An approach on various Digital Signature Algorithms

Neha Sahu[1]*, Nitin Kali Raman[2] & Jyotika Pruthi[3]

[1]Assistant Professor, CSE/IT, The North Cap University, Gurgaon, India
*Corresponding Author E-mail: *nehasahu@ncuindia.edu*

[2]Assistant Professor, ECE, ACEM, Faridabad, India, E-mail: *nitinkaliraman21@gmail.com*

[3]Assistant Professor, CSE/IT, The North Cap University, Gurgaon, India
E-mail: *jyotikapruthi@ncuindia.edu*

Abstract: Due to rapid increase of electronic communication. It becomes necessary to secure the transmission through digital signature. This paper examines different algorithms for generation of digital signature. Here, some of the implementation methods are described to optimize signing procedure. RSA and its variations algorithm are reviewed for creation of digital signature whereas SHA algorithm is used for verification purposes. Also, different types of algorithms are compared on the basis of security, efficiency, and so on. Results show that best algorithm depends on security, complexity and other important factors.

Keywords: Digital Signature, Private Key, Public Key, RSA, SHA, Security, Signature Schemes

I. INTRODUCTION

A digital signature algorithmic program may be a public key scientific discipline algorithmic program created to guard the credibleness of a digital message or a document. A message is signed by a secret (Private) key to come up with a signature and so the signature is verified against the message by a public key. Therefore, anyone will verify the signatures however just one with the key key will sign the messages.

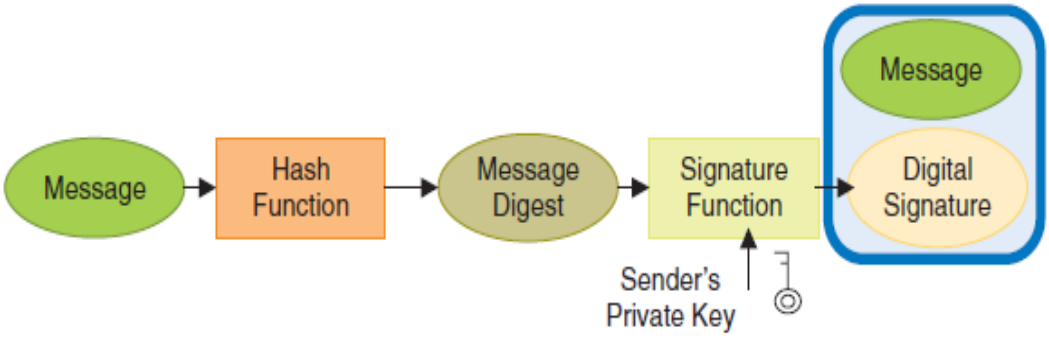

Figure 1.Digital Signature Generation

Digital signature proves its owner identity and he or she can't refuse his or her sign. As shown in figure 1, when original message is created by user and is sent for signing, then message is hashed and after performing private-key algorithm, digital signature is generated and is added to message as "Digital Signature". When user gets signed message, he or she can make sure that it is valid or not. This procedure known as verification is shown in figure 2 which is performed by public-key algorithms.

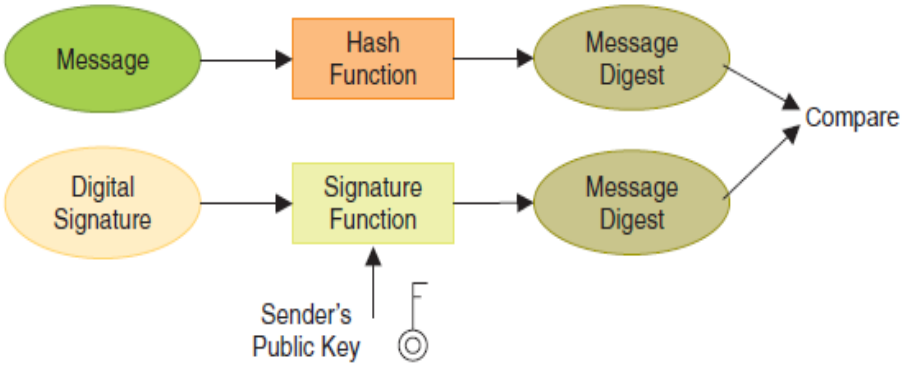

Figure 2. Digital Signature verification

II. LITERATURE REVIEW

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts, as well, for math, etc.

A. RSA Cryptosystem

As declared [1] that RSA is predicated on the principle that a number of the mathematical operations area unit easier to perform in one direction however the inverse is sort of tough while not some extra information within the case of RSA, the concept is that it's easier to multiply however way more tough to factorize [2]. Multiplication is worn out polynomial time whereas resolving time will grow exponentially proportional to the dimensions of the amount. Following steps generates Key:

- Choose two numbers as prime, x and y.
- cipher z=x*y, wherever z is that the modulus that's created public. The length of z is taken because the RSA key length.
- Random range 'p' is taken as a public key within the vary 0<p<(x-1)*(y-1) such gcd (p,(x-1)*(y-1))=1.
- Find personal key[3] k such p*k=1(mod (x-1)(y-1)).

Encryption:

- Consider the device A that must send some message to B securely [4].
- Let e be B's public key. Since p may be a public key, A will access 'p'.
- In order to encipher the message M, represent the message as associate degree number within the vary 0<M<z.
- Now, Cipher text C = M^p mod n, wherever n is that the modulus.

Decryption:

- Cipher text is received in the form of C from A.
- Calculate Message M = metallic element mod n, where d is B's personal key and n is that the modulus.

The working of the RSA is predicated on the following drawbacks: the matter of resolving massive numbers referred to as attack, hence the problem of idea all doable personal keys referred to as brute force attack [5]. Therefore so as to boost the protection, this concept presents a replacement algorithmic rule supported additive homomorphic properties referred to as changed RSA cryptography algorithmic rule (MREA)[6]. Consistent with [6] MREA is safe as compared to RSA because it is predicated on the resolving drawback. The theme is associate degree additive homomorphic cryptosystem; i.e. if solely the public-key is given and therefore the cryptography of 'm1' and 'm2', one will cipher the cryptography of M1 + money supply. This theme to boot presents a comparison between RSA and MREA cryp cryptosystems in terms of security and performance.

B. Proposed Scheme (MREA)

MREA is associate degree asymmetric-key algorithmic rule, i.e. for communication, two keys area unit needed: a public key and a personal key. Moreover, it's a way, i.e. the general public key's used solely to encipher, and therefore the personal key's used solely to decipher. Thus it cannot be used for authentication by cryptographic signing.

Here, a key generation algorithm for MREA cryptosystem is given. Here, a, b, c, d denotes four large prime numbers which are used to obtain the public key and the private key. Where 'x' and 'y' store the product of a,b and c,d respectively.

Key Generation Algorithm:

- Taking four values a,b, c and d which denote prime numbers randomly and independently of each other.
- All prime numbers should be of equivalent length.
- Calculate x = a x b, z= c x d, t=(a-1) x (b-1) and u=(c-1) x (d-1).
- Let 'p' be an integer, 1 < p < t, such that gcd (p, t) = 1.
- Calculate the secret exponent q, one < q < t, such that m x q mod t=1.
- Take associate degree number g wherever g=m+1.
- Compute the standard increasing inverse: v= (t^ -1) mod p.
- Public (encryption) key's (n, p, g, m).
- personal (decryption) key's (q, t, u).

Encryption:

- Assume m be a message to be encrypted wherever 0< mesg < n.
- Take random r wherever r < m.
- Generate ciphertext as: c=g^(mesg^e mod n)x r^m mod m^2.

Decryption

- Generate message: m = (((c^u mod m^2 – 1)/ m) x v mod m)d mod n.

Security analysis of MREA cryptosystem

Since the MREA cryptosystem relies on additive homomorphic properties and RSA, additive homomorphic theme neededfour prime numbers, it will be more durable and tedious to factorize twin modulus, thus one ought to factorize the dualmodulus into its four primes to separate the MREA algorithm [6]. If RSA, that's predicated on single modulus, is split in time x and additive homomorphic is tamed time y then the time needed to interrupt MREA formula is x*y. Thus, the protection of MREA formula is enhanced as compared to RSA formula and it shows that the MREA formula is immune for Mathematical attacks[5].
As just in case of MREA double decipherment is performed and in contrast to RSA that's not solely supported non-public key however is additionally supported the set total drawback thus one can't break MREA by solely guess the non-public key solely. Thus, it shows that MREA formula is safer as compare to RSA for brute force.

C. Method to Factorize the RSA Public Key Encryption

Plenty of algorithms are projected concerning resolving, the Pollard alphabetic character formula [7], and therefore the Pollard (p-1) formula [8], Brent's technique [9], ar probabilistic, and may not end, even for lowest values of N, but Trial division formula and projected technique will end all trivial and nontrivial values of N, shown in Table II.A resolving technique is projected by [10], that is employed to get the issue of positive whole number N that additionally reduces the time pass on. For coding (e, n) it transforms when public key for coding. It focuses on generation of a personal key as a result of the generation of personal secret's dependent Euler's totient perform $\phi(N)=(p-1)(q-1)$, p and letter is prime factors of N =p*q, p!=q, non-public key d=e-1mod(ϕ(N)), thus we have a tendency to ar last that if we will verify the prime factors of n, then we will simply generate non-public key. A changed Pierre de {fermat|mathematician} resolving(MFF) technique supported Fermat technique, during this technique resolve solely product of 2 prime numbers, by practice this technique; we will resolve quickly all positive range|number} number N, that is that the product of 2 prime numbers, MATLAB surroundings is employed for numerous analyses and nontrivial values of N, shown in Table II [10]. This technique isn't probabilistic. to interrupt RSA in to 2 prime numbers we should always have the merchandiseof that prime numbers is capable N. resolving of N is incredibly troublesome to seek out that prime. MFF will factors of N, that is P and letter, ar its individual prime factors. numerous steps concerned within the technique are as follows:

- Let N = P*Q.
- Compute X =ceil (sqrt (N)).
- Compute Y =sqrt (X^2 – N).
- If Y is whole number .
- Compute P =X – Y and letter =X + Y.
  Stop.
- Otherwise X →X +1, X+ 2,…. , X + 2*X, … X+ N.
- Carry on steps three to six, until Y is whole number.

Fig. 3 depicts a plot of your time move on and range of digits for given range by mistreatment ancient Trial technique, Pierre de Fermat factorization technique and projected MFF technique. The algorithmic rule was dead mistreatment MATLAB tool and Intel(R) core a pair of Quad processor, 2.66 GHz, 3.24 GB of RAM. RSA 1024 also can be break by mistreatment higher than projected technique desires 64-bits compiler [11]

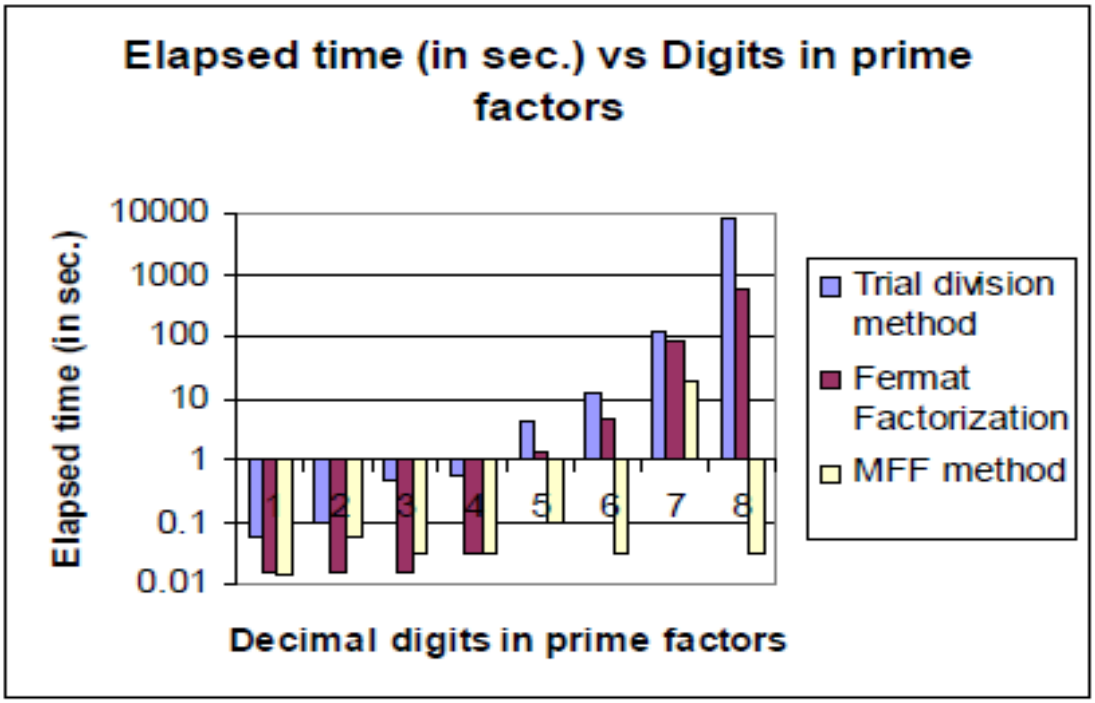

Figure. 3 Number of Digits vs. Elapsed time Prime Factors

In this paper associate degree algorithmic rule is projected for RSA modulus factorization. The new algorithmic rule aims to get the prime factors of modulus N in RSA algorithmic rule. During this technique [10] area unit dividing Pierre de Fermat factorization technique in 2 half initial is one is, factories range with respect ceiling operate of root of N, as a result of we tend to get most factors area unit neighbor to the that price, second is that if we tend to don't get positive number price of root (square root of N), then we tend to sequence between ceil (sqrt(N)) to N. Shown in Figure three, time period for prime factorization area unit decreasing as compare to the Pierre de Fermat and trial division technique. Therefore, we tend to area unit last, if we discover factor of decipher to the key message. RSA Modulo N, then we are able to generate personal key and decipher to the key message. This algorithmic rule is comparatively straightforward and ascendable. MFF technique for factorization of positive number N, terribly useful to get results at economical and quicker rate.

D. High Throughput Hardware Implementation of Secure Hash Algorithm (SHA-3)

[12] shows area unit associate degree application of a secure hashing algorithmic rule for securing the documents. Secure hashing algorithmic rule uses a cryptological operate that may be a settled procedure whose takes associate degree arbitrary block of information and offers a fixed-size bit string, that is termed because the (cryptographic) hash price. The paper represents a high outturn economical hardware implementation of the ultimate spherical candidate of SHA-3: Blake. the info to be hashed is termed because the "message", and therefore the hash price generated is termed because the message digest or just the digest. A hash price H of plaintext M is made by a hash operate h wherever H=h(M).

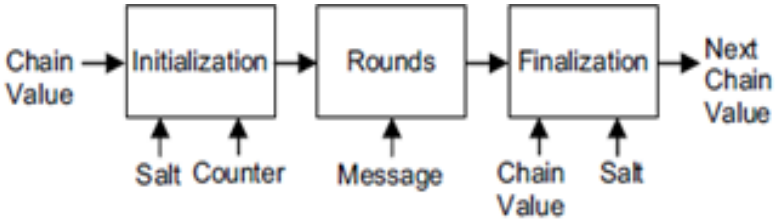

Figure. 4. Construction of BLAKE's compression function.

The cryptological hash operate having the inputs M,M' and therefore the outputs H,H' should have the subsequent properties:

• Simplicity: It ought to be easier to cipher the hash price for a given message M.

• Pre image Resistance: It ought to be terribly exhausting to seek out a message that features a given equivalent hash.

• Second Pre image Resistance: It ought to be tough to seek out another input message such each messages area unit having constant Hash price.

• Collision Resistance: It ought to be tough to seek out 2 totally different messages having constant hash price .This property is additionally spoken as 'strong collision resistance'.

• Input Sensitivity: Message modification ought to be unfeasible while not dynamical its hash.

III. IMPLEMENTATION

The design is completely autonomous with an entire I/O interface. This approach is business to common development surroundings, having same style methodology and mistreatment same set of chip resources.

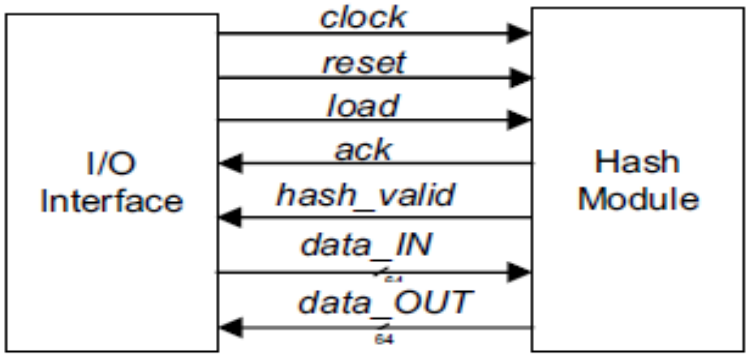

Figure 5. Input/ Output Interface

In I/O interface, all I/O transactions area unit synchronous every of the I/O is examined at the rising fringe of clock pulse. The input cycle is started by I/O interface by setting the load signal [13] to high. Hash Module acknowledges the request if it's receiving the knowledge by setting ack signal to high. And whereas transacting the info, ack. signal maintains it at logic high. once needed quantity of input is received, Hash Module resets the ack signal to low. Consequently, I/O interface additionally pulls the load signal to low, if no any transactions area unit needed. If message blocks area unit still there, load signal can stay at logic high however Hash Module can acknowledge it solely when one clock cycle from the previous dealing. Hash module has 2 vital components, initial the management path and second the info path

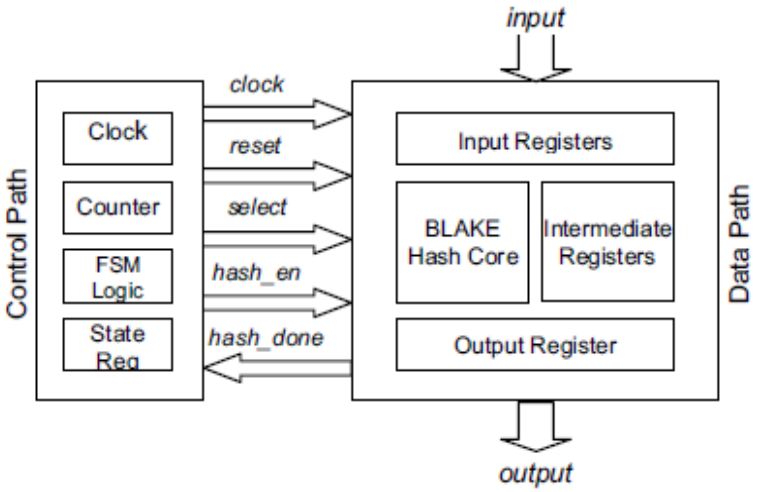

Figure. 6. Different control and data paths represented in hash module

In this work [12] have tried to gift the economical hardware implementation of SHA-3 finalist: Blake and even have reportable the performance figures that's the potency of implementation in respect of space, outturn and outturn per space and additionally compared it with last reportable implementation results. Results gathered during this work area unit surpassing the performance reportable thus far. [12] have used the 256-bit variant of Blake for the economical implementation. different variants like 224, 384 and 512, are gift as such that by bureau for SHA-3. Gift work is changed for of these variants.

IV. CONCLUSION

Various cryptography techniques area unit being employed therefore on guarantee privacy and authentication of info sent digitally. Digital Signatures uses cryptography, hashing and Digital Signature algorithms to ease its users therefore on attain desired properties privacy, integrity and authentication for info security. There area unit many doable ways in which to use Digital Signatures and every have its execs and cons.

V. FUTURE SCOPE

For RSA, projected future work, if we tend to take away the method of cryptography freelance of N, power of security of RSA algorithmic rule is magnified by incorporating this method. And for SHA, Future work consists of SHA's performance calculations for all domains. Pipelining the planning at applicable points may end in greater outturn rates. Current style is increased by mistreatment applicable pipelining techniques.

Conflict of interest: The authors declare that they have no conflict of interest.

Ethical statement: The authors declare that they have followed ethical responsibilities.

REFRENCES

[1] Sonal Sharma, Prashant Sharma, Ravi Shankar Dhakar, "RSA Algorithm Using Modified Subset Sum Cryptosystem", International Conference on Computer & Communication Technology (ICCCT)-2011.

[2] Hung-Min Sun, Mu-En Wu, Wei-Chi Ting, and M. Jason Hinek, "Dual RSA and Its Security Analysis", IEEE Transactions on Information Theory, Vol. 53, No. 8, Aug. 2007

[3] Sattar J Aboud, "An efficient method for attack RSA scheme", IEEE 2009.

[4] Allam Mousa , "Sensitivity of Changing the RSA Parameters on the Complexity and Performance of the Algorithm", ISSN 1607 – 8926, Journal of Applied Science, Asian Network for Scientific Information, pages 60-63,2005.

[5] William Stallings, "Cryptography and Network Security", ISBN 81-7758-011-6, Pearson Education, Third Edition, pages 42-62,121-144,253-297.

[6] Prashant Sharma, Ravi Shankar Dhakar, AmitKumar Gupta, Modified RSA Encryption Algorithm (MREA), 2012 Second International Conference on Advanced Computing & Communication Technologies.

[7] J. Pollard, "Monte Carlo methods for index computation (modp)",Math. Comp., Vol. 32, pp.918-924, 1978.

[8] J. Pollard, "Theorems on factorization and primality testing", Proc. Cambridge Philos.Soc., Vol. 76, pp.521-528, 1974.

[9] R. P. Brent, "An improved Monte Carlo factorization algorithm", BIT 20 (1980), 176-184. MR 82a:10007, Zbl 439.65001. rpb051.

[10] B R Ambedkar, Ashwani Gupta, Pratiksha Gautam, SS Bedi "An Efficient Method to Factorize the RSA Public Key Encryption", 2011 International Conference on Communication Systems and Network Technologies.

[11] João Carlos Leandro da Silva, "Factoring Semi primes and Possible Implications", IEEE in Israel, 26th Convention, pp. 182-183, Nov. 2010.

[12] Kashif Latif, Athar Mahboob, Arshad Aziz. "High Throughput Hardware Implementation of Secure Hash Algorithm (SHA-3) Finalist: BLAKE", 2011 Frontiers of Information Technology.

[13] NIST Interagency Report 7764, "Status Report on the Second Round of the SHA-3 Cryptographic Hash Algorithm Competition", February 2011, pp. 1-38.

