Remark (3.8): For any two triangular t-$\mathbb{IFN}$ $A_t = \langle m, \alpha, \beta; \alpha', \beta' \rangle$ and $B_t = \langle n, \gamma, \delta; \gamma', \delta' \rangle$

1. The addition and subtraction of any two triangular t- $\mathbb{IFN}$ A_t and B_t is triangular t- $\mathbb{IFN}$ and is calculated in the following way:
   i. $A_t + B_t = \langle m + n, \alpha + \gamma, \beta + \delta; \alpha' + \gamma', \beta' + \delta' \rangle$
   ii. $A_t - B_t = \langle m - n, \alpha - \gamma, \beta - \delta; \alpha' - \gamma', \beta' - \delta' \rangle$
2. For any scalar λ, the scalar multiplication of λ and A_t is also triangular t- $\mathbb{IFN}$ and is determined as follows:
   i. $\lambda A_t = \langle \lambda m, \lambda\alpha, \lambda\beta; \lambda\alpha', \lambda\beta' \rangle$ for $\lambda > 0$
   ii. $\lambda A_t = \langle \lambda m, \lambda\beta, \lambda\alpha; \lambda\beta', \lambda\alpha' \rangle$ for $\lambda < 0$
3. The exponent of a triangular t-$\mathbb{IFN}$ is obtained as follows:
   i. $A_t^p = \langle m^p, pm^{p-1}\alpha, pm^{p-1}\beta; pm^{p-1}\alpha', pm^{p-1}\beta' \rangle$, where p is a positive integer.

I. Application of t-intuitionistic Fuzzy Subgroup to Cryptography

In this section, we develop a mechanism and present an algorithm in which we apply the concept of a t-$\mathbb{IFSG}$ to secure data using RSA modulus.

1. Generating Server Public and Private Keys:

i. Choose any two distinct prime numbers $\mathcal{p}$ and $\mathcal{q}$

ii. Calculate a modulus $\mathcal{n} = \mathcal{p}\mathcal{q}$ for both public and the private key

iii. Compute the totient function: $\varphi(\mathcal{n}) = (\mathcal{p} - 1)(\mathcal{q} - 1)$

iv. Choose an encryption exponent e such that $1 < e < \varphi(\mathcal{n})$ and $gcd(e, \varphi(\mathcal{n})) = 1$

v. Compute decryption exponent d which satisfies the following congruence

$$de \equiv 1\big(\mathrm{mod}\varphi(\mathcal{n})\big)$$

vi. The receiver sends the public key $(e, \mathcal{n})$ to the sender and retains the private key $(d, \mathcal{n})$

2. Encrypting the plain text:

i. The sender receives the public key $(e, \mathcal{n})$ of the receiver

ii. Represents the experimental message $\mathcal{s}$ into an integer or plain text $\mathcal{S}$ in view of table 1

Table 1. Experimental Message into the integer													
$\mathcal{s}$	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{C}$	$\mathcal{D}$	$\mathcal{E}$	$\mathcal{F}$	$\mathcal{G}$	$\mathcal{H}$	$\mathcal{I}$	$\mathcal{J}$	$\mathcal{K}$	$\mathcal{L}$	$\mathcal{M}$
$\mathcal{S}$	01	02	03	04	05	06	07	08	09	10	11	12	13
$\mathcal{s}$	$\mathcal{N}$	$\mathcal{O}$	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{R}$	$\mathcal{S}$	$\mathcal{T}$	$\mathcal{U}$	$\mathcal{V}$	$\mathcal{W}$	$\mathcal{X}$	$\mathcal{Y}$	$\mathcal{Z}$
$\mathcal{S}$	14	15	16	17	18	19	20	21	22	23	24	25	26

Table 1

iii. Compute a t-$\mathbb{IFSG}$ correspond to the set $\mathcal{S}$

iv. Determine the level subgroup of t-$\mathbb{IFSG}$

v. Compute the t-$\mathbb{IFN}$ of the level subgroup for the set of integers

vi. Obtain the triangular t-$\mathbb{IFN}$ from t-$\mathbb{IFN}$

vii. Compute ciphertext by using RSA encryption formula

$$\mathcal{CT} \equiv \mathcal{S}^e (\mathrm{mod}\, n)$$

viii. The sender sends the ciphertext in the form of triangular t-$\mathbb{IFN}$

3. Decrypting the cipher text:

i. The message is retrieved by employing the RSA decryption formula using a private key (d, n)

$$\mathcal{PT} \equiv \mathcal{CT}^d (\mathrm{mod}\, n)$$

And triangular t-$\mathbb{IFN}$ exponentiation operation is employed.

ii. The message is in triangular t-$\mathbb{IFN}$ form and is verified by applying the definition of congruence and subtraction of triangular t-$\mathbb{IFN}$

iii. Obtain t-$\mathbb{IFN}$ from triangular t-$\mathbb{IFN}$

iv. Obtain the set of integers

v. Obtain the plain text from table 1

The flowchart below clearly explains the RSA algorithm in the framework of t- t-$\mathbb{IFSG}$, which is adopted here.

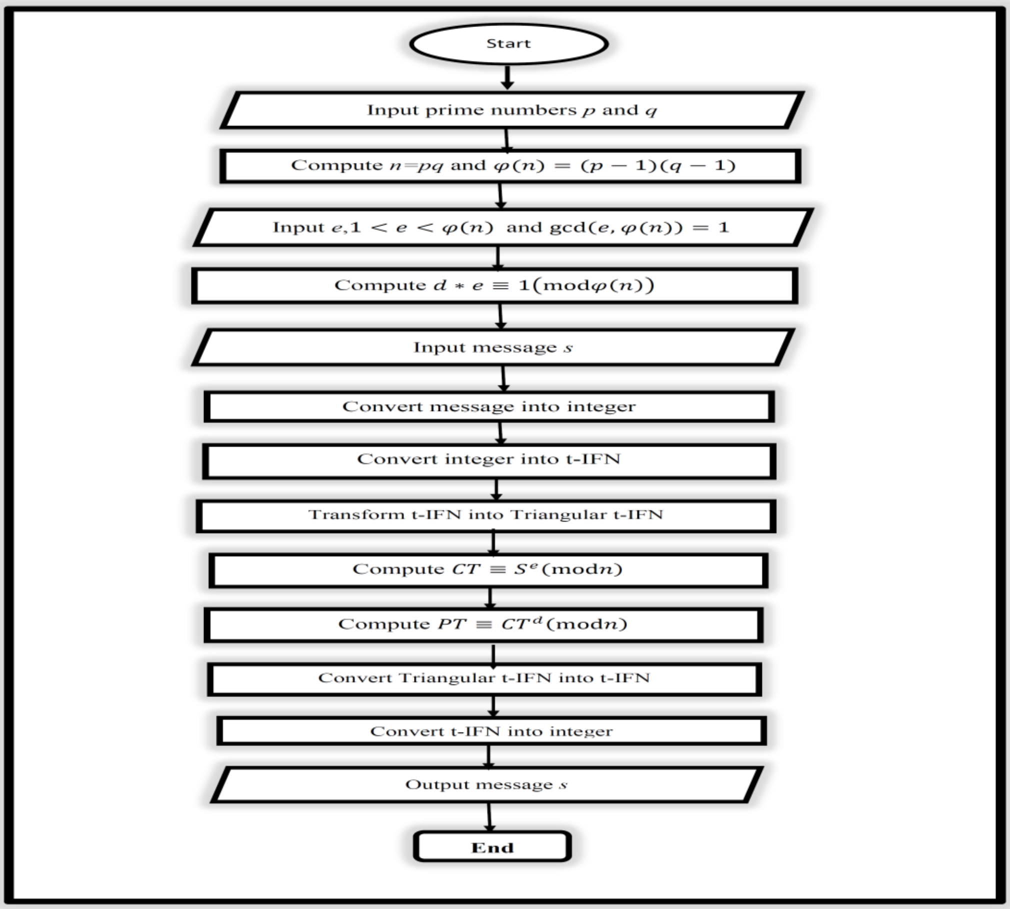

Fig 1. Flow chart of RSA Algorithm in the framework of t-$\mathbb{IFSG}$

4.1 Numerical Example of t-Intuitionistic Fuzzy RSA Algorithm:

In this section, we present a numerical example that illustrates the application of t-$\mathbb{IFSG}$ to encrypt and decrypt a message by using the t-intuitionistic fuzzy RSA module. The process of t-intuitionistic fuzzy RSA Cryptosystem consists of three steps: generate keys, encryption and decryption. The subsequent example depicts the mechanism of this method where an experimental message is "*Rose*".

1. **Generate public and private keys:**
   i. Choose two distinct prime numbers, such as $p = 5$ and $q = 11$
   ii. Compute $n = pq$ giving: $n = 55$
   iii. Compute $\varphi(n) = (p-1)(q-1)$ giving: $\varphi(55) = 40$
   iv. Choose any number $\boldsymbol{e}$, $1 < e < \varphi(n)$ and $\gcd\big(e, \varphi(n)\big) = 1$ such as $1 < e < 40$ and $\gcd(e, 40) = 1$ giving: $e = 7$
   v. Choose a suitable solution for d that satisfies $7d \equiv 1(mod40)$ giving: $d = 23$
2. **Encryption:**
   i. The public key is $(7{,}55)$ and the private key is $(23{,}55)$
   ii. The experimental message is taken as "Rose"

iii. Convert the experimental message into the set of integers: {18,15,19,05}

iv. Obtain a 0.7-$\mathbb{IFSG}$ correspond to the set $\mathcal{S}$ as follows:

$$\mu_{A_{0.7}}(z_1) = \begin{cases} 0.7 & \text{if } z_1 \in < 0 > \\ 0.5 & \text{if } z_1 \in < 2 > - < 0 > \\ 0.4 & \text{if } z_1 \in Z_{26} - < 2 > \end{cases} \text{ and } \nu_{A_{0.7}}(z_1) = \begin{cases} 0.3 & \text{if } z_1 \in < 0 > \\ 0.4 & \text{if } z_1 \in < 2 > - < 0 > \\ 0.5 & \text{if } z_1 \in Z_{26} - < 2 > \end{cases}.$$

v. Compute the $(0.4,0.5)$ $-$level subgroup of the above 0.7-$\mathbb{IFSG}$ as follows:

$$\hat{C}_{(0.4,0.5)}(A_t) = \mathcal{S}.$$

vi. In view of definition (3.2), 0.7-$\mathbb{IFN}$ of $\hat{C}_{(0.4,0.5)}(A_t)$ for the experimental message "Rose" is given by:

[1,1,18;1,19] [1,1,15;1,16] [1,1,19;1,20] [1,1,5;1,6]

vii. Transform the above 0.7-$\mathbb{IFN}$ into Triangular 0.7-$\mathbb{IFN}$:

<1,0,17;1,19> <1,0,14;1,16> <1,0,18;1,20> <1,0,4;1,6>

viii. Encrypt the Triangular 0.7-$\mathbb{IFN}$ using a public key as follows:

<1,0,9;7,23> <1,0,43;7,2> <1,0,16;7,30> <1,0,28;7,42>

3. Decryption:

i. The receiver receives the ciphertext in Triangular 0.7-$\mathbb{IFN}$:

<1,0,9;7,23> <1,0,43;7,2> <1,0,16;7,30> <1,0,28;7,42>

ii. Decrypt the ciphertext using a private key as follows:

<1,0,42;51,34> <1,0,54;51,46> <1,0,38;51,30> <1,0,39;51,31>

iii. Verify the ciphertext with plaintext modulo 55.

iv. The original message is in Triangular 0.7-$\mathbb{IFN}$ as follows:

<1,0,17;1,19> <1,0,14;1,16> <1,0,18;1,20> <1,0,4;1,6>

v. Convert Triangular 0.7-$\mathbb{IFN}$ into 0.7-$\mathbb{IFN}$:

[1,1,18;1,19] [1,1,15;1,16] [1,1,19;1,20] [1,1,5;1,6]

vi. Transform 0.7-$\mathbb{IFN}$ into the set of integers: {18,15,19,05}

vii. The plain text is "Rose".

VI. C++ Program to Implement the t-Intuitionistic Fuzzy RSA Algorithm

$\Rightarrow$ Intuitionistic Fuzzy subgroup (IFSG) (A) I

Defined on S

$S = \{1, 2, 3, 4, 5, \ldots, 26\}$

$$\mu_A(x) = \begin{cases} l & x \in \{26\} \text{ or } \{26\} \\ m & x \in \{2,4,6,8,10,12,14,16,18,20,22,24\} \text{ or } \langle 2 \rangle - \{26\} \\ n & x \in \{1,3,5,7,9,11,13,15,17,19,21,23,25\} \text{ or } S - \langle 2 \rangle \end{cases}$$

$$\nu_A(x) = \begin{cases} l' & x \in \{26\} \\ m' & x \in \{2,4,6,8,10,12,14,16,18,20,22,24\} \\ n' & x \in \{1,3,5,7,9,11,13,15,17,19,21,23,25\} \end{cases}$$

Here $l, m, n, l', m', n' \in [0,1]$ & $0 \le l + l' \le 1$, $0 \le m + m' \le 1$, $0 \le n + n' \le 1$

and $l \geq m \geq n$ and $l' \le m' \le n'$

$\Rightarrow$ t - Intuitionistic fuzzy subgroup (t-IFSG) (A_t)

Here $t \in [0,1]$

$$\mu_{A_t}(x) = \begin{cases} \min\{t, l\} = p & x \in \{26\} \\ \min\{t, m\} = q & x \in \{2,4,6,8,10,12,14,16,18,20,22,24\} \\ \min\{t, n\} = r & x \in \{1,3,5,7,9,11,13,15,17,19,21,23,25\} \end{cases}$$

II

$$\nu_{A_t}(x) = \begin{cases} \max\{1-t, l'\} = p' & x \in \{26\} \\ \max\{1-t, m'\} = q' & x \in \{2,4,6,8,10,12,14,16,18,20,24\} \\ \max\{1-t, n'\} = r' & x \in \{1,3,5,7,9,11,13,15,17,19,21,23,25\} \end{cases}$$

Here $p, q, r, p', q', r' \in [0,1]$ $\quad 0 \le p+q \le 1$

$p \ge q \ge r$ and $p' \le q' \le r'$ $\quad 0 \le q + q' \le 1$

$0 \le r + r' \le 1$

$\Rightarrow$ Level subgroup of t-IFSG.

(δ, η)-cut set of $A_t = \{x \in S : \mu_{A_t}(x) \ge \delta$ and $\nu_{A_t}(x) \le \eta\}$

where $\delta, \eta \in [0,1]$ and $0 \le \delta + \eta \le 1$

$\delta = \min\{p', q', r'\}$ and $\eta = \max\{p', q', r'\}$

we must obtain (δ,η)-level subgroup $= S$

⇒ t-IFN (t-Intuitionistic fuzzy number)

$$A_{t\text{-IFN}} = [m, \alpha, \beta : \alpha', \beta']$$

Here $m, \alpha, \beta, \alpha', \beta' \in \delta$

$$\alpha' \le \alpha \le m \le \beta \le \beta'$$

⇒ How to convert t-IFN into Triangular t-IFN:

Triangular t-IFN,

$$A_{Tr.\ t\text{-IFN}} = \langle m, 1-\alpha, 1-\beta ; \alpha', \beta' \rangle$$

$$= \langle m, 1-\alpha, 1-\beta : \alpha', \beta' \rangle$$

⇒ For encryption process

$$CT \equiv (PT)^e = (S)^e \bmod n$$

$$CT = \langle m, \alpha, \beta : \alpha', \beta' \rangle^e$$

$$= \langle m^e, em^{e-1}\alpha, em^{e-1}\beta ; em^{e-1}\alpha', em^{e-1}\beta' \rangle \bmod n$$

⇒ For decryption process

$$PT \equiv (CT)^d \bmod 77$$

$$PT = \langle m, \alpha, \beta : \alpha', \beta' \rangle^d$$

$$= \langle dm^d, dm^{d-1}\alpha, dm^{d-1}\beta ; dm^{d-1}\alpha', dm^{d-1}\beta' \rangle \bmod 55$$

$\Rightarrow$ For verification:- IV

In example, in decryption part (ii) the PT verify with decryption part (vii) (with linear congruence apply $ax \equiv b \bmod n$)

$$\langle 1,0,42;51,34\rangle x \equiv \langle 1,0,17;1,19\rangle \bmod 55$$

$$\langle x,0,42x;51x,34x\rangle \equiv \langle 1,0,17;1,19\rangle \bmod 55$$

verify if solution axists 'x'

$55 / (x-1)$ solution exists when $x=1$.

I use online linear congruencey calculator.