ISSN No. 0976-5697

Volume 4, No. 3, March 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Modified ElGamal over RSA Digital Signature Algorithm (MERDSA)

Kapil Madhur
M.Tech Student
Computer Engineering
S.B.C.E.T, Jaipur, India

Ruchi Patira
Assistant Professor
Information Technology
S.B.C.E.T, Jaipur, India

Abstract-Generally digital signature algorithms are based on a single hard problem like prime factorization problem, discrete logarithm problem, elliptic curve problem. If one finds solution of this single hard problem then these digital signature algorithms will no longer be secured and due to large computational power, this may be possible in future. There are many other algorithms which are based on the hybrid combination of prime factorization and discrete logarithms problem but different weaknesses and attacks have been developed against those algorithms. This paper also presents a new variant of digital signature algorithm which is based on two hard problems, prime factorization and discrete logarithm.

Keyword-Digital Signature; Discrete logarithm; Factorization; Cryptanalysis

I. INTRODUCTION

In modern cryptography [5], the security of digital signature algorithms are based on the difficulty of solving some hard number theoretical problems. These algorithms stay secure as long as the problem, on which the algorithm is based, stays unsolvable. The most used hard problems for designing a signature algorithm are prime factorization (FAC) [27] and Discrete Logarithm (DL) [6] problems. For improving the security, the algorithms may be designed based on multiple hard problems. Undoubtedly, the security of such algorithms is longer than algorithms based on a single problem. This is due to the need of solving both the problems simultaneously. Many digital signature algorithm have been designed based on both FAC and DL [8, 11, 12, 14, 17, 19, 26, 28, 30, 31] but to design such algorithms is not an easy task since many of them have been shown to be insecure [9, 18, 19, 20, 21, 29, 30, 31].

In 1994, He and Kiesler [11] proposed digital signature algorithms based on two hard problems-the prime factorization problem and the discrete logarithm problem. In 1995, Harn [9] showed that one can break the He-Kiesler algorithm if one has the ability to solve the prime factorization. Lee and Hwang [18] showed that if one has the ability to solve the discrete logarithms, one can break the He-Kiesler algorithm. Shimin Wei [31] showed that any attacker can forge the signature of He-Kiesler algorithm without solving any hard problem. In 2002, Z. Shao [28] presents an algorithm based on factoring and discrete logarithms. But later Tzeng [30] showed that Shao digital signature algorithm is not secure and there are many weaknesses. He then proposed a new signature algorithm [30] to overcome the weaknesses inherent in Shaos signature algorithm. In 2005, Shao [29] proved that Tzeng signature algorithm is not secure as if attackers can solve discrete logarithm problems, they can easily forge the signature for any message by using a probabilistic algorithm proposed by Pollard and Schnorr [24] and if attacker can factor the composite number, he can recover the private keys of legal signers. Therefore the security of Tzeng digital signature algorithm depends only one of the problem, prime factorization or discrete logarithm.

A signature scheme cannot be unconditionally secure, since Adv can test all possible signature for a given message m. So, given sufficient time, Adv can always forge Sender's signature on any message. Thus, our goal is to find signature schemes that are computationally or Provable secure. In this paper, a new variant of digital signature algorithm (DSA) is proposed which is based on the combined difficulties of integer factorization problem and discrete logarithm problem. Rest of the paper is organized as follows. Section II describes security threats against DL and FAC problem based algorithms. The proposed algorithm is described in section III. In section IV, security analysis is carried out for the proposed algorithm. Performance analysis of the proposed algorithm is discussed in section V. Finally, in section VI, paper is concluded.

II. SECURITY THREATS AGAINST DISCRETE LOGARITHM AND FACTORIZATION PROBLEM BASED ALGORITHMS

The ElGamal signature algorithm [6] is a digital signature algorithm which is based on the difficulty of computing discrete logarithms. The main threat against the ElGamal algorithm is that the strength of the algorithm solely depends on the discrete logarithm problem. If the discrete logarithm problem can be solved then it is possible to obtain the secret x from the public value gx, and then one could sign messages as a genuine sender. In 1993 Daniel M. Gordon presented an algorithm [7] that could solve discrete logarithms for small numbers in a finite field of prime order p, GF (p), using the Number Field Sieve. Takuya Hayashi [10] presented an algorithm that can solve a 676-bit Discrete Logarithm Problem in GF (36n) for n is any positive integer. It is clear from the work of Gordan and Hayashi that, in near future, it could be feasible to solve the discrete logarithms problem for large numbers in a polynomial time.

RSA Digital Signature algorithm (RSADSA) [27] proposed by Rivest, Shamir and Adleman, is a popular and well known digital signature algorithm. RSADSA is an asymmetric digital signature algorithm as it uses a pair of keys, one of which is used to sign the data in such a way that it can only be verified with the other key. Security of RSADSA algorithm is based on difficulty of solving the prime factorization problem. Many efforts have been made in past to solve the prime factorization problem [13, 23, 22, 25]. In 2002, Weger [4] described a new attack for solving prime factorization problem as if there is small difference between the prime factors of modulus then a polynomial time cryptanalysis for factoring modulus is possible. In 2003, Boneh and Brumley [1] demonstrated a more practical attack capable of recovering RSA factorizations over a network connection.

This attack takes advantage of information leaked by the Chinese remainder theorem optimization used by many RSA implementations. RSADSA is not only vulnerable to the prime factorization attacks but also to the private key d. Paul Kocher [16] described that if an Adversary Eve knows Alice's hardware in sufficient detail and is able to measure the decryption times for several known cipher texts, she can deduce the decryption key d quickly. Next, there are many threats if the RSA private exponent is chosen small. The first significant attack on small private exponent RSA was Wieners continued fraction attack [32]. Given only the public key (e, n), the attack factors the modulus using information obtained from one of the convergent in the continued fraction expansion of e/n. It was shown by Coppersmith [13], that an RSA modulus with balanced primes could be factored given only 1/2 of the most significant bits of one of the primes. It was later shown by Boneh, Durfee and Frankel [2] that 1/2 of the least significant bits of one of the primes was also sufficient. A theoretical hardware device named TWIRL designed by Shamir and Tromer in 2003 [15], questioned the security of 1024 bit keys. Nowadays due to the availability of high end resources of computation the chances of the various types of attacks have increased. It is quite possible that an organization with sufficiently deep pockets can build a large scale version of his circuits and effectively crack an RSA 1024 bit message in a relatively short period of time. The RSADSA algorithm is also forgeable for chosen-message attack, since RSA is multiplicative; the signature of a product is the product of the signatures.

III. THE PROPOSED SIGNATURE ALGORITHM

This section proposes a new variant of digital signature algorithm based on the two NP-Complete problems named prime factorization and discrete logarithm. Following are the formal definitions of the problems:

Definition 1: (Discrete Logarithm problem :) If $y = g^x \bmod p$ such that p is a prime number and g is a primitive root in Z_p^* and a, y, and p are given then finding the value of x is a discrete logarithm problem. If g, x, p are large numbers then it is a hard number theoretic problem [6].

Definition 2: Prime factorization problem: For a given composite number n, such that $n = p \times q$; where p and q are prime numbers, finding p and q is a prime factorization problem. If a large, b-bit number is the product of two primes that are roughly the same size, then no algorithm has been published that can factor in polynomial time, i.e., that can factor it in time $O(b^k)$ for some constant k.

A new digital signature algorithm based on combined application of DL and FAC is described as follows:

A. *Key Generation:*

a. Choose a large prime p such that computing discrete logarithms modulo p is difficult and two large prime numbers p_1 and q_1 such that $p < n$ where $n = p_1 \times q_1$.
b. Choose random numbers k and v such that $1 < k, v < p-1$.
c. Choose random number b such that $1 < b < n - 1$.
d. Choose a primitive root g in Z^p.
e. Calculate $\varphi(n) = (p_1 - 1) \times (q_1 - 1)$.
f. Choose e and x such that $e, x \in Z_{\varphi(n)}^*$.
g. Calculate d such that $d \times e \bmod \varphi(n) = 1$.
h. Calculate c such that $b^x \times c(\bmod)n = 1$.
i. Calculate u, w, and t* as follows: $u = g^k \bmod p$,
   $w = g^v \bmod p$,
   $t = u^w \bmod p$,
j. Public key is (e, x, c, g) and private key is (k, v, t, b, d).

B. *Signature Generation:*

Step-1: Choose an integer z such that $1 < z < (p - 1)$ and it is relative prime to $(p - 1)$ i. e. $\gcd(z, p - 1) = 1$. z should be different for every message m and is not public. Here H (.) is a one way hash function.

Step-2: Calculate

$$h = g^z \bmod p,$$
$$\gamma = t \times w^h \bmod p,$$
$$s_1 = H(m)^d \bmod n,$$
$$s_2 = (H(m) \times b^s1) \bmod n,$$
$$s_3 = ((((H(m) - kw - hv) \times z^{-1})) \bmod (p - 1)).$$

If $\gamma = 0$ and/or $s_1 = 0$ and/or $s_2 = 0$ and/or $s_3 = 0$ and/or $H(m) \equiv (kw + hv) \bmod (p - 1)$ then repeat step 1 and 2 else tuple $(\gamma, h, s_1, s_2, s_3)$ is the signature of m.

Here $-kw$, $-hv$ are additive inverse of kw and hv respectively and z^{-1} is the multiplicative inverse of z with respect to $\bmod(p - 1)$.

C. *Signature Verification:*

a. Calculates H(m) using the received message m at receiver's end.
b. If $g^{H(m)} \times s^{1\times x} \equiv (\gamma \times h^s3 \times s^2 \times c^s1 \bmod n) \bmod p$
   then the signature is valid else reject the signature.

D. *Proof of correctness:*

L.H.S. $=(gH(m) \times s^{1\times x}) \bmod p,$

$=(g^{H(m)} \times (H(m)^d \bmod n)^{e\times x}) \bmod p,$

$=(g^{H(m)} \times H(m)^x \bmod n) \bmod p,$

$=(g^{H(m)}) \bmod p \times (H(m)^x \bmod n) \bmod p,$

R.H.S. $=(\gamma \times h^s3 \times s^2 \times c^s1 \bmod n) \bmod p,$

$=((t \times w^h \bmod p) \times h^{((((H(m)-kw-hv)\times z}-1)) \bmod (p-1)) \times s^2 \times c^s1 \bmod n) \bmod p,$

$=(((u^w \bmod p \times w^h \bmod p) \times (g^{H(m)} \times u^{-w} \times w^{-h}) \bmod p) \times s^2 \times c^s1 \bmod n) \bmod p,$

$=(g^{H(m)} \bmod p \times ((H(m) \times b^s1) \bmod n)^x \times c^s1 \bmod n) \bmod p,$

$=(g^{H(m)} \bmod p \times ((H(m)^x \times b^s1^{\times x}) \bmod n) \times c^s1 \bmod n) \bmod p,$

$=(g^{H(m)} \bmod p \times H(m)^x \bmod n) \bmod p,$
$=g^{H(m)} \bmod p \times (H(m)^x \bmod n) \bmod p,$
$=$ L.H.S.

Therefore, L. H. S. is equal to R. H. S.

IV. SECURITY ANALYSIS

In this section, security analysis of the proposed algorithm is carried out. We shall show that the security of proposed algorithm is based on solving both the problem; prime factorization and discrete logarithm, simultaneously. It is observed that if an oracle O breaks the FAC and DL then it can break the proposed algorithm also, if given the public key of the scheme and a message m_{adv}

Theorem 1: If there is an ORACLE that can solve the prime factorization and discrete logarithm problem, then it can also break the proposed algorithm.

Proof: Let us the oracle O gives values of prime factor (p1, q1) of n and (k, v, z, w) from solving DL and FAC using (γ, h). We know that n = p1 × q1, and φ(n) is the Euler's totient function. Consider the equation

$$b^x \times c = \bmod n \qquad (1)$$

Where b and x ∈ Zn. Now from Diophantine equation for x and φ(n); ∃ u and v such that xu − φ(n)v = f , where f $\in Z_n$ .Now a sin the proposed algorithm gcd(x,φ(n))=1, so it is easy to solve equation (1) and the computation $b \equiv (^c)^u(\bmod\ )n$ gives the required value of b, since

b = (1/c)u mod n
= (1/c) 1+v_(n)x mod n;
= (1/c) 1/x mod n:

Further, consider the equation

$$d \times e \equiv 1 \bmod \varphi(n) \qquad (2)$$

where d is a private key element and e is a public key element. If Adv knows the prime factorization of modulus n then he can easily calculate φ(n) and hence using equation (2), private key d. Therefore, one can easily find the value of private key elements d and b.

Further, we know the value of z, k and v, hence the signature $(\gamma, h, s_1, s_2, s_3)$ of a message m_{adv}, can be generated as follows:

$$u = g^k \bmod p,$$
$$w = g^v \bmod p,$$
$$t = u^w \bmod p,$$
$$h = g^z \bmod p,$$
$$\gamma = t \times w^h \bmod p,$$
$$s_1 = H(m)^d \bmod n,$$
$$s_2 = (H(m) \times b^s 1) \bmod n,$$
$$s_3 = ((((H(m) - kw - hv) \times z^{-1})) \bmod (p-1)).$$

Therefore, the tuple $(\gamma, h, s_1, s_2, s_3)$ is a valid signature of message m_{adv} using the proposed algorithm.

There are some possible areas where an adversary (Adv) may try to attack on this new developed signature algorithm. Following are the possible attacks (not exhaustive) and the reasons why that would fail:

Key-Only Attack: Adv wishes to obtain private key (k, v, t, b, d) using all information that is available from the system. In this case, Adv needs to solve the prime factorization problem to find d and b from modulus $n = p_1 \times q_1$. Also he has to solve discrete logarithm problem to find z, k and v using γ, h and g. For finding b, Adv has to solve $b=c^{-1/x} \bmod n$ which is NP-Complete for large b because Adv has to find prime factorization of modulus n to calculate x^{th} root of c^{-1}. Further, d can also be calculated easily, if factorization of modulus n is known. Therefore an Adv has to solve DL problem and FAC problem for finding the private key. This makes the proposed algorithm secure enough for this type of attacks.

Chosen-Message Attack: In this attack, Adv requires a sign on some messages of his choice by the authorized signatory. With the help of chosen-messages and corresponding signatures, Adv generates another message and can forge sender's signature on it. The RSADSA algorithm is forgeable for this attack. For attack on RSADSA, suppose, Adv asks signer to sign two legitimate messages m1 and m2 for him. Let us assume s1 and s2 are signatures of m_1 and m_2 respectively. Adv later creates a new message $m = m_1 \times m_2$ with signature $s = s_1 \times s_2$. Adv can then claim that signer has signed m. The chosen-message attack for the proposed algorithm is a matter of further research as there is no obvious method which shows that the proposed algorithm is vulnerable to this attack.

Known partial key and Message Attack: Let us assume that Adv is able to solve FAC problem hence, he knows the secret key component b and d. Therefore Adv is able to calculate the signature element s_1 and s_2. Adv may also have i valid signatures $(\gamma_j, h_j, s_{1j}, s_{2j}, s_{3j})$ on message m_j where j = 1,2,...,i and public key (e,c,x,g) and he attempts to find secret keys (k, v, u, w, z_j). Now, Adv has i equations as follows representing z_{j-1} as l_j :

$$s_3 1 = ((H(m_1)l_1 - kwl_1 - hvl_1)$$
$$s_3 2 = ((H(m_2)l_2 - kwl_2 - hvl_2)$$
$$s_3 i = ((H(m_i)l_i - kwl_i - hvl_i)$$

In the above i equations, there are (i + 3) variables namely k,w,v and l_j where j = 1,2,...,i which are not known by the Adv. Hence, k, w, v and l_j stay hard to detect because for Adv, there are i+3 unknowns to be found from i equations.

Blinding: In this attack, in case of RSADSA suppose Adv wants sender's signature on his message m. For this Adv try the following: he picks a random $r \in Z^n$ and calculates $m' = r^e \times m \bmod n$. He then asks sender to sign the message m′. Sender may provide his signature s′ on the message m′. But we know that $s' = (m')^d \bmod n$. Adv now computes $s = s'/r \bmod n$ and obtains sender's signature s on the original m. This technique, called blinding, enables Adv to obtain a valid signature on a message of his choice by asking Sender to sign a random blinded message. Sender has no information as to what message he is actually signing. So, RSA is vulnerable to this attack. Again an intensive research is required to check whether the proposed algorithm is vulnerable to Blinding or not. Currently, best of authors' efforts it seems not vulnerable for Blinding.

V. PERFORMANCE ANALYSIS

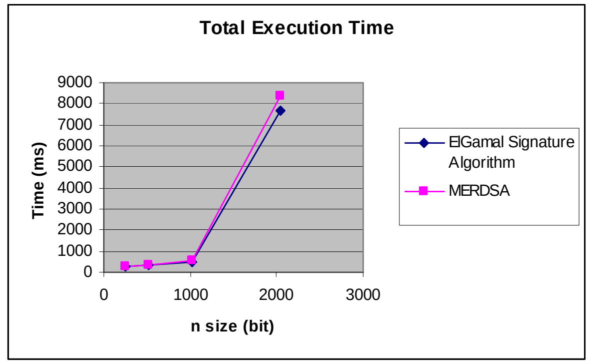
Using the criterion presented in [3], the complexity of each method is estimated as a function of number of bit operations required. The basic exponential operation here is $a^b \bmod n$ and time complexity of this operation is O (logb × M (n)), where M (n) is the complexity of multiplying two n bit integers. In the proposed algorithm signature generation requires 4 modular exponentiation and signature verification requires 5 modular exponentiation which leads to the complexity of the algorithm to be O(4 × $\log^3$n) and O(5 × $\log^3$n) for signature generation and verification respectively as here b = O(n) and time complexity of multiplying two n bit integers is O($\log^2$n). If the complexity of proposed DSA compared with other DSA algorithms of same category (i.e. DSA algorithms that are based on multiple hard problems) then we see that the Dimitrios Poulakis signature algorithm [26] requires 6 modular exponentiation in signature generation and 2 modular exponentiation in signature verification. Ismail E. S signature algorithm [14] requires 5 modular exponentiation in signature generation and 5 modular exponentiation in signature verification. Shimin Wei signature algorithm [31], requires 5 modular exponentiation in signature generation and 5 modular exponentiation in signature verification. So it is clear that the complexity of the proposed algorithm is competitive equivalent to most of the digital signature algorithms which are based on prime factorization and discrete logarithm.

A. Changing the Length/Size of the Prime Number (p) or Modulus (n):

Effect of Changing the Modulus Size with Constant Public Key Size (E) 512 Bit

n size (bit)	public key (e) size (bit)	d size (bit)	k,v,b and x size (bit)	ElGamal Signature Algorithm: Key Generation Time (ms)	Signature Generation Time (ms)	Signature Verification Time (ms)	Total Time (ms)	MERDSA Algorithm: Key Generation Time (ms)	Signature Generation Time (ms)	Signature Verification Time (ms)	Total Time (ms)
2048	64	2046	64	3406	281	16	3703	3468	594	344	4406
2048	128	2047	64	3625	282	15	3922	3687	594	344	4625
2048	256	2045	64	5813	282	32	6127	5875	594	375	6844
2048	512	2047	64	5968	282	78	6328	6037	594	390	7015

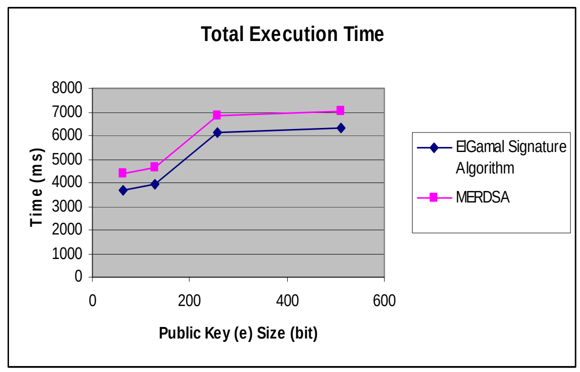
p size (bit)	n size (bit)	public key (e) size (bit)	d size (bit)	k,v,b and x size (bit)	ElGamal Signature Algorithm: Key Generation Time (ms)	Signature Generation Time (ms)	Signature Verification Time (ms)	Total Time (ms)	MERDSA Algorithm: Key Generation Time (ms)	Signature Generation Time (ms)	Signature Verification Time (ms)	Total Time (ms)
128	256	512	255	64	219	15	15	249	235	15	15	265
256	512	512	508	64	328	15	16	359	344	16	16	376
512	1024	512	1022	64	391	47	23	461	407	94	62	563
1024	2048	512	2047	64	7313	281	62	7656	7375	594	390	8359



Modulus (n) Size (bit) v/s Total Execution time (ms), taking Size of Public Key (e) 512 bit and k, v, b & x 64 bit.

B. Changing the Size of Public Key:

Effect of changing the public key (e) size on signature generation and verification time taking size of modulus size (n) 2048 bit.



Public Key (e) Size (bit) v/s Total Execution time (ms), taking Size of Modulus (n) 2048 bit and k, v, b & x 64 bit.

VI. CONCLUSION

In this paper, a new variant of digital signature algorithm is proposed which is based on the two hard problems called prime factorization and discrete logarithm. It is shown that one has to solve both the problems simultaneously for crypt-analysis of this algorithm. The performance of the proposed algorithm is found to be competitive to the most of the digital signature algorithms which are based on multiple hard problems.

VII. REFERENCES

[1]. D.Boneh and D. Brumley. Remote timing attacks are practical. Proceedings of 12th USENIX Security Symposium, 2003.

[2]. Boneh, G. Durfee, and Y. Frankel. Exposing an RSA private key given a small fraction of its bits. Full versionof the work from Asiacrypt, 98, 1998.

[3]. D. Boneh and H. Shacham. Fast variants of RSA. CryptoBytes (RSA Laboratories), 5:1-9, 2002.

[4]. B. De Weger. Cryptanalysis of RSA with small prime difference. Applicable Algebra in Engineering, Commu-nication and Computing, 13(1):17-28, 2002.

[5]. W. Diffie and M. Hellman. New directions in cryp-tography. Information Theory, IEEE Transac-

tions on,22(6):644-654, 2002.

[6]. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. Information Theory, IEEE Transactions on, 31(4):469-472, 2002.

[7]. M. Gordon. Discrete Logarithms in GF(P) Usingthe Number Field Sieve. SIAM Journal on DiscreteMathematics, 6(1):124-138, 1993.

[8]. L. Harn. Public-key cryptosystem design based onfactoring and discrete logarithms. In IEE Proc.-Compul.Digit. Tech, volume 141, pages 193-195. IET, 1994.

[9]. L. Harn. Comment: Enhancing the security of El Gamal'ssignature scheme. IEE Proceedings-Computers and Dig-ital Techniques, 142:376, 1995.

[10]. T. Hayashi, N. Shinohara, L. Wang, S. Matsuo, M. Shirase, and T. Takagi. Solving a 676-Bit Discrete Logarithm Problem in GF (3 6n). Public Key Cryptography-PKC 2010, pages 351-367, 2010.

[11]. J. He and T. Kiesler. Enhancing the security of ElGamal's signature scheme. In Computers and DigitalTechniques, IEE Proceedings-, volume 141, pages 249-252. IET, 1994.

[12]. W. H. He. Digital signature scheme based on factoring and discrete logarithms. Electronics Letters, 37(4):220-222, 2002.

[13]. M.J. Hinek. Cryptanalysis of RSA and its variants. Chapman & Hall/CRC, 2009.

[14]. ES Ismail, NMF Tahat, and RR Ahmad. A New Digital Signature Scheme Based on Factoring and Discrete Logarithms. Journal of Mathematics and Statistics, 4(4):222-225, 2008.

[15]. B. Kaliski.TWIRL and RSA Key Size.http://www.rsa.com/rsalabs/node.asp?id=2004,2003, Accessed on Nov. 2010.

[16]. P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Advances in Cryptology CRYPTO96, pages 104-113. Springer, 1996.

[17]. C.S. Laih and W.C. Kuo. New signature schemes based on factoring and discrete logarithms. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 80(1):46-53, 1997.

[18]. NY Lee. Security of Shao's signature schemes based on factoring and discrete logarithms. In Computers and Digital Techniques, IEE Proceedings-, volume 146, pages 119-121. IET, 2002.

[19]. N.Y. Lee and T. Hwang. Modified Harn signature scheme based on factorising and discrete logarithms. In Computers and Digital Techniques, IEE Proceedings-, volume 143, pages 196-198. IET, 2002.

[20]. N.Y. Lee and T. Hwang. The security of He and Kiesler'ssignature schemes. In Computers and Digital Techniques,IEE Proceedings-, volume 142, pages 370-372. IET, 2002.

[21]. J. Li and G. Xiao. Remarks on new signature scheme based on two hard problems. Electronics Letters, 34(25):2401, 2002.

[22]. P.L. Montgomery. A survey of modern integer factorization algorithms. CWI quarterly, 7(4):337-365, 1994.

[23]. M.A. Morrison and J. Brillhart. A Method of Factoring and the Factorization of F 7. Mathematics of Computation, 29(129):183-205, 1975.

[24]. J.M. Pollard and C.P. Schnorr. An efficient solution of the congruence x2+ ky2= m (mod n). IEEE Transactions on Information Theory, 33(5):702-709, 1987.

[25]. C. Pomerance. A tale of two sieves. Biscuits of Number Theory, page 85, 2008.

[26]. D. Poulakis. A variant of Digital Signature Algorithm. Designs, Codes and Cryptography, 51(1):99-104, 2009.

[27]. R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2):120-126, 1978.

[28]. Z. Shao. Signature schemes based on factoring and discrete logarithms. In Computers and Digital Techniques,IEE Proceedings-, volume 145, pages 33-36. IET, 2002.

[29]. Z. Shao. Security of a new digital signature scheme based on factoring and discrete logarithms. International Journal of Computer Mathematics, 82(10):1215-1219, 2005.

[30]. S.F. Tzeng, C.Y. Yang, and M.S. Hwang. A new digital signature scheme based on factoring and discrete logarithms. International Journal of Computer Mathematics, 81(1):9-14, 2004.

[31]. S. Wei. A New Digital Signature Scheme Based on Factoring and Discrete Logarithms. Progress on Cryptography, pages 107-111, 2004.

[32]. M.J. Wiener. Cryptanalysis of short RSA secret exponents. Information Theory, IEEE Transactions on, 36(3):553-558, 2002.

Short Bio Data for the Authors

Kapil Madhur was born on 19 September 1984.He is the M.Tech student in S.B.C.E.T, Jaipur (Rajasthan). He has completed **B.E**. (IT) in 2007 from University of Rajasthan, Jaipur.

Ruchi Patira is working as a assistant professor in S.B.C.E.T, Jaipur. He has 5 years teaching Experience. He has completed M.Tech. (CSE).