 0.0432$, n_{24} =0.064, $n_{25} = 0.1568$ and $n_{26} = 0.192$. Each $n_{2i},\ i = 1$ to 6 is the vertex membership value ($\mathcal{V}_{mem}v$) of F_{SN_2}. Construct the $L - F_{SN_2}$ from $L - P_{Poly_2}$.
Let the vertices of $L - F_{SN_2}$ be $\mathcal{O}_2$ as the middle vertex, and its neighbors are $f_{2i},\ i =$ 1 to 6. Then $\mathcal{V}_{mem}v(f_{2i}) = n_{2i},\ i = 1$ to 6 are respectively 0.0007, 0.003, 0.0432, 0.064, 1568 and 0.192. Let $\mathcal{V}_{mem}v(\mathcal{O}_2) = o_2 = 0.2$. $\mathcal{E}_{mem}v(\mathcal{O}_2 f_{2i} = \min(o_2, n_{2i}),\ i = 1$ to 6, $\mathcal{E}_{mem}v(\mathcal{O}_2 f_{21}) = \min(o_2, n_{21}) = (0.2, 0.0007) = 0.0007$; $\mathcal{E}_{mem}v(\mathcal{O}_2 f_{22}) = \min(o_2, n_{22}) = \min(0.2, 0.003) = 0.003, \mathcal{E}_{mem}v(\mathcal{O}_2 f_{23}) = \min(o_2, n_{23}) = \min(0.2, 0.0432) = 0.0432$, $\mathcal{E}_{mem}v(\mathcal{O}_2 f_{24}) = \min(o_2, n_{24}) = \min(0.2, 0.064) = 0.064$; $\mathcal{E}_{mem}v(\mathcal{O}_2 f_{25}) = \min(o_2, n_{25}) = \min(0.2, 0.1568) = 0.1568$ and $\mathcal{E}_{mem}v(\mathcal{O}_2 f_{26}) = \min(o_2, n_{26}) = \min(0.2, 0.192) = 0.192$, see Figure 7.

Step 4: Let $P_{Poly_3} = a_{31}a_{32}a_{33}a_{34}a_{35}a_{36} = 3344556677$ where $a_{31} = 33$; $a_{32} = 44$; $a_{33} = 55$; $a_{34} = 66$ and $a_{35} = 77$. The corresponding plain text polynomial is $L - P_{Poly} = a_{31} + a_{32} * x + a_{33} * x^2 + a_{34} * x^3 + a_{35} * x^4 + a_{36} * x^5 = 33 + 44 * x + 55 * x^2 + 66 * x^3 + 77 * x^4$.$\mathrm{P}_{Poly_3}(x) = \sum_{i=1}^{5} a_{3i} * x^{(i-1)}$ is converted to encrypted polynomial $L - En(P_3(x)) = \sum_{i=1}^{5} (a_{3i}{}^e \ mod\ 221) * x^{(i-1)}$ using multi-prime RSA. $L - En(P_3(x)) = \sum_{i=1}^{5} (a_{3i}{}^e \ mod\ 165) * x^{(i-1)} = \sum_{i=1}^{5} b_{3i} * x^{(i-1)}$, where $(a_{3i}{}^e \ mod\ 165) = b_{3i},\ i = 1\ to\ 5$.
Using normalization, convert the coefficient of $x^{(i-1)}$ into fuzzy number by (Coefficient of $x^{(i-1)}$)/10000.$\$Choosethevalueofx$, $1 \le x \le 3$, let the value be $x = 1$ or 2 or 3 throughout $x^{(i-1)}$. $\left(\frac{b_{35}}{10000}\right) * 2^4 = 0.2112 = n_{35}$, $\left(\frac{b_{34}}{10000}\right) * 3^3 = 0.1188 = n_{34}$. $\left(\frac{b_{33}}{10000}\right) * 3^2 = 0.0495 = n_{33}$. $\left(\frac{b_{32}}{10000}\right) * 3 = 0.018 = n_{32}$, $\left(\frac{b_{31}}{10000}\right) = 0.0143 = n_{31}$.
Corresponding n_{3i} values are $n_{31} = 0.0143$, $n_{32} = 0.018$, $n_{33} = 0.0495$, $n_{34} = 0.1188$ and $n_{35} = 0.2112$. Each $n_{3i},\ i = 1$ to 5 is the vertex membership value ($\mathcal{V}_{mem}v$) of $L - F_{SN_3}$. Construct $L - F_{SN_3}$from $L - P_{Poly_3}$.
Let the vertices of $L - F_{SN_3}$ be $\mathcal{O}_3$ as the middle vertex and its neighbors are $f_{3i},\ i =$ 1 to 5. The $\mathcal{V}_{mem}v(f_{3i}) = n_{3i},\ i = 1\ to\ 5$ are respectively 0.0143, 0.018, 0.0495, 0.1188 and 0.2112. Let $\mathcal{V}_{mem}v(\mathcal{O}_3) = o_3 = 0.3$. $\mathcal{E}_{mem}v(\mathcal{O}_3 f_{3i}) = \min(o_3, n_{3i}),\ i = 1\ to\ 5$, $\mathcal{E}_{mem}v(\mathcal{O}_3 f_{31}) = \min(o_3, n_{31}) = \min(0.3, 0.0143) = 0.0143$, $\mathcal{E}_{mem}v(\mathcal{O}_3 f_{32}) = \min(o_3, n_{32}) = \min(0.3, 0.018) = 0.018, v(\mathcal{O}_3 f_{33}) = \min(o_3, n_{33}) = \min(0.3, 0.0495) = 0.0495$, $\mathcal{E}_{mem}v(\mathcal{O}_3 f_{34}) = \min(o_3, n_{34}) = \min(0.3, 0.1188) = 0.1188$ and $\mathcal{E}_{mem}v(\mathcal{O}_3 f_{35}) = \min(o_3, n_{35}) = \min(0.3, 0.2112) = 0.2112$, see Figure 8.

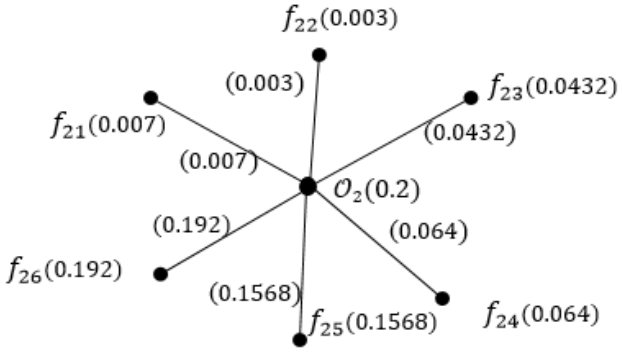

Figure 7: $L - F_{SN_2}$

Step 5: Let $P_{Poly_4} = a_{41}a_{42}a_{43}a_{44}a_{45}a_{46} = 425663721437$, where $a_{41} = 42$; $a_{42} = 56$; $a_{43} = 63$; $a_{44} = 72$; $a_{45} = 14$ and $a_{46} = 37$. The corresponding plain text polynomial is $L - P_{Poly_4}(x) = a_{41} + a_{42} * x + a_{43} * x^2 + a_{44} * x^3 + a_{45} * x^4 + a_{46} * x^5 = 42 + 56 * x + 63 * x^2 + 72 * x^3 + 14 * x^4 + 37 * x^5$. $P_{Poly_4}(x) = \sum_{i=1}^{6} a_{4i} * x^{(i-1)}$ is converted to encrypted polynomial $L - En(P_4(x)) = \sum_{i=1}^{6} (a_{4i}{}^e \ mod\ 165) * x^{(i-1)}$ using multi-prime RSA. $L - En(P_4(x)) = \sum_{i=1}^{6} (a_{4i}{}^e \ mod\ 165) * x^{(i-1)} = \sum_{i=1}^{6} b_{4i} * x^{(i-1)}$, where $(a_{4i}{}^e \ mod\ 165) = b_{4i},\ i = 1\ to\ 6$. b_{4i} where i = 1 to 6 are $b_{41} = 148$, $b_{42} = 119$, $b_{43} = 63$, $b_{44} = 57$, $b_{45} = 56$ and $b_{46} = 48$.
Using normalization, convert the coefficient of $x^{(i-1)}$ into a fuzzy number by (Coefficient of $x^{(i-1)}$)/10000. $1 \le x \le 3$, let $x = 1$ or 2 or 3 throughout $x^{(i-1)}$. $n_{41} = 0.0148$, $n_{42} = 0.0357$(here x is 3), $n_{43} = 0.0567$(here x is 3), $n_{44} =$

0.1539(here x is 3), $n_{45} = 0.0896$ (here x is 2) and $n_{46} = 0.1536$(here x is 2. Each $n_{4i},\ i = 1\ to\ 6$ is the vertex membership value ($\mathcal{V}_{mem}v$) of $L - F_{SN_4}$.
Construct the $L - F_{SN_4}$from P_{Poly_4}. Let the vertices of $L - F_{SN_4}$ be $\mathcal{O}_4$ as the middle vertex and its neighbors are $f_{4i},\ i =$ 1 to 6. Then $\mathcal{V}_{mem}v(\ f_{4i}) =\ n_{4i},\ i = 1\ to\ 6$ are respectively 0.0148, 0.0357, 0.0567, 0.1539, 0.0896 and 0.1536 and let $\mathcal{V}_{mem}v(\mathcal{O}_4) = o_4 = 0.4$. $\mathcal{E}_{mem}v(\mathcal{O}_4\ f_{4i}) = \min(\ o_4,\ n_{4i})\ ,\ i = 1\ to\ 6,\ \mathcal{E}_{mem}v(\mathcal{O}_4\ f_{41}) = \min(o_4,\ n_{41}) = \min(0.4,$ 0.0148) = 0.0148; $\mathcal{E}_{mem}v(\mathcal{O}_4 f_{42}) = \min(o_4, n_{42}) = \min(0.4,\ 0.0357) = 0.0357$;$\mathcal{E}_{mem}v(\mathcal{O}_4 f_{43}) = \min(o_4, n_{43}) = \min(0.4,$ 0.0567) = 0.0567; $\mathcal{E}_{mem}v(\mathcal{O}_4 f_{44}) = \min(o_4, n_{44}) = \min(0.4,\ 0.1539) = 0.1539$; $\mathcal{E}_{mem}v(\mathcal{O}_4 f_{45}) = \min(o_4, n_{45}) = \min(0.4,$ 0.0896) = 0.0896 and $\mathcal{E}_{mem}v(\mathcal{O}_4 f_{46}) = \min(o_4, n_{46}) = \min(0.4,\ 0.1536) = 0.1536$, see Figure 9.

Step 6: Let $P_{Poly_5} = a_{51}a_{52}a_{53}a_{54} = 58657299$ where $a_{51} = 58$; $a_{52} = 65$; $a_{53} = 72$ and $a_{54} = 99$. The corresponding plain text polynomial is $P_{Poly_5}(x) = a_{51} + \ a_{52} * \ x + a_{53}\ *\ x^2 + a_{54}\ *\ x^3 = 58 +\ 65 * \ x +\ 72\ *\ x^2 +\ 99\ *\ x^3$. $P_{Poly_3}(x) = \sum_{i=1}^{4} a4i\ *x^{(i-1)}$ is converted to encrypted polynomial $L - En\,(P_5\,(x)) = \sum_{i=1}^{4}(a_{5i}{}^e\ mod\ 165) *\ x^{(i-1)}$ using RSA. $L - En\,(P_5\,(x)) = \sum_{i=1}^{4}(a_{5i}{}^e\ mod\ 221) *\ x^{(i-1)} = \sum_{i=1}^{4} b_{5i} *\ x^{(i-1)}$, where $(a_{5i}{}^e\ mod\ 165) =\ b_{5i},\ i =$ 1 to 4. The coefficient of $x^{(i-1)}$, b_{5i} where i = 1 to 4 are $b_{51} = 99$, b_{52} =63, $b_{53} = 65$ and $b_{54} = 97$.
Using normalization, convert the coefficient of $x^{(i-1)}$ into a fuzzy number by (Coefficient of $x^{(i-1)}$)/10000.$\$Choose\ 1 \leq x \leq 3$, let $x = 1$ or 2 or 3 throughout $x^{(i-1)}$. $n_{51} = 0.0099$, $n_{52} = 0.0189$ (here x is 3), $n_{53} = 0.0585$(here x is 3), $n_{54} =$ 0.2619(here x is 3), Each $n_{5i},\ i = 1\ to\ 4$ is the vertex membership value ($\mathcal{V}_{mem}v$) of the $L - F_{SN_5}$. Construct the $L - F_{SN_5}$from $L - P_{Poly_5}$.

Let the vertices of L-F_{SN_5} be $\mathcal{O}_5$ as the center vertex and let its neighboring vertices be f_{5i}, where $i = 1, \ldots, 4$. The vertex membership values $\mathcal{V}_{\text{mem}}(f_{5i}) = n_{5i}$, $i = 1, \ldots, 4$, are 0.0099, 0.0189, 0.0585, and 0.2619, respectively. Let $\mathcal{V}_{\text{mem}}(\mathcal{O}_5) = o_5 = 0.5$. The edge membership values are computed as

$$\mathcal{E}_{\text{mem}}(\mathcal{O}_5 f_{5i}) = \min(o_5, n_{5i}), \qquad i = 1, \ldots, 4.$$

Hence,

$$\begin{aligned}
\mathcal{E}_{\text{mem}}(\mathcal{O}_5 f_{51}) &= \min(o_5, n_{51}) = \min(0.5, 0.0099) = 0.0099,\\
\mathcal{E}_{\text{mem}}(\mathcal{O}_5 f_{52}) &= \min(o_5, n_{52}) = \min(0.5, 0.0189) = 0.0189,\\
\mathcal{E}_{\text{mem}}(\mathcal{O}_5 f_{53}) &= \min(o_5, n_{53}) = \min(0.5, 0.0585) = 0.0585,\\
\mathcal{E}_{\text{mem}}(\mathcal{O}_5 f_{54}) &= \min(o_5, n_{54}) = \min(0.5, 0.2619) = 0.2619.
\end{aligned}$$

The resulting fuzzy graph is shown in Figure 10.

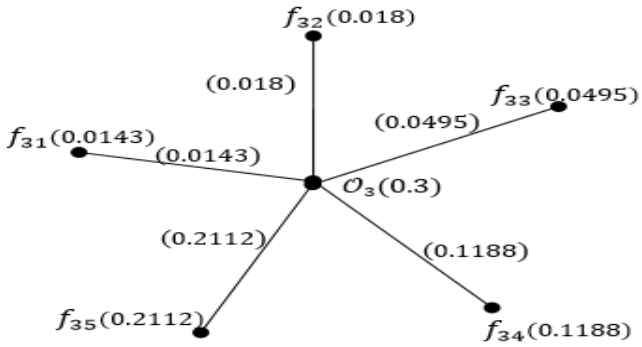

Figure 8: $L - F_{SN_2}$

Step 7: Using the $L - F_{SN_1}$, $L - F_{SN_2}$, $L - F_{SN_3}$,..., $L - F_{SN_k}$, frame three types of fuzzy graph networks based on the number of edges; the construction is explained in Section 3. Figure 11 is the $F_{GN_{Avg}}$.

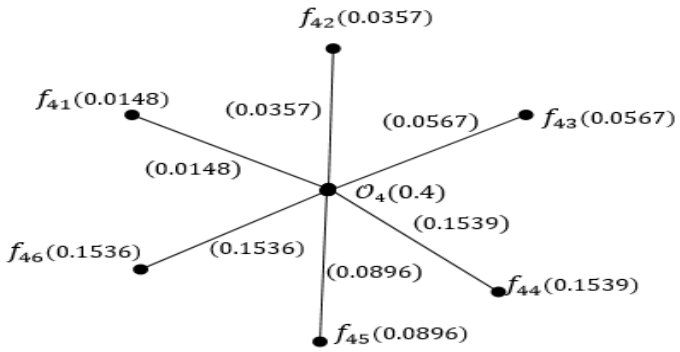

Figure 9: $L - F_{SN_4}$

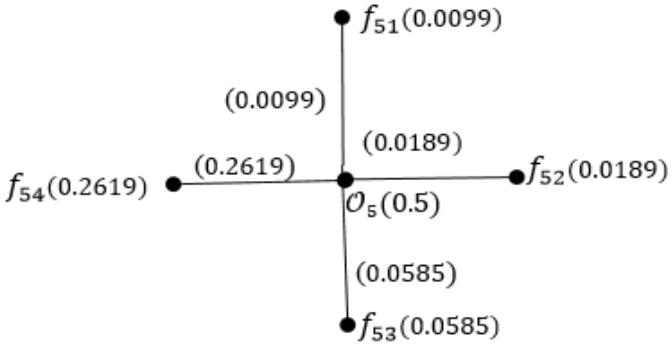

Figure 10: $L - F_{SN_5}$

4.2 Decryption algorithm

The final encrypted ciphertext generated by the proposed multi-layer encryption framework is used to reconstruct the original plaintext by the proposed decryption algorithm. The algorithm's input consists of the final ciphertext and the decryption parameters, such as the cryptographic keys and parameters for decrypting each layer. The result of the algorithm is the recovered plaintext, which is the same as the original message prior to encryption.
The decryption process is performed by reversing the encryption operations step by step, in the reverse order in which they were applied during encryption. The detailed steps of the proposed decryption algorithm are outlined below.
Input: $L - F_{GN}$
Output: $L - P_{Num}$

Step 1: Find the Efficient dominating members of F_{GN}, which are $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_k$. The neighbors of $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_k$ are f_{1i} ; $i =$ 1 to 7, f_{2i}; $i =$ 1 to 6, f_{3i}; $i =$ 1 to 5, f_{4i}; $i =$ 1 to 6, f_{5i}; $i =$ 1 to 4 respectively.

Step 2: The $\mathcal{V}_{mem}v(f_{1i}) = n_{1i}$; $i = 1$ to 7 which are 0.0119, 0.0396, 0.0572, 0.036, 0.0336, 0.0224 and 0.5632 respectively. $\mathcal{V}_{mem}v(f_{2i}) = n_{2i}$; $i = 1$ to 6 which are 0.0007, 0.003, 0.0432, 0.064, 0.1568, 0.192. $\mathcal{V}_{mem}v(f_{3i}) = n_{3i}$; $i =$ 1 to 5 which are 0.0143, 0.018, 0.0495, 0.1188, 0.2112. $\mathcal{V}_{mem}v(f_{4i}) = n_{4i}$; $i = 1$ to 6 which are 0.0148, 0.0357, 0.0567, 0.1539, 0.0896, 0.1536. $\mathcal{V}_{mem}v(f_{5i}) = n_{5i}$; $i = 1$ to 4 which are 0.0099, 0.0189, 0.0585, 0.2619.

Step 3: Find b_{1i} from n_{1i} ; $i = 1$ to 7 which are 119, 132, 143, 45, 21, 7, 88 respectively b_{2i}; $i = 1$ to 6 which are 7,10, 48, 80, 98, 60 respectively. b_{2i} ; $i = 1$ to 6 which are 7,10, 48, 80, 98, 60 respectively. b_{3i} ;$i = 1$ to 5 which are 143,66, 55, 44, 132 respectively. b_{4i} ; $i = 1$ to 5 which are 148,119, 63, 57, 56, 48 respectively. b_{5i} ; $i = 1$ to 4 which are 99,63, 65, 97 respectively.

Step 4: $PU_{key}(e, N)$ and $PR_{key}(d, N) =$ (23,165). Find a_{1i} from $b_{1i} = {a_{1i}}^e \ mod N$; $i = 1$ to 7 which are 22, 13, 21, 45, 77, 33, 17 respectively. Likewise find a_{2i}; $i = 1$ to 6 which are 15, 32, 5, 42, 20, 13 respectively. Find a_{3i}; $i = 1$ to 5 which are 33, 44, 55, 66, 77 respectively. Find a_{4i}; $i = 1$ to 6 which are 42, 56, 63, 72, 14, 37 respectively. Find a_{5i}; $i = 1$ to 4 which are 58, 65, 72, 99 respectively.

Step 5: From $a1i; i = 1$ to 7 , we get $L - P_{Num_1} = a_{11}a_{12}a_{13}a_{14}a_{15}a_{16}a_{17}$. From $a2i; i = 1$ to 6, we get $L - P_{Num_2} = a_{21}a_{22}a_{23}a_{24}a_{25}a_{26}$. From $a_{3i}; i = 1$ to 5 we get $L - P_{Num_3} = a_{31}a_{32}a_{33}a_{34}a_{35}$.
From $a_{4i}; i = 1$ to 6 we get $L - P_{Num_4} = a_{41}a_{42}a_{43}a_{44}a_{45}$. From $a_{5i}; i = 1$ to 4 we get $L - P_{Poly_5} = a_{51}a_{52}a_{53}a_{54}$, Finally the plaintext is $L - P_{Poly} = L - P_{Poly_1}/L - P_{Poly_2}/\ L - P_{Poly_3}/\ L - P_{Poly_4}/\ L - P_{Poly_5}$.

The correctness of the proposed framework is due to the deterministic and information-preserving nature of each transformation. The ciphertext is then encoded as a polynomial of whose coefficients uniquely represent the components of the ciphertext. Normalization process produces fuzzy values and keeps the coefficient information by means of predefined transformation parameters. These fuzzy values are then inputted to build the fuzzy network. In the decryption phase, the fuzzy network is deciphered to obtain the fuzzy values, and then they are renormalized to get the original polynomial coefficients and thus original RSA cipher text. Lastly, Multi-Prime RSA decryption decodes the plaintext. Hence, the sequence is reversible and if the necessary parameters and keys are known then the original plaintext could be recovered correctly.

Table 3: Comparative analysis of existing approaches and the proposed framework

Approach	**Main Security Mechanism**	**Representation of Encrypted Data**	**Key Limitation**	**Improvement in Proposed Framework**
RSA-Based Cryptographic Schemes	Integer factorization problem based on two-prime RSA	Numerical ciphertext	Security depends mainly on RSA structure; ciphertext remains purely numerical	Introduces polynomial and fuzzy-network representations to create additional abstraction layers
Multi-Prime RSA Schemes	Multi-prime modular arithmetic for improved computational efficiency	Numerical ciphertext	Focuses primarily on computational performance rather than structural security representation	Combines Multi-Prime RSA with graph-theoretic and fuzzy-network modeling
RSA–AES Hybrid Schemes	Public-key encryption combined with symmetric-key encryption	Numerical ciphertext and symmetric-key operations	Requires management of multiple cryptographic keys and remains independent of network structure	Incorporates network-based representation and domination concepts in addition to encryption
Graph-Based Encryption Models	Graph structures used for encoding and transmission of encrypted information	Graph representations	Generally do not address uncertainty associated with communication networks	Employs fuzzy graph networks capable of handling uncertainty through membership values
Fuzzy Graph-Based Security Models	Fuzzy membership values used to represent uncertain network relationships	Fuzzy graph structures	Limited integration with established public-key cryptographic algorithms	Integrates fuzzy graph modeling directly with Multi-Prime RSA encryption
Proposed Framework	Multi-Prime RSA, polynomial transformation, fuzzy graph modeling, and domination theory	Polynomial-based fuzzy network representation	Multi-stage construction requiring additional processing steps	Provides a multi-layer cryptographic framework combining algebraic, fuzzy, and graph-theoretic security mechanisms for enhanced reconstruction complexity

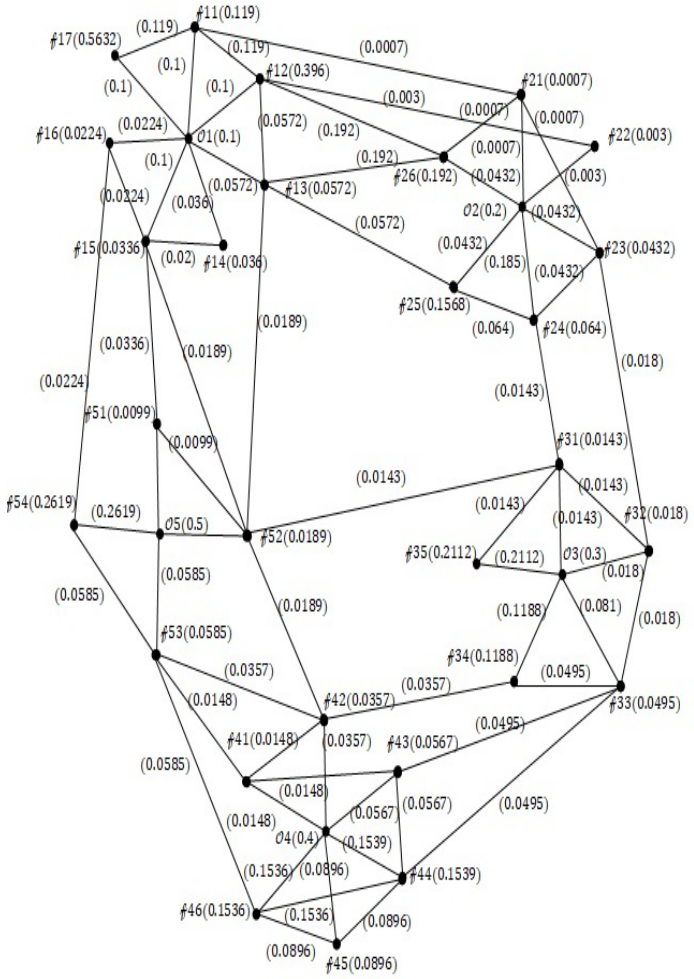

Figure 11: $L - F_{GN_{Avg}}$

A comparative analysis of existing approaches and the proposed framework is given above. The table contrasts the proposed solution with the RSA-based schemes, Multi-Prime RSA schemes, hybrid cryptographic schemes, and graph-based encryption models on the bases of security mechanism, data representation, limitations, and distinguishing features.

5 Flowchart of the proposed research work

5.1 Structural reconstruction

The proposed framework transforms the plaintext to encrypted numerical values by applying the multi-prime RSA mechanism first. These values are then used to construct the polynomial and it is part of the cryptographic key structure. This encrypted value is then mapped onto a fuzzy graph network, where the vertices and edges of the network have fuzzy characteristics. The domination parameters further provide identification of strategically important vertices which control and monitor the information flow in the network.
Therefore, the key to success in the reconstruction of the original message is to recover:

1. the encrypted numerical values,
2. the polynomial representation,
3. the fuzzy graph structure,
4. the domination characteristics of the network.

Because these components are interdependent the encrypted representation has greater structural complexity than any individual components in isolation. Thus, the proposed fuzzy graph network encodes information through domination parameters and polynomial transformations, adding another layer of representation.

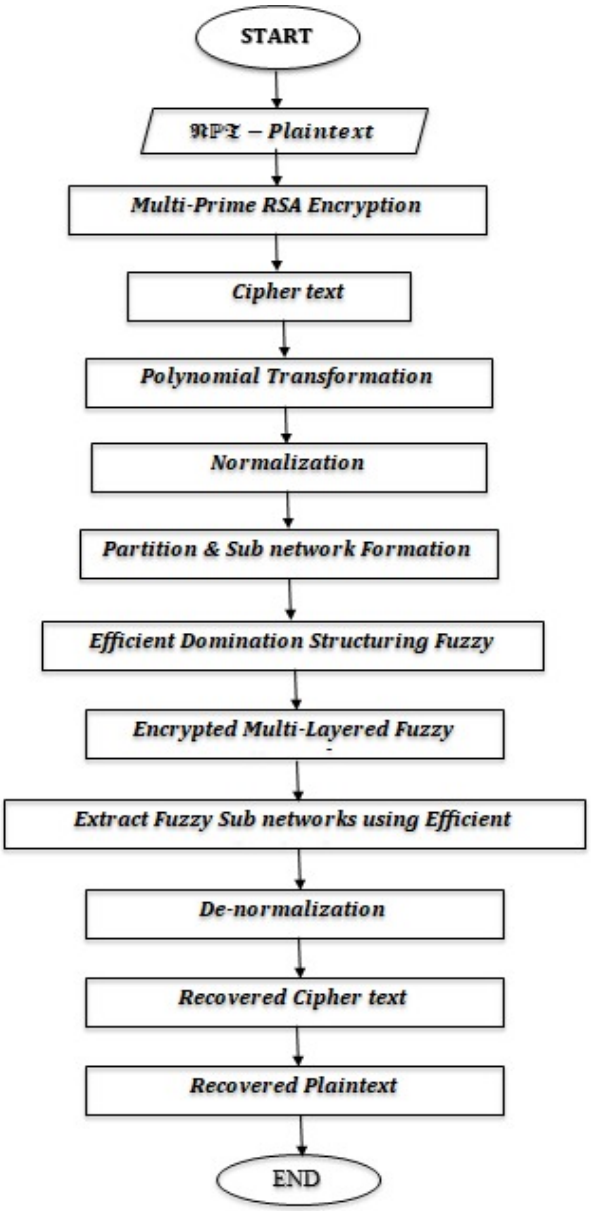

Figure 12: Flowchart

6 Applications

The proposed cryptographic structure has many practical merits for the security of modern communication networks. It can effectively solve uncertainty, dynamics of the network and changeable security threats by integrating fuzzy network modeling with advanced cryptographic techniques. The following is an overview of the main uses of the proposed framework.

(i) Dealing with Uncertainty in Secure Communication: Fuzzy networks handle partial trust, noisy communication channels, and uncertain communication environments. This is particularly beneficial in wireless, IoT, and distributed communication networks where the conditions of security are not purely binary.

(ii) Increasing Structural Security: The cryptosystem becomes more complex by using a fuzzy network to describe the

ciphertext or key elements. This multi-level description of the cryptosystem makes it more difficult for attackers to identify deterministic elements or reverse-engineer the key structure.
(iii). Dynamic Key Modeling: Fuzzy networks enable the use of graded relationships to describe keys instead of using fixed values. This enables dynamic or adaptive key modeling, which increases the unpredictability of the encryption process.
(iv) Fault-Tolerant Secure Communication: In cryptographic networks, fuzzy connectivity helps to ensure that even in the event of compromised or lost connectivity with some nodes, the overall secure communication network will still be able to function with reduced capability.
(v) Trust-Based Cryptographic Modeling: Fuzzy networks can model trust relationships between users or nodes. This is very important in blockchain networks, cloud security, and trust-based access control models, where trust is not absolute but rather a matter of degree.
(vi) Enhanced Resilience to Structural and Graph-Based Attacks: The introduction of fuzzy networks, which are based on graded relationships rather than absolute binary relationships, makes graph-based cryptanalysis and structural attacks less effective.

7 Structural security enhancement and threat model

This section provides an overview of the security improvements provided by the proposed cryptographic framework in terms of structure. The system combines graph-theoretic modeling with several cryptographic transformations to further enhance the security of the communication network against various attacks, including unauthorized access, ciphertext analysis, and structural attacks. The proposed methodology enhances the overall security by making the calculations more complicated, maintaining the confidentiality of the data, and using multiple layers of security during data transmission. The structural security properties are discussed in the next subsections for the proposed framework.

7.1 Structural security enhancement

The proposed framework assumes a passive adversary who can hear all the information transmitted in encrypted form and the fuzzy network representation. The attacker is supposed to be familiar with the general encryption method, which involves using Multi-Prime RSA, polynomial modification, normalization process, and fuzzy graph construction. The private decryption key, the partition information of the ciphertext, the normalizing parameters, however, and the network configuration based on domination are kept confidential. It can therefore be seen that the attacker can see the fuzzy network, but cannot get the original ciphertext without reconstructing the polynomial representation, recovering the fuzzy values, figuring out the structure of the network and getting the private RSA key. The fuzzy graph representation is an extra layer of abstraction in which the encrypted information is spread across several vertices and edges, via membership values. This makes it easier to detect unauthorized reconstruction, and gives an extra layer of security over the computational security given by the Multi-Prime RSA scheme.

7.2 Threat model

The proposed approach assumes that the adversary is passive and can intercept the ciphertext that is being sent and can also observe the graph network representation where the points are fuzzified. The adversary is assumed to know the encryption algorithm, without knowing the private key for decryption. This is based on the hardness of the multi-prime RSA problem. Moreover, the polynomial transformation and fuzzy graph representation add additional layers of complexity so it is harder for an illegal observer to reconstruct the original plaintext.

8 Conclusion

In this work, a new cryptographic framework, combining Multi-Prime RSA encryption, polynomial modeling, fuzzy graph networks and domination theory, is introduced in a single multi-layer security model. Multi-Prime RSA produces the output of the ciphertext as a polynomial representation and then fuzzy numbers are created from this polynomial representation for the construction of fuzzy domination based subnetworks. This multi-layered representation makes unauthorized reconstruction more complex, as it intertwines algebraic, cryptographic and graph-theoretic structures, all in one. The prime contribution of the study is the development of mathematical model of cryptographic encryption and fuzzy network representation and domination concepts. The approach suggested in this paper shows how information can be encrypted and represented and managed securely by using fuzzy graph structure and maintaining

the security of Multi-Prime RSA. The proposed framework is expected to be further developed in the following ways: computational complexity analysis, security metrics analysis, attack resistance studies, and performance comparison with other cryptographic methods, to name a few. The model can also be extended by incorporating other elements of intuitionistic fuzzy graph, neutrosophic fuzzy graph, dynamic network structure and post-quantum cryptographic tools to further extend its applicability and security.

Acknowledgement

The authors wish to express their appreciation for several excellent suggestions for improvements in this paper made by the referees.

References

[1] A. Alghafis, H. M. Waseem, M. Khan, S. S. Jamal, *A hybrid cryptosystem for digital contents confidentiality based on rotation of quantum spin states*, Physica A: Statistical Mechanics and its Applications, **554** (2020), 123908. https://doi.org/10.1016/j.physa.2019.123908

[2] K. Altarawneh, I. Altarawni, M. Almaiah, et. al., *A hybrid model of rsa and ntru for securing of cloud computing*, International Journal of Information Technology, **102**(07) (2024).

[3] E. Y. Baagyere, P. A. N. Agbedemnab, Z. Qin, M. I. Daabo, Z. Qin, *A multi-layered data encryption and decryption scheme based on genetic algorithm and residual numbers*, IEEE Access, **8** (2020), 100438-100447. https://doi.org/10.1109/ACCESS.2020.2997838

[4] D. W. Bange, A. E. Barkauskas, P. J. Slater, *Efficient dominating sets in graphs*, Applications of Discrete Mathematics, SIAM, Philadelphia, PA, USA, (1988), 189-199.

[5] A. Belazi, M. Khan, El-Latif, S. Belghith, *Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption*, Nonlinear Dynamics, **87** (2017), 337-361. https://doi.org/10.1007/s11071-016-3046-0

[6] D. Chen, *A feasible chaotic encryption scheme for image*, 2009 International Workshop on Chaos-Fractals Theories and Applications, (2009). https://doi.org/10.1109/IWCFTA.2009.43

[7] G. Cheng, J. Xia, L. Luo, H. Mi, D. Guo, R. T. B. Ma, *HyperPart: A hypergraph-based abstraction for deduplicated storage systems*, IEEE Transactions on Cloud Computing, **13**(1) (2025), 1-15. https://doi.org/10.1109/TCC.2024.3502464

[8] L. Chu, Y. Su, X. Zan, W. Lin, X. Yao, P. Xu, W. Liu, *A deniable encryption method for modulation-based DNA storage*, Interdisciplinary Sciences: Computational Life Sciences, **16**(4) (2024), 872-881. https://doi.org/10.1007/s12539-024-00648-5

[9] E. J. Cockayne, R. M. Dawes, S. T. Hedetniemi, *Total domination in graphs*, Networks: An International Journal, **10**(3) (1980), 211-219. https://doi.org/10.1002/net.3230100304

[10] B. Kaushik, V. Malik, V. Saroha, *A review paper on data encryption and decryption*, International Journal of Research in Applied Science and Engineering Technology, (IJRASET), **11**(4) (2023), 1986-1992. https://doi.org/10.22214/ijraset.2023.50101

[11] V. Kulli, D. K. Patwari, *Total efficient domination in graphs*, International Research Journal of Pure Algebra, **6**(1) (2016), 227-232.

[12] V. Kychak, V. Krasilenko, D. Nikitovych, *A cryptographic protocol for creating a joint secret key-permutation of significant dimension and its modeling*, The 3rd International Scientific and Practical Conference: Global Trends Develop. Educ. Syst., Bergen, Norway, Jan. 21-24, 2025.

[13] M. Y. Mahardika, A. Triayudi, *Comparative analysis of performance of the encryption and decryption times of cryptography*, SAGA: Journal of Technology and Information Systems, **2**(3) (2024), 304-310. https://doi.org/10.58905/saga.v2i3.359

[14] K. I. Masud, M. M. Hoque, U. D. Nath, et. al., *A new approach of cryptography for data encryption and decryption*, 5th International Conference on Computing and Informatics (ICCI), (2022), 234-239. https://doi.org/10.1109/ICCI54321.2022.9756078

[15] A. Meenakshi, A. Kannan, R. Cep, M. Elangovan, *Efficient graph network using total magic labeling and its applications*, Mathematics, **11**(19) (2023). https://doi.org/10.3390/math11194132

[16] A. Meenakshi, O. Mythreyi, L. Mrsic, A. Kalampakas, S. Samanta, *A fuzzy hypergraph-based framework for secure encryption and decryption of sensitive messages*, Mathematics, **13**(7) (2025), 1-20. https://doi.org/10.3390/math13071049

[17] J. Mehta, H. Rana, *Safest-value of the number of primes in RSA modulus and an improvised generalized multi-moduli RSA*, Mathematics, **13**(10) (2025), 1690. https://doi.org/10.3390/math13101690

[18] O. Ore, *Theory of graphs*, American Mathematical Society Colloquium Publications, **38**, Providence, RI, USA, 1962.

[19] A. Pius, D. R. Kirubaharan, *Application of cryptography in data privacy using fuzzy graph theory*, Journal of Discrete Mathematical Sciences and Cryptography, **24**(8) (2021), 1-10. https://doi.org/10.1080/09720529.2021.2014146

[20] A. Razaq, L. A. Maghrabi, M. Ahmad, F. Aslam, W. Feng, *Fuzzy logic-based substitution-box for robust medical image encryption in telemedicine*, IEEE Access, **12** (2024), 7584-7608. https://doi.org/10.1109/ACCESS.2024.3351794

[21] A. Rosenfeld, *Fuzzy graphs*, Fuzzy Sets and their Applications to Cognitive and Decision Processes, 1975. https://doi.org/10.1016/B978-0-12-775260-0.50008-6

[22] M. Shariatzadeh, M. J. Rostami, M. Eftekhari, S. Saryazdi, *An adaptive image encryption scheme guided by fuzzy models*, Iranian Journal of Fuzzy Systems, **21**(1) (2022), 1-18. https://doi.org/10.22111/ijfs.2023.44875.7915

[23] D. Wang, F. Yi, X. Li, P. Luo, Y. Dai, *On the analysis and generalization of extended visual cryptography schemes*, arXiv, (2006). https://doi.org/10.48550/arXiv.cs/0610172

[24] Q. Wu, J. Lu, *A secure model based on hypergraph in multilayer and multi-domain intelligent optical network*, Wireless Communications, Networking and Applications (WCNA), Springer, (2016), 35-40. https://doi.org/10.1007/978-81-322-2580-5-4

[25] L. A. Zadeh, *Fuzzy sets*, Information and Control, **8**(3) (1965), 338-353. https://doi.org/10.1016/S0019-9958(65)90241-X

[26] Q. Zhou, C. Chan, *Secret key generation for minimally connected fuzzy hypergraphical sources*, IEEE Transactions on Information Theory, **66**(7) (2020), 4226-4244. https://doi.org/10.1109/TIT.2020.2971215