www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13492-13494

A Survey over Various Variants of RS and Similar Cryptography Techniques

Pramila Patidar[1] Namrata Sharma[2]
[1]PG Scholar CSE,
[1]Sushila Devi Bansal College of Engineering, Indore, India
Email-ppatidar@sdbce.ac.in

[2]Assistant professor CSE
Sushila Devi Bansal College of Engineering, Indore, India
Email- nsharma@sdbce.ac.in

Abstract- **The high growth within the networking technology leads a typical culture for interchanging of the digital pictures terribly drastic. Thus, it's additional vulnerable of duplicating of digital image and re-distributed by hackers. So the knowledge needs to be protected whereas sending it, Sensitive data like credit cards, banking transactions and social insurance numbers have to be compelled to be protected. For this several cryptography and decoding techniques are a unit existing that area unit accustomed avoid the knowledge stealing. In the recent days of the web, the cryptography and decoding of information play a serious role in securing the information in on-line transmission focuses chiefly on its security across the web. Totally different cryptography and decoding techniques are units accustomed defend the confidential knowledge from unauthorized use.**

In this paper, a review of the cryptography based techniques has proposed. This review contains the working, merits, demerits of the current encryption decryption techniques.

Keywords: Encryption , Decryption, Cryptography , Symmetric Key Cryptography , Asymmetric Key Cryptography.

I. INTRODUCTION

II.

Cryptography is that the study of mathematical techniques associated with aspects of data security like confidentiality, knowledge, integrity, entity authentication, and knowledge origin authentication. Cryptography isn't the sole means that of providing info security, however instead of that it's a collection of techniques.

There square measure 2 cryptography mechanisms, counting on what keys square measure used. If an identical secret is employed for coding and secret writing, we tend to tend to call the mechanism as Symmetric key cryptography. On the various hand, if 2 fully totally different keys square measure used in science mechanism, then we tend to tends to call mechanism as uneven Key or asymmetric key [2].

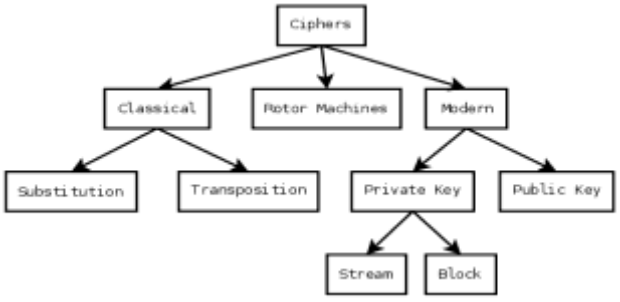

Figure 1: Cryptography Classification

The above figure 1 shows cryptography classification named bilaterally symmetric key and uneven or Asymmetric key cryptography.

CRYPTOGRAPHY SECURITY SERVICES:

The security services include [2]:

- **Data Confidentiality**
- **Data Integrity**
- **Authentication**
- **Non repudiation**
- **Access Control**
- **Data Confidentiality**

II. LITERATURE SURVEY

RSA has various security issues and general considerations based on mathematical calculations.[4] RSA is the best algorithm for security purpose but it's key length is too large so to decrypt any message there is too much wastage of time and energy. So if some concept of ECC may be added then it will give better response for

security as well as complexity point of view because ECC is strongest concept having higher security level than RSA and it is easy to use. Due to the recent development in field of factoring of large prime, the key length for secure RSA has increased. The increment in the length can increase the security of the RSA Cryptography, but it requires extra communicational, computational cost [6]. When we calculate multiplicative inverse of an element in GF (p) for small values of p, it is very easy. But when we calculate it for larger numbers then RSA becomes very complex so Euclid's algorithm can be extended for this purpose.

The attack is difficulty equivalence to the division of the product of two very large prime numbers say p, q, however the RSA having the higher security [1,5,2]. The private key e is used to encrypt when we are sending any plaintext message to others.
[7] presents a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices. Several points can be concluded from the Experimental results.
DES and 3DES are known to have worm holes in their security mechanism; Blowfish and AES do not have any so far [3].

[8] four image encryption algorithms have been studied by means of measuring the encryption quality and the execution time of the encryption. In addition, the security analysis of these schemes is investigated from cryptographic viewpoint; statistical and differential attacks. The results are compared, focusing on those portions where each scheme is performed differently.

This paper deals with cryptography that makes use of the public key also called as the PKC systems in short. In systems pertaining to PKC , two keys that are entirely different are utilized for encoding and decoding the data. The strength and security depends on large key size as among the two keys one is distributed and kept open to the public in PKC systems . Previously in PKC systems the mathematical problems of prime factorization and discrete logarithm are used. The security with a almost euql to the above with relatively small sizes of the key has been promised by ECC and it has been proved. The ECC implementation on application specific systems is the main point focused in the field of research. The requirement of separate crypto coprocessor can be reduced by doing a research in the category of ECC mainly related to present various combinations of speed optimized algorithms. Various mathematical techniques are considered to enhance the speed and security of ECC. [9]

In this paper the security aspect of embedded has been discussed in detail. A case study that takes into account the efforts that is needed for securing the electronic systems has been created with the increasing cases where the data from systems concerned with embedded are being hacked and destroyed leading to huge loss in the last few year. Systems in the embedded world that are dedicatedly and specifically utilized to capture the data and then storing it and accessing it when required keeping its security sensitivity do possess a large security and other challenges in providing the full security to the data. In the world of cryptography the computing and security to the networks are the subject of intensive research. However, the inclusion of added features like the algorithms that are specific to cryptography and protocols pertaining to security, to the system is often taken by mistake and misunderstood as security by embedded system designers. With many parameters like the amount to be spend the expected performance and the power these are the various ideal new metric that designers must take into consideration in reality throughout the design process. This paper deals with the various challenges and ways to make the maximum security to the designers of systems in the embedded world and to the developers of tools From an end-user perspective attempt has been made to give a security that is uniform and unbiased to all the systems in the embedded world and this is achieved by scutenizing the working security requirements for such systems. The underlying challenges associated with different architectures in the embedded world are then identified, then complications involved with designers of hardware and software side for instance processing requirements for security ,tamper-resistant embedded system design, impact on battery life etc.). The availability of limited resources in embedded systems also poses a major challenge in reaching the expected level of security. By joining the architectural advances it the field of embedded systems and the incorporation of various design paradigms has helped us scale up and enable us to meet the new requirement in the next generation of embedded system design. To realize the desired goal, not only the basic aspects of security in an embedded system but also need to go beyond that and provide safety against a variety of possible attacks and one has to do this not leaving the elements like performance of the system the memory usage the consumption of energy should not go up and the other factors like cost and use [10].

Possible Attacks on RSA signature:

- **Factorization**

  The Problem of whole number factorization is one amongst the oldest in number theory. However, the safety of the many cryptanalytic techniques depends upon the intractableness of the number factorization drawback.[8]
  If AN somebody is ready to issue the general public modulus n of some entity A, then the somebody will reckons φ(n) so, mistreatment the extended Euclidean algorithm, deduce the personal key d from φ(n) and public exponent e by finding ed≈1 (mod φ(n)),this constitutes a complete break of the system.

- **Common module attack:**

  To avoid generating a special modulus =pq for every user one would like to repair N once and for all. A similar N is employed by all users. A trusty central may offer user I with a novel combine ei,di from that user I type a public key(N,ei) and a secret key (N,di).
  At first look, this might appear to work: a ciphertext c = m^{e}_{a} mod N meant for Alina can not be decrypted by Balina since Balina doesn't posses d_a. However, this can be incorrect and also the Ensuing system is insecure. By truth one Balina will use his on exponents e_b, sound unit to issue the modulus N. Once N is factored Balina will recover Alina private key d_a from her public key e_a.

- **Wiener's attack**

The Wiener's attack, named once decipherer archangel J. Wiener. The wiener's attack uses the fraction technique to show the non-public key d once d is less.

A wiener's attack is based on two facts:

- If N=pq is a "good" RSA modulus (with p (approx) ≈ (approx) ≈√N), then N (approx) ≈φ(n).
- The wiener's set up is this: as a result of ed ≈ one mod m for variety of|some|many} modulus m>=1 and positive number e and d, then d looks as a divisor at intervals the convergence of e/m. (For identical reason that one can use the Euclidean algorithm to work reciprocal modulo m.)

III. CONCLUSION

As the demand for effective data security is increasing day by day, any organization has an obligation to protect secret and sensitive data from theft or loss. Such sensitive data can be potentially damaging if it is altered, destroyed, or hacked. This makes it necessary to protect the data. Cryptography attempts to provide such guarantee and it ensures the security of data being transmitted. It is implemented in many day-to-day applications such as the security of ATM card, computer passwords, e-commerce, military, etc. A review of modern methods is also done in brief. The most of the modern data security techniques have been reviewed. Each of the method has been analyzed with the advantages and the disadvantages. Then a list of common problems in the current version has been identified.

IV. REFERENCES

[1] Prashant Sharma, "Modified Integer Factorization Algorithm using V-Factor Method", 2012 Second International Conference on Advanced Computing & Communication Technologies, IEEE 2012.

[2] Prof.Dr.Alaa Hussein Al-Hamami,Ibrahem Abdallah Aldariseh ,"Enhanced Method for RSACryptosystem Algorithm" 2012International Conference onAdvanced Computer Science Applications and Technologies, IEEE 2012.

[3] Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept.

[4] Giraud, "An RSA Implementation Resistant to Fault Attacks and to Simple Power Analysis," IEEE Trans. Computers, vol. 55, no. 9, pp. 1116- 1120, Sept. 2006.

[5]. R. changramouli,"Batterypower-aware encryption –ACM Transaction on information and System Security (TISSEC),'' Vol. 9 Issue 2, May 2006.

[6] Shashi Mehrotra Seth, 2Rajan Mishra," Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Iss ue 2, June 2011 pp.192-192

[7] Diaa Salama1, Hatem Abdual Kader2, and Mohiy Hadhoud2" Wireless Network Security Still Has no Clothes", International Arab Journal of e-Technology, Vol. 2, No. 2, June 2011 pp.112-123.

[8] Hongwei Si,Youlin Cai, Zhimei Cheng, ―An improved RSA algorithm based on Complex numeric operation function‖.

[9].Rahat Afreen1 and S.C. Mehrotra(June 2011) , **a review on elliptic curve cryptography for embedded systems**, International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, , Pp 84-103

[10] Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan and Srivaths Ravi(2004), **Security as a New Dimension in Embedded System Design** Proceedings of the 41st annual conference on Design automation DAC 4 Volume: 48, Issue: 1, Publisher: ACM Press, Pages: 753-760