Secure RSA Variant System to Avoid Factorization Attack using Phony Modules and Phony Public Key Exponent

Raghunandan K R, Ganesh Aithal, Surendra Shetty

Abstract*: In cryptography Public key cryptography plays a significant job in the field of data communication. Public key uses two distinctive keys where keys are related so those, the public key can use to encode the information and private key is utilized to decode. RSA is considered as one of the effective algorithm in public key cryptography. Effectiveness of RSA Algorithm for the most part relies upon how adequately public key segments is shared i.e. common modulus n and public key exponent e. If these components compromised by the hacker using mathematical attacks, acquiring private key becomes easier task for the intruder. This paper present an upgraded RSA algorithm which is used to avoid the limitations of Integer factorization attack by improving the complexity of factorization process by utilizing fake/phony public key exponent type f rather than e and phony modulus X rather than n. Paper also gives comparative analysis of the proposed work using standard metrics.

***Index Terms*: Euler's function, Fermat factorization, Public key cryptography, Wieners attack**

I. INTRODUCTION

In Communication period protection of information assumes a significant job in our day today life. In this way, verifying data from eavesdroppers is real assignment. A cipher is a strategy for concealing data by supplanting unique letters with different letters, numbers and images through some sort of mathematical traps. Cryptography uses pair of procedures called scrambling/encryption and unscrambling / decryption. A Function which is utilized to change over the plain content to cipher content utilizing a key is called Encryption. Getting Plaintext again from cipher message by applying another mathematical function is called Decryption [1].

There are different approaches are used in cryptography depends on the keys what they are adopting in encryption and decryption.

A. Symmetric Key Cryptography

In data transmission, encryption side (Sender) and decryption side(Receiver) utilizes a similar keys for encoding the information and decoding of the information, it is called as Symmetric Key Cryptography.

Limitations: Security of this algorithm predominantly relies upon key age algorithm and the space used to represent the key utilized. If user uses weak key (size of the key is small) then it leads to less amount of time to obtain the key.

Proposed work center around public key cryptography by introducing improvement of the limitations of attacks on private keys of RSA

B. Asymmetric Key Cryptography

Asymmetric key also called as public key encryption. In this algorithm pair of related keys are utilized which can be gotten from an ensured specialist, key utilized for encryption capacity called Public key and another key utilized for decoding called private key. Any client needs to send any data at first he should utilize beneficiary's public key data from public catalog to encode the message. It is difficult to decode the encoded message by any individual who knows the public key, just the authentic client having the private key can unscramble original data.

An asymmetric-key cryptography procedure gives cryptography services like confidentiality, integrity, and authentication of message. Figure 1 explains asymmetric key cryptography.

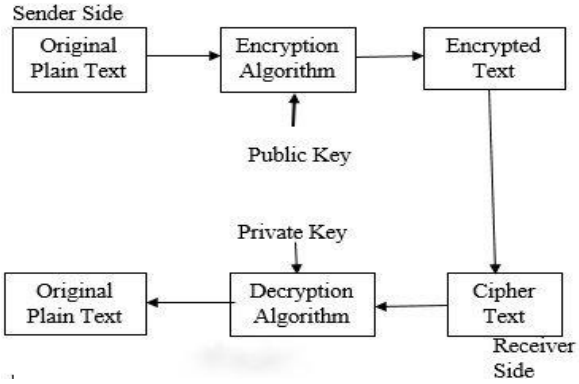

Fig. 1. Asymmetric Key Cryptography Process [16]

Public key algorithms are created dependent on some number theoretic idea which includes number-crunching tasks. Longer the keys and operands increasingly secure the algorithms is. RSA is considered as more secured, efficient and well-known Public Key Cryptosystem (PKC) which ruled public key cryptosystem from most recent 4 decades. RSA algorithm remains on the numerical capacities, for example, factorization, Euler totient work and modular exponent. During development of PKC discrete logarithms and integer factorization's are the regular issues [2].

Revised Manuscript Received on July 05, 2019.
Raghunandan K R, Department Of CSE, NMAM Institute Of Technology, Nitte, Affiliated to VTU, Karkala, Udupi, Karnataka, India.
Ganesh Aithal,, Department Of CSE, MITE, Moodabidre, Affiliated to VTU, Karnataka, India.
Surendra Shetty, Department Of MCA, NMAM Institute Of Technology, Nitte Affiliated to VTU, Karkala, Udupi, Karnataka, India.

The factorization issue was started in 1978, by Rivest, Shamir and Adleman during development of public key cryptosystem, known as RSA [3].

Processes used in RSA algorithms are, key generation, encryption and decryption. Key generation procedure includes, generation of Private keys by deducing the public key utilizing Euclidian algorithm. To get public key type e utilize Euler's totient function using the equation gcd(e, Ø(n))==1 and it should fall inside the range 1<e< Ø(n).

In this algorithm encryption process is purely based on the modulus of n and positive real integer value e and decryption process is based on private key exponent d and modulus n.

C. RSA Methodology

Select 2 large random (distinct) primes p and q. Compute the modulus n=p*q. Using Euler's totient function obtain ø(n)=(p-1)(q-1). Select random integer e which can satisfy the function GCD(e, ø(n))=1and it should fall between the range 1<e< ø(n). Private key component d can be computed using e×d mod ø(n)=1, and it should be in the range 1<d<ø(n). Now public key {n, e} shared publicly and private key {d} kept secret.

II. LITERATURE SURVEY

This section gives the idea about the work carried in the field of RSA by various researchers and their work along with the time complexity of the algorithm are listed

Cesar Alison and Monteiro Paixao proposed the concept of MPrime RSA, in that modular exponentiation that includes calculation of a big number of exponentiations that have a modulus that is reduced and exponents that are private. The complexity of this algorithm is O(log3N). This algorithm achieves a decryption speedup at the cost of extra modular exponentiations [4].

Cesar Alison and Monterio Paixao proposed R Prime RSA, in this they proposed combination of 2 variants of RSA. Here generation of key technique is borrowed from Rebalanced RSA and decryption technique is from M Prime RSA. Complexity of algorithm is O(s log2(n)/k).Gives better performance only for 1024 and 2048 bits moduli[5].

Takagi proposed a technique which computes based on the batch process and inverses of x and y, and he used modular inversion. Complexity used in this algorithm is O(b log n) where b is batch size. When public key exponents are small this batching technique is worthwhile otherwise extra operation required which leads to expensive [6].

Dan Boneh and Hovav Shacham proposed an algorithm called Multi-Power RSA. In this technique, encryption is same as Standard RSA. Complexity of this algorithm is O((n/r)3). The main limitation of this technique cannot be efficiently applied for usual sizes of N in RSA [7].

Akansha Tuteja and Amit proposed an algorithm which uses a phony modulus instead of the original one in order to make the decryption more secure. This algorithm is not secure against Weiner and Common Modulus Attack [8].

Kannan Balasubramanian proposed an algorithm called dependent RSA. A random integer f is introduced in the encryption and decryption computations. Complexity of this algorithm is O(|N|2,e x |e|2) .Against chosen cipher text attack this variant is secure [9].

Deepak Garg and Seema Verma proposed Rebalanced RSA, which uses the only two primes of n/k bits length during key generation and decryption algorithm uses Multi-Power RSA. Complexity of this algorithm is 0(log d log2 N). Here encryption involves high computational cost due to huge value of e [10].

By the survey it is clearly shown that, if s prime factor (n) and public exponent e shared publicly it is possible to obtain the secret key. Significant amount of computational power is required to obtain the prime factors, hence complexity of obtaining Private Key completely relayed on prime factors. An efficient technique is needed which gives solution to the factoring approach.

Next section we brief the technique of proposed RSA scheme along with numerical example. The remainder containing results and analysis section IV followed by conclusion.

III. MATHEMATICAL PRELIMINARIES

Groups are the essential parts of Abstract Algebra or Modern Algebra which is a part of Mathematics. In Abstract Algebra, we consider the components of the set that can be worked algebraically, for example consolidating two unique components of a set to get the third component.

Abelian groups are, if set G satisfies closure, associative, inverse, identity and commutative properties.

If a group generates all its elements using single elements then we refer it as cyclic group

A. Fermat's Little Theorem.

Let *p, q, r* and *s* be a prime number and *α* an integer. Then

$$\alpha\ p^{-1} \bmod p=1 \quad (1)$$

$$\alpha\ q^{-1} \bmod q=1 \quad (2)$$

$$\alpha\ r^{-1} \bmod r=1 \quad (3)$$

$$\alpha\ s^{-1} \bmod s=1 \quad (4)$$

Multiply (1) to (4) then equation we get,

$M(p-1)(q-1)(r-1)(s-1) \bmod (p\times q\times r\times s)=1.$

$$\text{Common modulus } n= p\times q\times r\times s \quad (5)$$

Using Euler's Totient function calculate Ø(n),

$$Ø(n)=(p-1) \times (q-1) \times (r-1) \times (s-1) \quad (6)$$

MØ(n) (mod n)=1 which is always equal to Mk*Ø(n) (mod n)=1k

Multiply M both side we get,

$$Mk*Ø(n)+1 \pmod n=M \quad (7)$$

B. Finding Phony Public Key Exponent

Upon computing the public key exponent e and private key exponent d of RSA,

Find an integer value k which satisfies the equation

$$(d \bmod k=0). \quad (8)$$

Find phony public key exponent f by multiplying integer value k to the actual public key exponent e,.

$$f=e*k. \quad (9)$$

Find phony private key exponent g by dividing integer value k from the actual private key exponent d,

$$g=d/k. \quad (10)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

C. Finding Phony Modulus

Modulus key *n* can be replaced by Phony modulus X, is a integer prime number which is greater than n and satisfies the equation.

$$(e*d) \bmod Ø(X)=1. \quad (11)$$

D. Factorization

Given a positive integer n ≥ 2, the prime factorization of n is written

$$n = p_1^{a1} p_2^{a2} \ldots\ldots p_k^{ak} = \prod_{i=1}^{k} p_i^{a^i} \quad (12)$$

Where p1,p2,⋯ ,pk are the k distinct prime factors of n, each of order ai ≥ 1. Furthermore, the factorization is unique.

All of the above theorems have an application in the following sections.

IV. PROPOSED MODEL

In normal RSA sending public key e directly help intruder to get d, because e is co- prime of Ø(n). It is needed to replace e for higher security. So that it is difficult to find private key.

Proposed System uses additional 2 variables in key generation process (f, g) which replace public key e and private d, where f is the multiplication of e and g is division of d. This algorithm hides the public key e from the intruder. And this algorithm also uses 4 prime numbers to calculate modulus n which will be difficult to factories Abbreviations and Acronyms

A. Proposed Algorithm

- Select 4 integer prime numbers *p1*, q_1, r_1, s_1 where $p_1 \neq q_1 \neq r_1 \neq s_1$.
- Calculate modulus *n* by multiplying the prime factors i.e. $n=p_1 \times q_1 \times r_1 \times s_1$ using equation *(5)*.
- Obtain *Ø(n)* using equation (6)
- Public key exponent *e* is calculated using, *gcd (e, Ø(n)) =1* and it should lies in between *1<e< Ø(n).*
- Find Private key exponent *d* which satisfies the equation *(e*d) mod Ø(n)=1*
- Continue the above process if *d* is not prime; otherwise select another *e* and *d*.
- Using equation (8) Find an integer *k* which satisfies the equation *(d mod k=0).*
- Find phony public key exponent *f* using equation (9).
- Find phony private key exponent *g* using equation (10).
- Obtain phony modulus using equation(11)
- Sender encrypts the plain text (*M*) by using the key pairs (*f, X)*

$$C=M^f \bmod X. \quad (13)$$

- On receiving cipher text receiver obtains the plain text (M) by using Private key pair (*g, X*) as,

$$M=C^g \bmod X. \quad (14)$$

B. Numerical Examples

Select four prime number p1=3, q1=5, r1=7, s1=11. Find n=p1*q1*r1*s1, hence n=1155. By using Euler's Totient equation (6) obtained Ø(n)= 480. Find e such that gcd(e, 480)=1 and 1<e< 48 0, hence we got e=47. Find d such that 47*d mod 480=1, then value of d will be 143. Find integer k using equation (8) which divides d, d/11=13 so, k=11. With the help of k public key f is obtained using equation (9) i.e. (47*11=517). Find private key g using equation (10), hence got g=143/11=13. Equation (11) gives phony modulus X =3361.

So public key (517,3361) shared to the sender by keeping private key (13,3361) secret.

Let P=123 be the plaintext during encryption sender calculates cipher text using the equation (13) obtained cipher value is 504, which is to be transmitted as cipher text to the receiver. Receiver obtains plain text back using the equation (14), i.e 504 13 mod 3361=123.

V. RESULTS AND ANALYSIS

A. Standard Deviation and mean

Standard deviation shows the difference or deviation of cipher values from the average value or variance [11] [16]. To calculate SD, we use the formula,

$$SD= \sqrt{\frac{\sum_{i=1}^{N}(E_i - V)^2}{N}} \quad (2)$$

Where Ei represents the cipher text value of plain text i, N is the number of character, V is variance or mean.

TABLE I. AVERAGE VALUE(MEAN)AND STANDARD DIVIATION FOR DIFFERENT FILE SIZES

File size	Mean	SD
10b	76.6	28.6782
100b	60.71	39.1631
1kb	61.7383	37.9576
10kb	62.1438	38.3347
100kb	61.7675	38.5933

Standard deviation and mean is calculated for the different data sets of different file sizes by keeping public key constant.

B. Execution time

Encryption time is calculated based on how much amount of time it elapsed to execute an encryption algorithm. Following table gives the results of RSA and Enhanced RSA schemes by comparing the encryption time for different file sizes by keeping same public key.

It illustrates that, for the lower bit length of prime numbers, two algorithms consume almost identical amount of time. But with the increase of bit length, the difference between curves rises rapidly.

TABLE II. EXECUTION TIME FOR DIFFERENT FILE SIZE SAMPLES

File size	RSA	MRSA
10b	129.5	68.6782
100b	109.1	59.1631
1kb	106.424	57.9576
10kb	107.617	58.3347
100kb	107.314	58.5933

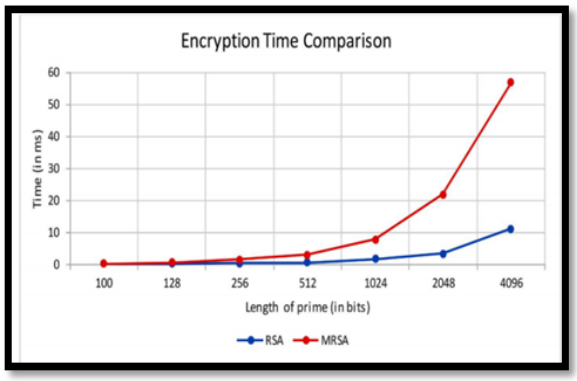

Fig. 2. Encryption time comparission (RSA v/s Proposed RSA)

The following graph demonstrates the identical amount of time consumed by RSA and Enhanced RSA (MRSA). With the increase of file sizess, the difference between curves rises rapidly.

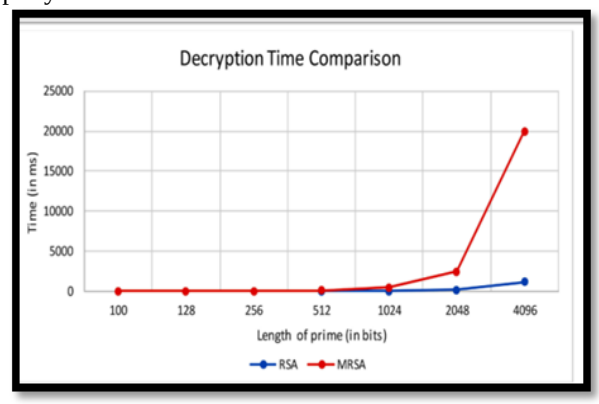

Fig. 3. Decryption time comparission (RSA v/s Proposed RSA)

C. Avalanche Effect

TABLE III. AVALANCHE EFFECT FOR ORIGINAL AND CHANGED PUBLIC KEY

Plain Text	Original P_k=517		Changed P_k =5	
	Encryption	Decryption	Encryption	Decryption
c	248	c	1414	·
i	3333	i	2939	!
p	3249	p	3217	û
h	2833	h	1431	╠
e	2068	e	1426	ȯ
r	3118	r	1929	ʐ

Avalanche effect is a measure used to find the security of any cryptographic algorithm. It gives the rate of change in cipher text by one-bit variation in public key [12][16]

Above table gives avalanche effect for the given input plain text cipher. The result shows when one bit flip in the public key (MSB) there will be tremendous change in the ciphertext, which will result in wrong result in decryption.

D. Histogram Analysis

A histogram is an accurate representation of the distribution of numerical data [16].

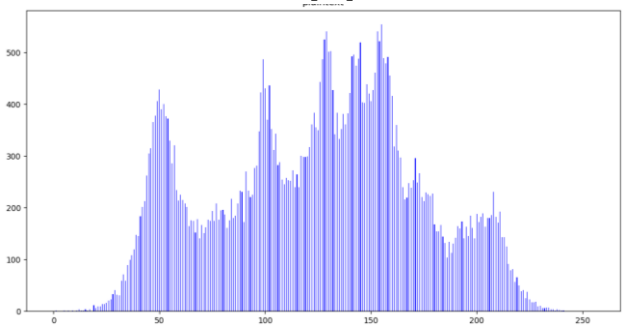

Fig. 4. Histogram of Plaintext

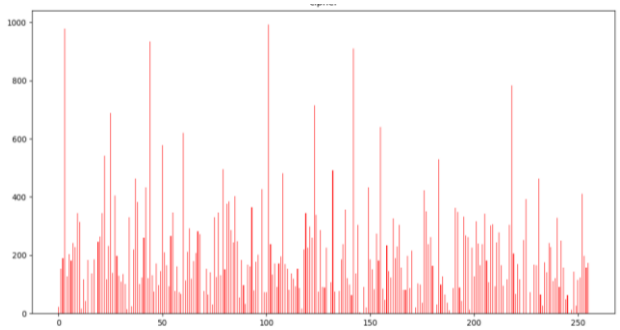

Fig. 5. Histogram of RSA cipher text

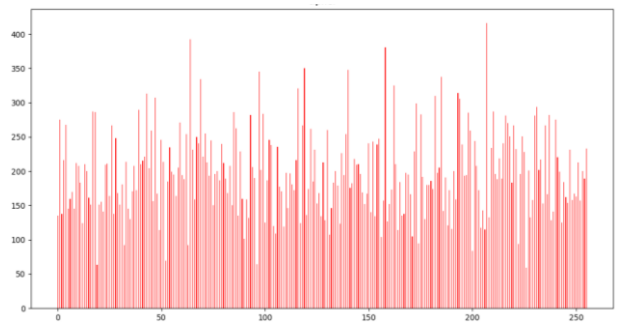

Fig. 6. Histogram of Modified RSA cipher text (MRSA)

By observing above histograms its clearly depicted modified RSA approach is better compared to normal RSA approach all the cipher texts are uniform probability distribution of cipher texts.

E. Security Analysis

In normal RSA only 2 prime numbers used but proposed model uses 4 prime numbers, which needs longer time to factorize the modulus n.

Also by introducing the concept of phony exponents and phony modulus attacks on RSA such as low private key exponent [13], low public key exponent [13], Wiener's attack [13], Common modulus attack [14], and Factorization attack [15] can be eliminated. Therefore, in terms of security, we can claim that proposed model is better compared to normal RSA.

TABLE IV. TIME REQUIRED

TABLE V. TO PERFORM THE ATTACK USING VARIOUS ATTACKING METHOD IN SECONDS

	Normal RSA	Modified RSA
Fermat's factorization	0.019000	855.6236587
Trail and Division	0.0131876	1860.551775
Weiner's attack	0.0172509	2984.09944

Table IV gives the comprehensive results of security attacks of proposed work and RSA, where the value of common modulus n of RSA replaced by Phony modulus X in proposed model. By the results, observed that the proposed method takes more time for each of the attacks which leads very difficult to crack using Fermat's factorization and Trial and Division attack and Wiener's attack.

F. Complexity Analysis

The time complexity is unit or the computation measure which gives the amount of time it elapses to run a function. This unit estimated based on the number of operation performed by the function under a fixed amount of time.

TABLE VI. COMPREHENSIVE ANALYSIS OF TIME COMPLEXITY (RSA V/S PROPOSED RSA)

Parameters	Normal RSA	Modified RSA
N	$O(n^2)$	$O(n^4)$
Φ(n)	$O(n^2)$	$O(n^4)$
E	$O(n^2 + O(\log n))$	$O(n^4 + O(\log n))$
D	O(log(n))	O(log(n))
F	-	$O(n^2)$
G	-	O(M(n))
Encryption	$O(\log(n)^2)$	$O(\log(n)^2)$
Decryption	$O(\log(n)^3)$	$O(\log(n)^3)$

Table V gives the comprehensive analysis of the time complexity of both RSA and Modified RSA approach for each step of operation it carried out during implementation stage.

VI. CONCLUSION

Proposed method try to introduce a Secure system for encryption so that present system will improve its performance automatically by large by concentrating more on security feature of RSA by keeping factorization attack of RSA in mind. Algorithm introducing 2 features, first one finding modulus n using 4 prime factors, second feature is the elimination of modulus n and public key exponent e from the original RSA by introducing phony modulus X and phony public key exponent's f.

This method will consider more security compared to RSA, by reducing encryption and decryption time. The histogram analysis of proposed method shows each letter has equal probability and uniformly distributed by making attacker difficult to guess the plaintext. Using Avalanche effect, we proposed on flipping one bit in public key, it is unable to decrypt the cipher text to get original plain text back. Anticipated algorithm eliminates the issue of mathematical attacks by providing more security to the algorithm with a slight increase in time complexity. Even though the proposed work uses secure cipher system with a limited security it has been worked out to get immunity more than that of the RSA.

REFERENCES

1. Diffie W. and Hellmann Martin, New direction in cryptography. IEEE Transaction on Information Theory, v.22, 1976, 644-654
2. Rivest R.L., Shamir A. and Adllemann L., A method for obtaining digital signature and public key cryptosystems. Comm. Of the ACM 21, 2 pp. 120-126 (1978).
3. H. C. WILLIAMS, A Modification of the RSA Public-Key Encryption Procedure pgno: 726-729, IEEE transactionon In-formation Theory.
4. S. Karthick, S. Perumal Sankar, and T. Raja Prathab. "An Approach for Image Encryption/Decryption Based on Quaternion Fourier Transform." In 2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR), pp. 1-7. IEEE, 2018.
5. Cesar Alison Monteiro Paixao, An efficient variant of the RSA cryptosystem, Institute of Mathematics and Statistics, University of Sao Paulo - Brasil.
6. T. Takagi. "Fast RSA-type Cryptosystem Modulo pkq." In H. Krawczyk, ed., Proceedings of Crypto 1998, vol. 1462 of LNCS, pp. 318–326. Springer-Verlag, Aug. 1998.
7. Dan Boneh and Hovav Shacham, Fast Variants of RSA.
8. AkanshaTuteja, Amit Shrivastava, Implementation of Modern RSA Variants, Department of Computer Science & Engineering, RGPV UniversitySVCE INDORE 452009, INDIA.
9. Kannan Balasubramanian Professor, Dept. of Computer Science and Engineering, Mepco Schlenk Engineering College, Variants of RSA and their Cryptanalysis.
10. Deepak Garg, Seema Verma on Improvement over Public Key Cryptographic Algorithm, 2009 IEEE International Advance Computing Conference (IACC 2009), Thapar University, Patiala, India.
11. G. Aithal, K. N. H. Bhat and U. Sripathi, "Implementation of stream cipher system based on representation of integers in Residue Number System," 2010 IEEE 2nd International Advance Computing Conference (IACC), Patiala, 2010, pp. 210-217
12. D.Ganga Raju, Kalla Kiran, "Analysis of Avalanche Effect in Asymmetric Cryptosystem Using NTRU & RSA", IJDCST, Vol. 1, Issue 6, October.
13. Thuc D. Nguye, Than Duc Nguyen, Long D. Tran, "Attacks on low private exponent RSA: an experimental study".
14. John McKeown, Grant Page, Ben Schoenfeld, "Attacks on RSA".
15. Dan Boneh, "Twenty Years of Attacks on the RSA Cryptosystem".

AUTHORS PROFILE

Raghunandan K R pursuing his Ph.D in the field of Public key Cryptography and working as Assistant professor in the Department Of Computer Science and Engineering, NMAM Institute Of Technology,

Nitte. He published around 12 Research Papers in the Field Of Cryptography.

Dr. Ganesh Aithal, working as Professor & Dean Research at Mangalore Institute of Engineering and Technology, Badaga Mijar, Moodabidri.– 574 225, South Canara, Karnataka – India. He is currently guiding 4 research scholars. The Research areas of interest are Cryptography and Securities -Random Number Generator, Stream Cipher System, Parallel Processing in the area of Cryptography, Public Key Cryptographic System and Securities in the area of Sensor Networks.

Dr. Surendra Shetty, Professor & Head had been awarded his doctoral degree for his research work "Audio Data Mining Using Machine Learning Techniques" in 2013 from university of Mangalore. He has published more than 25 research papers in different international journals and conferences. He is currently guiding six research scholars. Dr. Surendra Shetty authored two book chapters in different publications entitled "Machine Learning Approach for Carnatic Music Analysis" and "Applications of Unsupervised Techniques for Clustering of Audio Data". He has received research grant of 20 lakhs from VGST (GoK) for carrying out research on "Automatic Natural Language Processing and Speech Disorder Problems in Kannada Language". The Research areas of interest are Cryptography, Data mining, Pattern Recognition, Speech Recognition, MIS, Software Engineering and Testing.