A Review on Implementation of RSA Cryptosystem Using Ancient Indian Vedic Mathematics

Shahina M. Salim Prof. N.N. Mandaogade

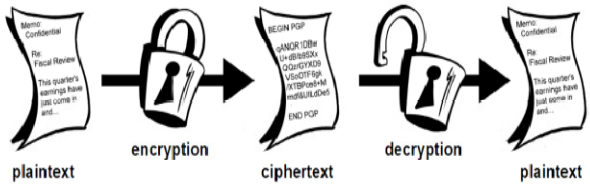
***Abstract*— The standard techniques for providing privacy and security in information networks include encryption/decryption of RSA algorithmic rule. RSA is one in every of the safest normal algorithms, supported public-key, for providing security in networks. it's wide used for secure information transmission. the protection of RSA depends on the process issue of factorisation massive integers. As computing power will increase and additional economical factorisation algorithms square measure discovered, the flexibility to issue larger and bigger numbers also will increase. The performance of most crypto systems is primarily determined by Associate in Nursing economical implementation of arithmetic operations. The RSA algorithmic rule entails a standard operation operation on massive integers, that is significantly long to implement. The implementation of RSA encryption/decryption algorithmic rule mistreatment the algorithmic rule of Ancient Indian religious text arithmetic that are changed to enhance performance. RSA electronic equipment enforced mistreatment religious text multiplication is economical in terms of space, speed compared to its implementation using standard multiplication.**

***Index Terms*— FPGA, Modular exponentiation, Modular Multiplication, RSA Cryptosystem, VHDL.**

I. INTRODUCTION

The history of cryptography begins with secret writings within the Ancient civilizations. The hieroglyphic writings on the tombs of ancient Egypt's and ancient Spartan's Scytale , ancient Indian and Hebrew scripts square measure samples of ancient cryptography. The Caesar cipher is one in every of the famous substitution ciphering ways. throughout the amount of Second war magnetic attraction machines like enigma were used.

The modern cryptography will be divided into personal (symmetric) key secret writing ways and public (asymmetric) key secret writing ways . encoding normal – DES may be a personal key technique. to solve the insecurity owing to the usage of single key, twin key ways known as public key ways were introduced. Diffie – Hell man key exchange is that the initial approach towards public key ways. the primary made public key technique is RSA cryptosystem, introduced by Rivest, Shamir, and Adleman in 1977. RSA public key cryptosystem desires quick division design, so as to figure as quick as its computer code counterparts. however division is that the slowest ALU operation. therefore it cannot use in RSA systems. rather than this, standard multiplication schemes square measure used. RSA algorithmic rule is that the best familiar, the foremost versatile and wide used public key algorithmic rule nowadays RSA depends on the standard operation of long integers, that is that the essential operation for a range of the foremost wide accepted cryptosystems . Therefore, quick standard multiplication becomes the key to time period secret writing and secret writing since a high turnout is required in digital communication. the foremost wide used algorithmic rule for economical standard multiplication is Montgomery's algorithmic rule . The binary Montgomery's modular-multiplication algorithmic rule employs solely straightforward addition, subtraction, and shift operation to avoid trial division, a essential and long operation in standard standard multiplication. The standard operation is typically accomplished by activity recurrent standard multiplications.



The Sanskrit word 'Veda' means that 'knowledge'. The Vedas incorporates an enormous variety of documents there square measure said to be thousands of such documents in India, several of that haven't nonetheless been translated, that square measure shown to be extremely structured, each at intervals themselves and in respect to one another. Some documents, known as 'Ganita sutras' (the name 'ganita' means that mathematics), were dedicated to mathematical data. religious text arithmetic is principally supported sixteen Sutras (or aphorisms) managing numerous branches of arithmetic like arithmetic, algebra, pure mathematics etc.

The FPGA configuration is usually outlined employing a hardware description language (HDL), the same as that used for an application-specific microcircuit (ASIC) FPGAs will be wont to implement any logical perform that an ASIC will perform. the flexibility to update the practicality when shipping, partial re-configuration of the portion of style the planning the look and therefore the low non-recurring engineering prices relative to an ASIC design, provide blessings for several applications. FPGAs contain programmable logic elements known as "logic blocks", and a hierarchy of reconfigurable interconnects that permit the blocks to be "connected together"—somewhat sort of a one-chip programmable board. Logic blocks will be designed to perform complicated combinable functions, or just straightforward logic like AND and NAND. In most FPGAs, the logic blocks also include memory parts, which can be straightforward flip-flops or additional complete blocks of memory. VHDL is an form for VHSIC Hardware Description Language (VHSIC is Associate in Nursing form for terribly High Speed Integrated Circuits). it's a hardware description

Journal Impact Factor-2.02
Indexed by- ProQuest, DOAJ and many International Bodies.

language that may be wont to model a digital system at several levels of abstraction starting from the recursive level to the gate level. The complexness of the digital system being sculptured may vary from that of an easy gate to a whole digital electronic system, or something in between. The digital system can even be described hierarchically. expressly can even be expressly sculptured within the same description.

II. LITERATURE REVIEW

Sriraman, L, Kumar K.S, Prabakar, T.N [1] presented religious text arithmetic is one in every of the traditional Indian arithmetic that contains sixteen sutras. These sutras will be wont to solve issues in any branch of arithmetic in a quicker method. The projected squarer relies on Sanskrit literature known as Ekadhikena Purvena. It means ―one quite the previous‖. This Sanskrit literature is employed for locating the sq. of decimal numbers ending with `5'. during this paper this Sanskrit literature is generalized and used for squaring of binary numbers. Gustavo D. Sutter, Jean-Pierre Deschamps, and José Luis Imaña [2] conferred standard operation with massive modulus and exponent, that is typically accomplished by recurrent standard multiplications, has been wide utilized in public key cryptosystems. Typically, the Montgomery's modular-multiplication algorithmic rule is employed since no trial division is important, and therefore the carry–save addition (CSA) is used to scale back the essential path. during this paper, we have a tendency to optimize the Montgomery's multiplication and propose architectures to perform the smallest amount vital bit initial and therefore the most important bit initial algorithmic rule [3],[4],[5].

Xiaoming Tang [6] presented a precise vary of complex quantity conferred by ASCII code is regenerate to single precision floating-point by pipeline process with VHDL language. Through useful simulation and transfer verification, the conversion time is concerning ten United States once the clock is fifty megahertz .

Huddar, S.R. , Rupanagudi, S.R. , Kalpana, M. , Mohan, S. [7] conferred With the appearance of latest technology within the fields of VLSI and communication, there's also an ever growing demand for prime speed process and low space style. it's also a accepted fact that the number unit forms an integral a part of processor style. owing to this regard, high speed number architectures become the requirement of the day. during this paper, we have a tendency to introduce a unique design to perform high speed multiplication mistreatment ancient religious text maths techniques. Jaina, D, Sethi, K. , Panda, R. [8] presented time period signal process needs high speed and high turnout Multiplier-Accumulator (MAC) unit that consumes low power, that is usually a key to attain a high performance digital signal process system. during this paper, style of mac unit is projected. The number used within the mac unit relies on the Sanskrit literature "Urdhva Tiryagbhyam" (Vertically and Cross wise) that is one in every of the Sutras of religious text arithmetic. religious text arithmetic is principally supported sixteen Sutras and was rediscovered in early twentieth century. In ancient India, this Sanskrit literature was historically used for decimal variety multiplications at intervals less time. identical construct is applied for multiplication of binary numbers to form it helpful within the digital hardware. G.P. Saggese , L. Romano[9] presented an accelerator which might effectively improve the protection and therefore the performance of nearly any RSA science application. The accelerator integrates 2 crucial security- and performance enhancing facilities: an RSA processor and an RSA key-store. an RSA processor may be a dedicated hardware block that executes the RSA algorithmic rule. an RSA key-store may be a dedicated device for firmly storing RSA key-pairs. we have a tendency to selected RSA since it's out and away the foremost wide adopted normal publicly key cryptography[10].

III. PROPOSED WORK

The RSA algorithmic rule relies on the mathematical indisputable fact that it's simple to search out and multiply the big prime numbers along, however it's very tough to issue their product. the general public and personal keys in RSA square measure supported terribly massive prime numbers[10]. The algorithmic rule is straightforward however the complexness lies within the choice and generation of public and personal keys.

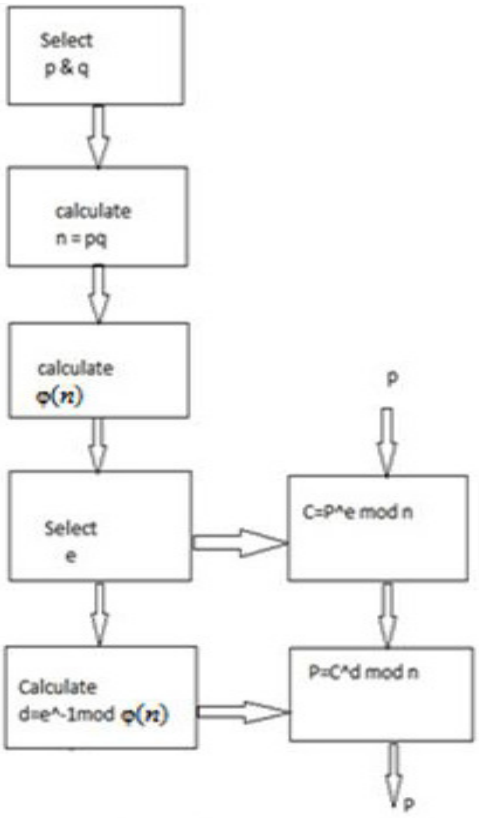


Fig: Flow chart of RSA algorithm

The RSA algorithm involves three steps: key generation, encryption and decryption.

1. Key generation : RSA involves a public key and a non-public key. the general public key will be familiar by everybody and is employed for encrypting messages. Messages encrypted with the general public key will solely be decrypted

in an exceedingly cheap quantity of your time mistreatment the personal key[11]. The keys for the RSA algorithmic rule square measure generated the subsequent way:

1. Choose 2 distinct prime numbers p and Q. For security functions, the integers p and Q should be chosen randomly, and will be of comparable bit-length. Prime integers will be with efficiency found employing a property take a look at.

2. Cipher n = pq.
n is employed because the modulus for each the general public and personal keys. Its length, sometimes expressed in bits, is that the key length.

3. Calculate $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, wherever φ is Euler's totient perform.

4. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e. e and φ(n) are coprime.
• e is discharged because the public key exponent.
• e having a brief bit-length and little hamming weight ends up in additional economical coding – most typically a pair of $2^{16} + 1 = 65,537$. However, a lot of smaller values of e (such as 3) are shown to be less secure in some settings.

5. verify d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is that the inverse of e (modulo φ(n)
• This is additional clearly expressed as: solve for d given
$d \cdot e \equiv 1 \pmod{\varphi(n)}$
• This is usually computed using the extended euclidian algorithmic rule. using the pseudocode within the standard integers section, inputs a and n correspond to e and φ(n), severally.
• d is unbroken because the non-public key exponent

The public key consists of the modulus n and also the public (or encryption) exponent e. The non-public key consists of the modulus n and also the non-public (or decryption) exponent d, that should be unbroken secret. p, q, and φ(n) should even be unbroken secret as a result of they'll be wont to calculate d.

2. Encryption : A transmits its public key (n, e) to B and keeps the non-public key d secret. B then desires to send message P to A , then computes the ciphertext C corresponding to

$$C = p^e \pmod{n}$$

This can be done with efficiency, even for 500-bit numbers, using standard mathematical operation. B then transmits C to A[10].

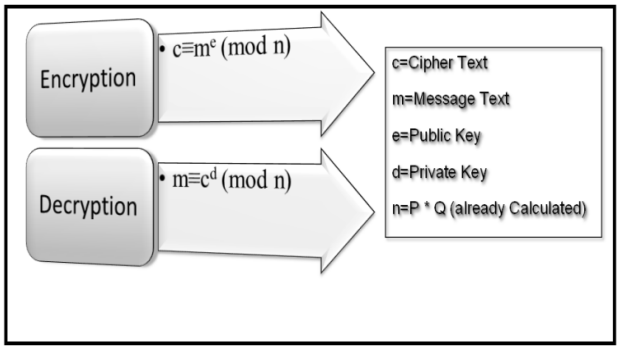
3. Decryption : A will recover P from C by using its non-public key exponent d via computing

$$P = C^d \pmod{n}$$

Thus we tend to get the initial message.

IV. CONCLUSION

The RSA encryption/decryption system is enforced using the vedic arithmetic algorithmic rule to extend its computation speed. The advantage of the vedic multiplier factor is that it



calculates the partial products in one single step and also there are not any shift operations that saves the time and the hardware. because the range of message bits will increase the gate delay still because the area increase slowly. thus it may be used effectively altogether the cryptologic applications. it's found that this design is kind of economical in terms of silicon area and speed and will lead to substantial savings of resources in hardware once used for crypto and security applications.

REFERENCES

[1] Sriraman, L. Dept. of Electron. & Commun. Eng., Oxford Eng. Coll., Trichy, India ; Kumar, K.S. ; Prabakar, T.N ,— Design and FPGA implementation of binary squarer using Vedic mathematics‖ IEEE Trans. Ind. Electron., July 2013.
[2] Gustavo D. Sutter, Member, IEEE, Jean-Pierre Deschamps, and José Luis Imaña ,— Modular Multiplication and Exponentiation Architectures for Fast RSA Cryptosystem Based on Digit Serial Computation‖ IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3308–3316, Oct. 2010.
[3] E. Monmasson and M. N. Cirstea, —FPGA design methodology for industrial control systems—A review,‖ IEEE Trans. Ind. Electron., vol. 54, no. 4, pp. 1824–1842, Aug. 2007.
[4] J. J. Rodriguez-Andina, M. J. Moure, and M. D. Valdes, —Features, design tools, and application domains of FPGAs,‖ IEEE Trans. Ind. Electron., vol. 54, no. 4, pp. 1810–1823, Aug. 2007.
[5] R. L. Rivest, A. Shamir, and L. Adleman, —A method for obtaining digital signatures and public-key cryptosystems,‖ Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[6] Xiaoming Tang ; Res. Inst. of Inf. Fusion, Naval Aeronaut. & Astronaut. Univ., Yantai, China; Tao Zhang ; Zhenjie Wang ; Wenliang Yuan, —A novel data format conversion method based on FPGA‖ IEEE Trans. Ind. Electron ,July 2011.
[7] Huddar, S.R. ; WorldServe Educ., Bangalore, India ; Rupanagudi, S.R. ; Kalpana, M. ; Mohan, S. , —Novel high speed vedic mathematics multiplier using compressors‖ IEEE Trans. Ind. Electron ,March 2013.
[8] Jaina, D. ; Dept. of Electron. & Telecommun. Eng., VSS Univ. of Technol., Burla, India ; Sethi, K. ; Panda, R, —Vedic Mathematics Based Multiply Accumulate Unit‖ IEEE Trans. Ind. Electron ,Oct. 2011.
[9] G.P. Saggese a, L. Romano a,*, N. Mazzocca b, A. Mazzeo, —A tamper resistant hardware accelerator for RSA cryptographic applications, Journal of Systems Architecture 50 (2004) 711–727 ‖.
[10] William Stallings, — Cryptography and Nework Security‖, Third Edition, Pearson Education, 2003
[11] S.E. Eldridge, C.D. Walter, Hardware Implementation of Montgomery's modular multiplication algorithm, IEEE Trans. Comput. 42 (6) (1993) 693–699.
[12] A.Z. Alkar, R. So¨ nmez, An ASIC Implementation of the RSA Algorithm 18th MUG International Conference, February 2002.
[13] Sumit Vaidya, Deepak Dandekar, —Delay-Power Performance Comparison of multipliers in VLSI circuit design‖, International Journal of Computer Networks & Communications (IJCNC), Vol.2, No.4, July 2010