Some Modification in ID-Based Public key Cryptosystem using IFP and DDLP

Chandrashekhar Meshram
Department of Applied Mathematics
Shri Shankaracharya Engineering College, Junwani,
Bhilai (C.G.), India

S.A. Meshram
Department of Mathematics
R.T.M.Nagpur University,
Nagpur (M.H.) India

***Abstract*— In 1984, Shamir [1] introduced the concept of an identity-based cryptosystem. In this system, each user needs to visit a key authentication center (KAC) and identify him self before joining a communication network. Once a user is accepted, the KAC will provide him with a secret key. In this way, if a user wants to communicate with others, he only needs to know the "identity" of his communication partner and the public key of the KAC. There is no public file required in this system. However, Shamir did not succeed in constructing an identity based cryptosystem, but only in constructing an identity-based signature scheme. Meshram and Agrawal [5] have proposed an id - based cryptosystem based on integer factoring and double discrete logarithm problem which uses the public key cryptosystem based on integer factoring and double discrete logarithm problem. In this paper, we propose the modification in an id based cryptosystem based on the integer factoring and double discrete logarithm problem and we consider the security against a conspiracy of some entities in the proposed system and show the possibility of establishing a more secure system.**

Keywords- Public key Cryptosystem; Identity based Cryptosystem; Discrete Logarithm Problem (DLP); Double Discrete Logarithm Problem (DDLP); Integer Factorization Problem (IFP).

I. INTRODUCTION

In an open network environment, secret session key needs to be shared between two users before it establishes a secret communication. While the number of users in the network is increasing, key distribution will become a serious problem. In 1976, Diffie and Hellman [6] introduced the concept of the public key distribution system (PKDS). In the PKDS, each user needs to select a secret key and compute a corresponding public key and store in the public directory. The common secrete session key, which will be shared between two users can then be determined by either user, based on his own secret key and the partner's public key. Although the PKDS provides an elegant way to solve the key distribution problem, the major concern is the authentication of the public keys used in the cryptographic algorithm.

Many attempts have been made to deal with the public key authentication issue. Kohnfelder [7] used the RSA digital signature scheme to provide public key certification. His system involves two kinds of public key cryptography: one is in modulo p, where p is a large prime number; the other is in modulo n, where n = p q, and p and q are large primes. Blom [11] proposed a symmetric key generation system (SKGS based on secret sharing schemes. The problems of SKGS however, are the difficulty of choosing a suitable threshold value and the requirement of large memory space for storing the secret shadow of each user.

In 1984, Shamir [1] introduced the concept of an identity. In this system, each user needs to visit a key authentication center (KAC) and identify himself before joining the network. Once a user's identity is accepted, the KAC will provide him with a secret key. In this way, a user needs only to know the "identity" of his communication partner and the public key of the KAC, together with his secret key, to communicate with others. There is no public file required in this system. However, Shamir did not succeed in constructing an identity-based cryptosystem, but only in constructing an identity-based signature scheme. Since then, much research has been devoted, especially in Japan, to various kinds of ID-based cryptographic schemes. Okamoto et al. [10] proposed an identity-based key distribution system in 1988, and later, Ohta [12] extended their scheme for user identification. These schemes use the RSA public key cryptosystem [18] for operations in modular n, where n is a product of two large primes, and the security of these schemes is based on the computational difficulty of factoring this large composite number n. Tsujii and Itoh [2] have proposed an ID- based cryptosystem based on the discrete logarithm problem with single discrete exponent which uses the ElGamal public key cryptosystem.

In 2004, Wei Bin lee & Kuan Chieh Liao [13] design a transformation process that can transfer all of the discrete logarithm based cryptosystems into the ID-based systems rather than reinvent a new system .After 2004 Several ID-Based cryptosystems [21,22,23, 24, 25, 26] have been proposed. But in these schemes, the public key of each entity is not only an identity, but also some random number selected either by the entity or by the trusted authority. Meshram [27] have also proposed Cryptosystem based on double generalized discrete logarithm problem whose security is based on double generalized discrete logarithm problem with distinct discrete exponents in the multiplicative group of finite fields. Meshram & Agrawal [4] have also proposed an ID- based cryptosystem based on the double discrete logarithm problem with double distinct discrete exponent which uses the Public key cryptosystem based on the double discrete logarithm problem.

Meshram and Agrawal [5] have proposed an id - based cryptosystem based on integer factoring and double discrete logarithm problem which uses the public key cryptosystem based on integer factoring and double discrete logarithm problem. Now we Modified this cryptosystem for integer factoring and discrete logarithm problem with distinct double discrete exponent because we face the problem of solving integer factoring and discrete logarithm problem simultaneously in the multiplicative group of finite fields as compared to the other public key cryptosystem. Where, we face the difficulty of solving the traditional discrete logarithm problem in the common group.

In this Study, we present modification in an ID based cryptosystem based on the integer factoring and double discrete logarithm with distinct discrete exponent (the basic idea of the proposed system comes on the public key cryptosystem based on integer factoring and double discrete logarithm problem) here we describe further considerations such as the security of the system, the identification for senders. etc. our scheme does not require any interactive preliminary communications in each message transmission and any assumption except the intractability of the discrete logarithm problem and integer factoring (this assumption seems to be quite reasonable)Thus the proposed scheme is a concrete example of an ID –based cryptosystem which satisfies Shamir's original concept [1] in a strict sense.

II. MODIFIED ID-BASED PUBLIC KEY CRYPTOSYSTEM

A. Implementation of the ID –Based Cryptosystem

1) Preparation for the center and each entity

Step 1: Each entity generates a k-dimensional binary vector for his ID. We denote entity A's ID by ID_A as follows

$$ID_A = \left(x_{A1}, x_{A2}, ..., x_{Ak}\right), x_{Aj} \in \{0,1\},\ (1 \le j \le k) \quad (1)$$

Each entity registers his ID with the center, and the center stores it in a public file.

Step 2: The center generates two random prime numbers p and q and compute

$$N = pq \quad (2)$$

Then the center chooses an arbitrary random number $e, 1 \le e \le \phi(N)$, such that $\gcd\left(e, \phi\left(N\right)\right) = 1$ where $\phi(N) = (p-1)(q-1)$ is the Euler function of N. Then center publishes (e, N) as the public key. Any entity can compute the entity $A's$ extended ID, EID_A by the following:

$$EID_A \equiv (ID)^e (\mathrm{mod}\, N)$$

$$= \left(y_{A1}, y_{A2}, ..., y_{At}\right), x_{Aj} \in \{0,1\} \quad , \quad (1 \le j \le t) \quad (3)$$

where $t = |N|$ is the numbers of bits of N.

Step3: *Center's secrete information:* - The center chooses an arbitrary large prime number p and q and compute $N = pq$ and also generated n-dimensional vector a and m-dimensional vector b over $z^*_{\phi(N)}$ which satisfies

$$a = \left(a_1, a_2, ..., a_n\right), b = \left(b_1, b_2, ..., b_m\right) \quad (4)$$

$$2 \le a_i b_l \le \phi(N) - 1,\ (1 \le i \le n), (1 \le l \le m), (m \le n)$$

$$abI \ne abJ (\mathrm{mod}(p-1)), I \ne J \quad (5)$$

Where I and J are n-dimensional binary vector and stores it as the centers secret information. The condition of equation (5) is necessary to avoid the accidental coincidence of some entities secrete key. A simple ways to generate the vectors a and b is to use Merkle and Hellmans scheme [19].

Step 4: The center also chooses w which satisfies $\gcd(w, \varphi(N)) = 1$ and $w < \lfloor \varphi(N)/n \rfloor$, where $\lfloor x \rfloor$ also denote the floor function which implies the largest integer smaller than compute x.

The center chooses a super increasing sequences corresponding to a and b as $a'_i (1 \le i \le n)$ & $b'_l (1 \le l \le m)$ satisfies

$$\sum_{j=1}^{i-1,l-1} a'_j b'_j + v \not\equiv \varphi(N), \text{ where } v = \lfloor \varphi(N)/w \rfloor \quad (6)$$

$$\sum_{j=1}^{n} a'_j b'_j \not\equiv \varphi(N), (m \le n) \quad (7)$$

Then the centre computes

$$a_i b_l = a'_i b'_l w (\mathrm{mod}\, \varphi(N))$$

$$c_i = a_i b_l (\mathrm{mod}\, w)(1 \le i \le n)(1 \le l \le m)(m \le n) \quad (8)$$

Where

$$a = \left(a_1, a_2, ..., a_n\right)\ b = \left(b_1, b_2, ..., b_m\right) \quad (9)$$

Remark 1: it is clear that the vector *a* and *b* defined by (9) satisfies (4)-(5) the above scheme is one method of generating n and m dimensional vectors a and b satisfies (4)-(5). In this paper, we adopt the above scheme. However, another method might be possible.

***Step 5*:** The center also chooses an unique integer d d, $1 \le d \le \varphi(N)$ such that $ed \equiv 1 (\mathrm{mod}\, \varphi(N))$ and arbitrary integer t such that $e = \left(e_1, e_2, ..., e_t\right)$, satisfying $\gcd(e_i, \varphi(N)) = 1,\ (1 \le i \le t)$ and compute n-dimensional and m- dimensional vectors D^j and D^k respectively:

$$D^j = (d^j_1, d^j_2, ... d^j_n)(1 \le j \le n)$$

$$d_l^j = e_l a_l (\mathrm{mod}\,\varphi(N))(1 \le l \le n) \quad (10)$$

$$D^k = (d_1^k, d_2^k, \ldots\ldots d_m^k)(1 \le k \le m)$$

$$d_l^k = e_l b_l (\mathrm{mod}\,\varphi(N))(1 \le l \le m)(m \le n) \quad (11)$$

Since D^j and D^k are one to one system.

Step 6: *Center public information:* The center chooses two arbitrary generators α and β of $Z^*_{\varphi(N)}$ and computes n-dimensional vector h using generator α & m-dimensional vector g using generator β corresponding to the vector a and b.

$$h = (h_1, h_2, \ldots\ldots\ldots, h_n),\ g = (g_1, g_2, \ldots\ldots\ldots, g_m) \quad (12)$$

$$h_i = \alpha^{a_i} (\mathrm{mod}\,N), (1 \le i \le n),$$

$$g_l = \beta^{b_l} (\mathrm{mod}\,N), (1 \le l \le m) \quad (13)$$

The center informs each entity (N, α, β, h, g) as public information.

Step 7 Each entity secrete key: Entity $A's$ secrete keys s_a and s_b are given by inner product of a and b (the centre's secret information) and EID_A (entity $A's$ extended ID, see eqn.3)

$$s_a \equiv d_l^j EID_A (\mathrm{mod}\,\phi(N))$$

$$= \sum_{1 \le j \le n} d_l^j y_{Aj} (\mathrm{mod}\,\phi(N)) \quad (14)$$

$$s_b \equiv d_l^k EID_A (\mathrm{mod}\,\phi(N))$$

$$= \sum_{1 \le j \le n} d_l^k y_{Aj} (\mathrm{mod}\,\phi(N)) \quad (15)$$

2) System Initialization Parameters

Center Secrete information

a : n -dimensional vector and b m-dimensional vector and d an integer {see (8)-(9)}

Center public information

h : n -dimensional vector & g m-dimensional vector {see eqn.(12-13)} p and q :large prime numbers, e : random integers , two generator α and β of $z^*_{\phi(N)}$.

Entity $A's$ secrete keys s_a and s_b = entity $A's$ public information = ID_A, k-dimensional vector

III. Protocol of the Proposed Cryptosystem

Without loss of generality supposes that entity B wishes to send message M to entity A.

A. Encryption

Entity B generates EID_A (Entity $A's$ extended ID, see eqn.3) from ID_A. It then computes γ_1 and γ_2 from corresponding public information h and g and EID_A.

$$\gamma_1 = \left(\prod_{1 \le i \le n} h_i^{y_{Ai}}\right)^{ei} (\mathrm{mod}\,N)$$

$$= \left(\prod_{1 \le i \le n} (\alpha^{a_i})^{y_{Ai}}\right)^{ei} (\mathrm{mod}\,N)$$

$$= \alpha^{\sum_{1 \le i \le n} ei\alpha i y_{Ai} (\mathrm{mod}\,\varphi(N))} (\mathrm{mod}\,N)$$

$$= \alpha^{\sum_{1 \le i \le n} d_l^j y_{Ai} (\mathrm{mod}\,\varphi(N))} (\mathrm{mod}\,N)$$

$$= \alpha^{sa} (\mathrm{mod}\,N)$$

$$\gamma_2 = \left(\prod_{1 \le l \le m} g_l^{y_{Al}}\right)^{el} (\mathrm{mod}\,N)$$

$$= \left(\prod_{1 \le l \le m} (\beta^{b_l})^{y_{Al}}\right)^{el} (\mathrm{mod}\,N)$$

$$= \beta^{\sum_{1 \le l \le m} el\beta_l y_{Al} (\mathrm{mod}\,\varphi(N))} (\mathrm{mod}\,N)$$

$$= \beta^{\sum_{1 \le l \le m} d_l^k y_{Al} (\mathrm{mod}\,\varphi(N))} (\mathrm{mod}\,N)$$

$$= \beta^{sb} (\mathrm{mod}\,N)$$

Entity B use γ_1 and γ_2 in Public key cryptosystem based on double discrete logarithm problem.

Let $M (1 \le M \le N)$ be entity B's message to be transmitted. Entity B select two random integer u and v such that $(2 \le uv \le \varphi(N) - 1)$ and computes

$$Y_1 = \alpha^u (\mathrm{mod}\,N)$$

$$Y_2 = \beta^v (\mathrm{mod}\,N)$$

$$\delta = M (\gamma_1)^u (\gamma_2)^v (\mathrm{mod}\,N)$$

$$= M(Y_1^{sa} Y_2^{sb}) (\text{mod } N)$$

And compute

$$C_1 = (Y_1)^e (\text{mod } N)$$

$$C_2 = (Y_2)^e (\text{mod } N)$$

$$E = (\delta)^e (\text{mod } N)$$

The cipher text is given by $C = (C_1, C_2, E)$.

B. Decryption

To recover the plaintext M from the cipher text

Entity A should do the following Compute

$$C_1^{\phi(N)-s_a} (\text{mod } N) = C_1^{-s_a} (\text{mod } N)$$

And $C_2^{\phi(N)-s_b} (\text{mod } N) = C_2^{-s_b} (\text{mod } N)$

Recover the plaintext $M = \left(C_1^{-s_a} C_2^{-s_b} E\right)^d (\text{mod } N)$

IV. Security Analysis

In this section, we shall show three possible attacks by which an adversary may try to take down the new encryption scheme. For each attack, we define the attack and give reason why this attack could be failed.

A. Direct Attack

Adversary wishes to obtain all secrete keys using all information available from the system. In this case, adversary needs to solve factoring and discrete logarithm problem with double distinct discrete exponent. The best way to factorize is by using the number field sieve method (NFS) [28].but this method is just dependent on the size of modulus n.It is computationally infeasible to factor a 1024-bit integer and to increase the security of our scheme; we should select strong primes [29] to avid attacks using special purpose factorization algorithms. To maintain the same security level for discrete logarithm problem with double distinct discrete exponent, one must uses with and respectively is product of two 512-bit primes.

B. Factoring Attack

Assume that the adversary successfully solves the factoring problem so that he knows secrete d. Thus he may obtain

$$\left(C_1^{-s_a} C_2^{-s_b} E\right)^d (\text{mod } N) = M^{ed} (\text{mod } N)$$

Unfortunately, at this stage he still does not knows secrete a and b and cannot extract the plaintext M from the above expression.

C. Discrete log Attack

An attacker should solve a discrete logarithm problem twice to obtain the private key given the public as following:

1) An attacker should solve a discrete logarithm problem twice to obtain the private key given the public as following:

In this encryption the public key is given by $\left(N, e, \alpha, \beta, \gamma_1, \gamma_2\right)$ and the corresponding secret key is given by $\left(s_a, s_b\right)$.

To obtain the private key $\left(s_a\right)$ he should solve the DLP

$$s_a \equiv \log_\alpha \left(\alpha^{s_a}\right) (\text{mod } N)$$

To obtain the private key $\left(s_b\right)$ he should solve the DLP

$$s_b \equiv \log_\beta \left(\beta^{s_b}\right) (\text{mod } N)$$

This information is equivalent to computing the discrete logarithm problem over multiplicative cyclic group $z^*_{\phi(N)}$ and corresponding secrete key s_a and s_b will never be revealed to the public.

2) An attacker might try to impersonate user A by developing some relation between w and w'

since $\gamma_1 \equiv Y^{ws_a} (\text{mod } N)$ and $\gamma_1' \equiv Y^{w's_a} (\text{mod } N)$

Similarly $\gamma_2 \equiv Y^{ws_b} (\text{mod } N)$ and $\gamma_2' \equiv Y^{w's_b} (\text{mod } N)$ by knowing $\gamma_1, \gamma_2, w, w'$ the intruder can derive γ_1' and γ_2' as $\gamma_1' = \gamma_1^{w^{-1}w'} (\text{mod } N)$ and $\gamma_2' = \gamma_2^{w^{-1}w'} (\text{mod } N)$ without knowing s_a and s_b however trying to obtain w from α and β is equivalent to compute the discrete logarithm problem.

V. Conclusion

In this study, some modification in an ID-based cryptosystem based on integer factoring and double discrete logarithm problem with distinct discrete exponents in the multiplicative group of finite fields. The proposed scheme satisfies Shamir's original concepts in a strict sense, i.e. it does not require any interactive preliminary communications in each data transmission and has no assumption that tamper free modules are available. This kind of scheme definitely provides a new scheme with a longer and higher level of security than that based on integer factoring and double discrete logarithm problem with distinct discrete exponents.

The proposed scheme also requires minimal operations in encryption and decryption algorithms and thus makes it is very efficient. The present paper provides the special result from the security point of view, because we face the problem of solving integer factoring and double and triple distinct discrete logarithm problem simultaneously in the multiplicative group of finite fields as compared to the other public key cryptosystem.

REFERENCES

[1] A. Shamir "Identity-based cryptosystem and signature scheme," Advances in Cryptology: Proceedings of Crypto' (Lecture Notes in Computer Science 196). Berlin, West Germany: Springer-Verlag, vol. 84 pp. 47-53,1985.

[2] S. Tsujii, and T. Itoh "An ID-Based Cryptosystem based on the Discrete Logarithm Problem"IEEE Jounral on selected areas in communications vol. 7 pp 467-473, 1989.

[3] T. ElGmal "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Trans. Inform. Theory, vol. 31, pp 469-472, 1995

[4] C.S.Meshram and S.S.Agrawal "An ID-Based Public key Cryptosystem based on the Double Discrete Logarithm Problem" International Journal of Computer Science and Network Security, vol.10 (7) pp.8-13,2010.

[5] C.S.Meshram and S.S.Agrawal "An ID-Based Public key Cryptosystem based on Integer Factoring and Double Discrete Logarithm Problem" Information Assurance and Security Letters, vol.1 pp.029-034,2010.

[6] W. Diffie and M.E. Hellman, "New direction in Cryptography", IEEE Trans.Inform.Theory, vol. 22, pp 644-654,1976.

[7] L. M. Kohnfelder, "A method for certification," Lab. Comput. Sci. Mass. Inst. Technol.. Cambridge, MA, May 1978.

[8] S. Tsujii, T. Itoh, and K. Kurosawa, "ID-based cryptosystem using discrete logarithm problem," Electron. Lett., vol. 23. no. 24, pp 1318-1320,1987.

[9] S. C. Pohlig and M. E. Hellman, "An improved algorithm for com puting logarithms over GF (p) and its cryptographic significance," IEEE Trans. Inform. Theory, vol. IT-24, pp. 106-110,1978.

[10] E. Okarnoto and K. Tanaka, "Key distribution system based on identification information," IEEE J. SeIecr. Areas Commun., vol. 7, pp.481485, May 1989.

[11] R. Blorn, "An optimal class of symmetric key generation systems." In Proc. Eurocryp '84, Pans, France, Apr. 9-11, pp. 335-338,1984.

[12] K. Ohta, "Efficient identification and signature schemes." Electron. Lett., vol. 24, no. 2, pp. 115-116,1988.

[13] Wei-Bin Lee and Kuan-Chieh Liao "Constructing identity-based cryptosystems for discrete logarithm based cryptosystems" Journal of Network and Computer Applications,vol. 27, pp. 191–199,2004.

[14] Min-Shiang Hwang, Jung-Wen Lo and Shu-Chen Lin "An efficient user identification scheme based on ID-based cryptosystem" Computer Standards & Interfaces,vol. 26,pp. 565–569,2004.

[15] Eun-Kyung Ryu and Kee-Young Yoo "On the security of efficient user identification scheme" Applied Mathematics and Computation 2005, vol.171, pp. 1201–1205.

[16] Mihir Bellare , Chanathip Namprempre and Gregory Neven "Security Proofs for Identity-Based Identification and Signature Schemes" J. Cryptol.,vol. 22, pp. 1–61, 2009.

[17] S. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms over GF (p) and its cryptographic significance," IEEE Trans. Inform. Theory, vol. IT-24, pp. 106-110,1978.

[18] R. L. Rivest, A. Shamir And L. Adelman, "A method for obtaining digital signatures and public-key cryptosystem," Comrnun. ACM., vol. 21, no. 2, pp. 120-126,1978.

[19] R. C. Merkle and M. E. Hellman, "Hiding information and signatures in trapdoor knapsacks" IEEE Trans. Inform. Theory, vol. IT- 24, pp. 525-530,1978.

[20] C.S.Laih and J.Y.Lee "Modified ID-Based Public key Cryptosystem using Discrete Logarithm Problem" Electronic Letters, vol.24 (14) pp.858-859,1988.

[21] Min-Shiang Hwang, Jung-Wen Lo and Shu-Chen Lin "An efficient user identification scheme based on ID-based cryptosystem" Computer Standards & Interfaces, vol. 26, pp. 565–569, 2004.

[22] Eike Kiltz and Yevgeniy Vahlis. "CCA2 Secure IBE: Standard model efficiency through authenticated symmetric encryption" In CT-RSA, Vol. 4964 of Lecture Notes in Computer Science, pp 221–239. Springer,2008.

[23] Raju Gangishetti, M. Choudary Gorantla, Manik Lal Das, Ashutosh Saxena "Threshold key issuing in identity-based cryptosystems" Computer Standards & Interfaces, vol.29, pp.260–264,2007.

[24] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang"An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks" IEEE Tran. On Parall. and Distributed Systems, vol.27, no.9,pp. 1227-1239,2010.

[25] Dan Boneh and Matthew K. Franklin. "Identity based encryption from the Weil pairing" SIAM Journal on Computing, Vol.32 (3), pp.586–615,2003.

[26] Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz "Chosen-ciphertext security from identity-based encryption" SIAM Journal on Computing,Vol.5(36), pp.1301–1328,2006.

[27] Chandrashekhar Meshram "A Cryptosystem based on Double Generalized Discrete Logarithm Problem" Int. J. Contemp. Math. Sciences,Vol. 6, no. 6, 285 -297,2011.

AUTHORS PROFILE

Chandrashekhar Meshram received the M.Sc and M.Phil degrees, from Pandit Ravishankar Shukla University, Raipur (C.G.) in 2007 and 2008, respectively and pursuing PhD from R.T.M. Nagpur University, Nagpur (M.H.) India. Presently he is teaching as an Assistant Professor in Department of Applied Mathematics, Shri Shankaracharya Engineering College, Junwani Bhilai, (C.G.) India. He is doing his research in the field of Cryptography and its Application. He is a member of International Association of Engineers, Hong Kong, Computer Science Teachers Association (CSTA)USA, Association for Computing Machinery (ACM) USA ,International Association of Computer Science and Information Technology (IACSIT), Singapore, European Association for Theoretical Computer Science (EATCS) Greece, International Association of Railway Operations Research (IAROR) Netherland, International Association for Pattern Recognition (IAPR) New York and International Federation for Information Processing (IFIP) Austria, International Mathematical Union , International Linear Algebra Society (ILAS) and Life -time member of Internet Society (ISOC) USA ,Indian Mathematical Society ,Cryptology Research Society of India and Ramanujan Mathematical Society of India (RMS). He is regular reviewer of ten International Journals and International Conferences.

Dr. (Mrs) S. A. Meshram received the MSc, M.Phil and PhD degrees, from R.T.M. Nagpur University, Nagpur (M.H.) India. Presently she is teaching as Associate Professor in Department of Mathematics, R.T.M. Nagpur University, Nagpur (M.H.) and is having 27 years of teaching experience postgraduate level in University. She is carrying out her research work in the field of Thermo elasticity, Solid Mechanics, Cryptography and its Application. Dr. Meshram published eighteen research papers in National and International Journals.