International Journal of Advanced Research in Engineering Technology & Sciences ISSN: 2394-2819
June-2016 Volume 3, Issue-6
Email:editor@ijarets.org www.ijarets.org

REVIEW ON PROTECTION OF DATA IN RSA TECHNIQUE

Monika Suhag
M. Tech Scholar
Department CSE
GITM, Kablana, Jhajjar

Dr. Neetu Sharma
Assistant Professor
Department CSE
GITM, Kablana, Jhajjar

ABSTRACT: - Most companies and government agencies have a dire need for protecting sensitive information. Encryption, access restriction, and locking documents behind firewalls are some common techniques for protecting sensitive information. Encryption is an effective way for preventing an unauthorized person from viewing the content of a sensitive document. Nonetheless, once the document is decrypted for viewing using the secret key, an ill-intentioned authorized person can save, copy, print, or transmit the unencrypted document anywhere he or she wants without any major difficulty. Many algorithms are invented by researcher for avoidance of risk. One of them is RSA algorithm which play important role for better security. In this paper we study about an invention on RSA algorithm.
KEYWORD*:* Cryptography, RSA, Hill Cipher, Bit Rotation

I. INTRODUCTION

Cryptography is best method to protect data and Important files from unauthorized parties. It is the science of writing the data in secret code and about the design and analysis of mathematical techniques that is enables secure communication in the presence of millions adversaries. Cryptography is the art of secret writing [1, 2]. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it [6]. Cryptographic systems involve both an algorithm and a secret value. The secret value is known as the key [3, 4]. The reason for having a key in addition to an algorithm is that it is difficult to keep devising new algorithms and it will allow reversible scrambling of information's.

Symmetric cryptography's distinctive feature is the use of the same key (hence symmetric) for encryption and decryption [5]. The key represents therefore a shared secret between two (or more) parties that wish to communicate. A Symmetric Encryption (SE) scheme is a 6-tuple (K; P; C; KeyGen; Enc; Dec) defined as follows.

Table I Symmetric Encryption scheme

K	The key space.
P	The set of messages to be encrypted, or plaintext space.
C	The set of the messages transmitted over the channel, or ciphertext space.
KeyGen	A probabilistic key generation algorithm that takes as input a security parameter 1 and outputs a key 2 K.
Enc	A deterministic encryption algorithm that receives as input a key 2 K and a plaintext - 2 P and returns a ciphertext 2 C.
Dec	A deterministic decryption algorithm that receives as input a key 2 K and a ciphertext 2 C and outputs a plaintext - 2 P.

Symmetric schemes are commonly called ciphers. The first cipher known dates back to the Romans: there is evidence of Julius Caesar using this method to communicate with his generals, hence the

scheme is usually referred to as \Caesar cipher" [7]. It consists simply of shifting the letters in a message by a certain number of positions. Modern ciphers are divided into two families: stream ciphers and block ciphers. Schemes in the first family encrypt the bits of a message one at a time, while the block ciphers, as the name suggests, take a certain number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size. An example is the very famous RSA [8] that uses blocks of size 128, 192 or 256.

II. SURVEY

[2] Vishwa Gupta,Gajendra Singh, Ravindra Gupta Information security is the process of protecting information. It protects its availability, privacy and integrity. Access to stored information on computer databases has increased greatly. More companies store business and individual information on computer than ever before. Much of the information stored is highly confidential and not for public viewing. In this paper I have developed a new cryptography algorithm which is based on block cipher concept. In this algorithm I have used logical operation like XOR and shifting operation. Experimental results show that proposed algorithm is very efficient and secured. To write this paper I have Study about information security using cryptography technique. After the detailed study of Network security using cryptography, I am presenting my proposed work. This paper is dividing in four sections. In section-I, I am presenting just basic introduction about Information Security using cryptography, in section-II, I am presenting detailed description of Information security using cryptography and various algorithms, in section-III, I am presenting my proposed algorithm, and in section IV I am Presenting summary and references where I have completed my research. The proposed algorithm has the batter speed compared with the comparing encryption algorithm. Nevertheless, the proposed algorithm improves encryption security by inserting the symmetric layer. The proposed algorithm will be useful to the applications which require the same procedure of encryption and decryption. [3] Mohammed AbuTaha, MousaFarajallah, RadwanTahboub, Mohammad Odeh Cryptography in the past was used in keeping military information, diplomatic correspondence secure and in protecting the national security. However, the use was limited. Nowadays, the range of cryptography applications have been expanded a lot in the modern area after the development of communication means; cryptography is essentially required to ensure that data are protected against penetrations and to prevent espionage. Also, cryptography is a powerful mean in securing e-commerce. Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one who has the decipher key, and data cannot be changed means the original information would not be changed or modified; this is done when the sender includes a cryptographic operation called a hash function in the original message. A hash function is a mathematical representation of the information, when any information arrives at its receiver; the receiver calculates the value of this hash function. If the receiver's hash function value is equivalent to the sender's, the integrity of the message is assured.

[4] Thai Duong, Juliano Rizzo This paper discusses how cryptography is misused in the security design of a large part of the Web. Our focus is on ASP.NET, the web application framework developed by Microsoft that powers 25% of all Internet web sites. We show that attackers can abuse multiple cryptographic design flaws to compromise ASP.NET web applications. We describe practical and highly efficient attacks that allow attackers to steal cryptographic secret keys and forge authentication tokens to access sensitive information. The attacks combine decryption oracles, unauthenticated encryptions, and the reuse of keys for different encryption purposes. Finally, we give some reasons why cryptography is often misused in web technologies, and recommend steps to avoid these mistakes.

[5] Sonalsharma, jitendrasinghyadav, parshantsharmaIn asymmetric key cryptography, also called Public Key cryptography; two different keys (which form a key pair) are used. One key is used for encryption & only the other corresponding key must be used for decryption. No other key can decrypt the message – not even the original (i.e. the first) key used for encryption. The beauty of this scheme is that every communicating party needs just a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, he /she can communicate with anyone else. The

Short Range Natural Number (SRNN) algorithm is similar to RSA algorithm with some modification. This modification increases the security of the cryptosystem. In this algorithm we have an extremely large number that has two prime factors (similar to RSA). In addition of this we have used two natural numbers in pair of keys (public, private).These natural numbers increase the security of the cryptosystem. So its name is "Modified RSA Public Key Cryptosystem using Short Range Natural Number Algorithm".

B.Persis Urbana Ivy, PurshotamMandiwa.Mukesh Kumar, [6]to secure data or information by a modified RSA cryptosystem based on 'n' prime. This is a new technique to provide maximum security for data over the network. It is involved encryption, decryption, and key generation. Prime number used in a modified RSA cryptosystem to provide security over the networks. In this technique we used 'n' prime number which is not easily breakable. 'n' prime numbers are not easily decompose. This technique provides more efficiency and reliability over the networks. In this paper we are used a modified RSA cryptosystem algorithm to handle 'n' prime numbers and provides security.

[7] Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lang, and Nicko van SomerenThis paper explains how an attacker can efficiently factor 184distinct RSA keys out of more than two million 1024-bit RSA keys downloaded from Taiwan's national \Citizen Digital Certificate" database. These keys were generated by government-issued smart cards that have built-in hardware random-number generators and that are advertised as having passed FIPS 140-2 Level 2 certification. These 184 keys include 103 keys that share primes and that are efficiently factored by a batch-GCD computation. This is the same type of computation that was used last year by two independent teams (USENIX Security 2012: Heninger, Durumeric, Wustrow, Halderman; Crypto 2012: Lenstra, Hughes, Augier, Bos, Kleinjung, Wachter) to factor tens of thousands of cryptographic keys on the Internet. The remaining 81 keys do not share prime. Factoring these 81 keys requires taking deeper advantage of randomness-generation failures: first using the shared primes as a springboard to characterize the failures, and then using Coppersmith-type partial-key-recovery attacks. This is the first successful public application of Coppersmith-type attacks to keys found in the wild.[8] M. Nordin A. Rahman, A. F. A. Abidin, Mohd Kamir Yusof, N. S. M. Usop, The Hill cipher is the first polygraph cipher which has some advantages in symmetric data encryption. However, it is vulnerable to known plaintext attack. Another setback is that an invertible key matrix is needed for decryption and it is not suitable for encrypting a plaintext consisting of zeroes. The objective of this work is to modify the existing Hill cipher to overcome these three issues. Studies on previous results showed that the existing Hill algorithms are not yet sufficient. Some of these algorithms are still vulnerable to known plaintext attack. On the other hand, some of these algorithms have better randomization properties and as a result they are more resistant against known plaintext attack. Nevertheless, these enhanced Hill cipher algorithms still face the non-invertible key matrix problem. Moreover, neither of these algorithms are suitable for all zeroes plaintext block encryption. In this paper, a robust Hill algorithm (Hill++) is proposed. The algorithm is an extension of the Affine Hill cipher. A random matrix key is introduced as an extra key for encryption. Moreover, an involuntary matrix key formulation is also implemented in the proposed algorithm. This formulation can produce an involuntary key where a same key can be used for both encryption and decryption. Testing on the proposed algorithm is carried out via two approaches, that is through comparative study and statistical analysis. Comparative study shows that Hill++ is resistant to all zeroes plaintext block encryption and does not face the non-invertible key matrix problem as what was faced by the original Hill, AdvHill and HillMRIV algorithms. Apart from this, the encryption quality of the proposed algorithm is also measured by using the maximum deviation and correlation coefficient factors. Results from statistical analysis shows that Hill++ (when compared to Hill, AdvHill and HillMRIV algorithms) has the greatest maximum deviation value and its correlation coefficient value is the closest to zero. The results from these two measures proved that Hill++ has better encryption quality compared to HillMRIV.

III. CONCLUSION

We have discussed that RSA encrypt image with 1 bit rotation. Now encryption of image improved by using 2 bit rotation in our thesis. There can be some improvement in the work done by us that future work about the more encryption of image. Here our last concept about apply 2 bit rotation at place of 1bit rotation. So in future 2 bit rotation can be used as input and other encryption scheme can be applied. Three bit rotation can used in coming time for more protection. 2 bit rotation can be applied with other existing technique like AES, DES etc.

REFERENCES

1 KalyanChakraborty," Introduction to Basic Cryptography", CIMPA School of Number Theory in
2 Cryptography and Its Applications School of Science, Kathmandu University, Dhulikhel, NepalJuly 20, 2010.
3 VishwaGupta,Gajendra Singh ,Ravindra Gupta , "Advance cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.
4 Mohammed AbuTaha, Mousa Farajallah, RadwanTahboub, Mohammad Odeh," Survey Paper: Cryptography Is The Science Of Information Security", International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (3) : 2011.
5 Thai Duong, Juliano Rizzo," Cryptography in theWeb: The Case of Cryptographic Design Flaws in ASP.NET", Unrecognized Copyright Information DOI 10.1109/SP.2011.42.
6 Sonalsharma, jitendrasinghyadav, parshantsharma," Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm"International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012 ISSN: 2277 128X.
7 B.Persis Urbana Ivy, PurshotamMandiwa. Mukesh Kumar," A modified RSA cryptosystem based on 'n' prime numbers", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume1 Issue 2 Nov 2012 Page No. 63-66.
8 Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou,NadiaHeninger, Tanja Lang, and Nicko van Someren," Factoring RSA keys from certi_ed smart cards:Coppersmith in the wild", Permanent ID of this document:278505a8b16015f4fd8acae818080edd. Date: 2013.09.16.
9 M. Nordin A. Rahman, A. F. A. Abidin, MohdKamirYusof, N. S. M. Usop," Cryptography: A New Approach of Classical Hill Cipher", International Journal of Security and Its Applications Vol. 7, No. 2, March, 2013
10 RajinderKaur, Er.Kanwalprit Singh," Image Encryption Techniques:A Selected Review" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 6 (Mar. - Apr. 2013), PP 80-83
11 Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM 21 (2): 120–126. doi:10.1145/359340.359342.
12 Håstad, Johan (1986). "On using RSA with Low Exponent in a Public Key Network".Advances in Cryptology — CRYPTO '85 Proceedings. Lecture Notes in Computer Science 218. pp. 403–408. doi:10.1007/3-540-39799-X_29