An Overview of Cryptanalysis of RSA Public key System

K.Berlin [#1], S.S.Dhenakaran [*2]

[#] Ph.D Research Scholar, Department of Computer Science, Alagappa University, Karaikudi
[1] berlinjenson@gmail.com
[*] Professor, Department of Computer Science, Alagappa University, Karaikudi
[2] ssdarvind@yahoo.com

***Abstract*- The RSA Cryptosystem was released in 1977. It used two distinct mathematically designed keys for both encryption and decryption process. RSA was one of the first practical public key cryptosystem among the various kinds of public key system. It secured sensitive data while the transmission of secrets through the improper channel like internet. It key sizes 1024 to 4096, 768 bit key had been broken. However 3328 bit typical keys are unbreakable. So it has been used for extensive research among the public key area researchers. The main principle of RSA is providing tough security from the difficulty of factoring large integers. The contribution of this paper is producing an overview of cryptanalysis on the RSA public key cryptosystem. From this research among the various attacks, timing attack has been interrupt against security in RSA algorithm. Hence the paper has proposed RSA cryptosystem is still a good security to transmit sensitive data.**

Key words: Attacks, Cryptosystem, Cryptanalysis, Data transmission, Key sizes, Security.

I. INTRODUCTION

Cryptography is an important action of converting the secret data into secured format to control unauthorized access, updating and so on. To provide security and authentication to the data, many algorithms and techniques were evolved. Even though the cryptographic technique remains best, still better secured mechanisms are needed. There are plenty of cryptosystems exist for providing security through the cryptographic concepts based on two different approaches named as “Symmetric and Asymmetric “. Every cryptosystem has a unique capability to prove their strong security against various hacking techniques. In spite of, many attacks are designed robustly to achieve their goal that is called as “breaking keys”. To achieve key break, the hackers try to increase their interest on the “cryptanalysis”.

Cryptanalysis is plays a major role among the cryptographic areas of research. Nowadays cryptanalysis technique plays equal opposite directions of cryptosystems. Due to some little bit of weakness; every cryptosystem has a breakable one in somehow. The means of cryptanalysis is the information about cryptosystem that have kept by hackers [1]. Here the main work of hackers is to find the weakness on the cryptosystems, is achieved by the study of ciphers.

This research paper fully cares about current cryptanalysis research of RSA cryptosystem. A lot of existence cryptanalysis research is done by various researchers. Particularly SANS institute says about RSA cryptanalysis with the name as cryptanalysis of RSA: a survey [2], the existence of side-channel attacks shows that the extensive study on functionality of RSA cryptosystem is not enough, because timing attacks are more effective and powerful too. So they are advised to the developers and designers of cryptographic applications need to give special care and assiduity to the implementation part for avoiding the data leakage. Through the research named as Cryptanalytic attacks on RSA Cryptosystem: Issues and challenges [3], Adamu Abubakar and Shehu Jabaka says, it is imperative to improve the security of secrets given by the algorithm. Without the attainment of an efficient factoring algorithm capable factoring large integers such as the ones used as the modulus n of the RSA system [3], no viable alternative for the future system of the RSA system remains assured.

Robert Statica says through his research article named as a new approach to cryptanalysis of RSA [4]: RSA security uses blinding instead and reports 2-10% performance penalty. Performance and exhaustive search of all possible private key values are not feasible with present technology. Here Statica [4] has concluded as both timing and brute-force attacks by themselves could be successful only for very small and static keys.

II. SURVEY OF BACKGROUND WORK

A new combined attack was designed and implemented successfully on CRT-RSA by Guillaume Barbu et al [5] that was named as "Combined Attack on CRT-RSA". The name of this combined process is Fault Injection and Side Channel Analysis. The working principle of this combined attack is to inject a fault on RSA cryptosystem while performing the signature computation. The authors work well to open the entire private keys of RSA with the help of factorizing the public modulus as initiation. The authors designed simulation to increase the efficiency of their combined attack.

Don Coppersmith was designed an algorithm with a small solution to avoid RSA vulnerabilities while it has a low exponent. The Coppersmith's research work was named as "Small Solutions to Polynomial Equations and Low Exponent RSA Vulnerabilities [6]". Here to find out the exact solution to univariate modular polynomial equations $p(x) = 0 \pmod N$, and bivariate integer polynomial equations $p(x, y) = 0$, the algorithm was designed. The author used lattice basis reduction method to select all possible related vectors to a hyper plane.

One of the attacks on RSA with low secret exponent d is Wiener's attack. Abderrahmane Nitaj was described the generalization of Wiener's attack [7]. This research article was named as Another Generalisation of Wiener's Attack on RSA. The author suggests based on his research as one should be very cautious when working with a class of RSA exponent. Also, author says, the attacks based on the continued fractions do not apply on RSA modulus N.

H. Imai and Y. Zheng [8], was implemented their research called as "The Effectiveness of Lattice Attacks against Low – Exponent RSA". Through this research, the authors have confirmed that to send a secret data with small public exponent e is dangerous when the modulus size is larger than e times the size of the hidden part.

III. RSA CRYPTOSYSTEM

Rivest, Shamir and Adelman published public key cryptography algorithm named as RSA cryptosystem on 1978. It uses two different keys, a public key known to everyone while the private is kept as a secret. The authorized users only know how to open the message. The encryption ratio of RSA algorithm is high and processing speed is also fast. The key length of this algorithm is more than 1024 bits. Block size of RSA algorithm is 446 bytes and 1 round for encryption. RSA is implemented using a stream cipher. The loss will arise while decrypting the data. Three different operations used to fulfill the encryption process: Key Generation, Encryption and Decryption.

A. Key Generation

Step 1: Choose two different prime numbers randomly, name as p and q

Step 2: Multiply these two prime numbers and the results stored in variable n. ($n= P*q$)

Step 3: Calculate the value of $\varphi(n) = \varphi(p)\,\varphi(q)$

Step 4: Select an integer e such that $1<e<\varphi(n)$ and calculate the greatest common divisor between the integer e and $\varphi(n)$. these gcd value is should equal to 1 ($\gcd(e, \varphi(n))=1$).

Step5: Calculate the value of d, such that $d= e-1$.

B. Encryption

Step 6: Sender transmits public key(n,e) to the receiver and kept d(private) as secret.

Step 7: Receiver sends message M to the sender in the form of $c= me \bmod n$.

C. Decryption

Step 8: Sender can recover message from cipher text with the help of private key d

Step9: d is calculated through the form of, $m= cd \bmod n$.

IV. CURRENT CRYPTANALYSIS MECHANISMS ON RSA

A. Correlation Attack

The category of correlation attack is as the class of known plain text attack. It was designed and working for breaking the keys on stream ciphers. Correlation attack achieved their goal with break keys whose key stream is designed by the output of linear feedback shift registers and Boolean function [10]. The correlation attack is more powerful than the Brute-force attack, for example, the size of key spaces for the break by Brute force is $2^{8\times8}$ and size of the key space of correlation is $2^8 + 2^{7\times8}$. Amar Pandey says about correlation attack through his research article named as "Correlation Attacks on Stream Cipher" [11]. To success the correlation attack, the hackers need to known about the structure of key stream generator. If the entire structure of the generator is known and the secret key is only the initial states of LFSRs, then for a key stream generator consisting of n LFSRs. In Brute force attack, the total number of keys to be tried for the break is $\Pi(2^{L_i} - 1)$ where L_i is the length of the i^{th} LFSR(Linear Feedback Shift Registers)[11].

B. Coppersmith Attack

Coppersmith attack is a class of cryptographic attack and mainly designed and focused on RSA Public key cryptosystem. In such a two cases, coppersmith attack to break RSA cryptosystem that are:

1. When the hacker having the partial knowledge of the secret key.
2. When the public exponent e is a small value.

The usual RSA model has a cipher text c modulus N and public exponent e. Now find out m (message) using m^e = c mod N. Here coppersmith says that if you are a looking for the message such that N^1/e. if it is then a small root, the attacker can easily find out keys and hack the plaintext through the breaking of keys process. Daniel J. Bernstein et al has done a research on RSA factorization that was named as "Factoring RSA keys from certified smart cards: Coppersmith in the wild "[12]. Authors explained, how the hackers can factor 184 specific RSA keys among two million RSA-1024 bit keys download from "Citizen Digital Certificate" database from Taiwan city. Through the government issued smart cards these keys were generated with the help of built-in hardware as well as the random number generator. A batch GCD computation was already factorizing the 103 keys among 184 keys. The rest of the 81 keys are factorized by the Coppersmith partial key recovery attack. The above mentioned process is considered as the first preeminent application of coppersmith attack to keys.

C. Attacks on RSA with Composed Decryption Exponent

A new attack is detected on RSA through the research that was named as "A New Attack on RSA with a Composed Decryption Exponent". Here Abderrahmane Nitaj and Mohamed Ould Douh advised that the RSA users should be more careful when using RSA with short exponents [13]. The author says about RSA cryptosystem, for instance, N=pq with a private exponent d in the form of d= Md1 + d0. Here an author shows that when d1 and d0 are suitable small, then one can find the factorization of N. The method is based on the transforming the key equation ed-k φ(N)=1 into the modular equation f(x;y;z)=ex-Ny+yz-1=0 where (x0;y0;z0) = (d0;k;p+q-1) is a small solution. Generally, the classical attacks on RSA give the factorization of n where $d < N^{0.292}$ as it is the suitable attack of Boneh and Durfee [13]. Through this research, article author says, this attack on RSA is to find the private exponent d even when $d > N^{0.292}$ depending on the possibility that d has the form d = Md1 + d0 for a suitable known M and suitable unknown parameters d1 and d0.

D. Brute Force Attack

Through the searching of all probable keys, the hackers work well to hack secrets with the help of Brute Force Attack. In some cryptosystem, plaintext will become known by attackers knowing half of the keys if keys were chosen randomly. 768 bits of key size in RSA was breakable by Brute Force attacks since 2009. Generally, frequency analysis method was used by brute force attack to hack keys. Sometimes hackers get some characters of plaintext while determined the private key and modulus from the public key for encryption. Based on the standard frequency of the alphabets, the hackers use frequency analysis method and get some part of the plain text. Abhishek Gupta and Vishal Sharma[14] designed modified RSA algorithm to provide secured RSA against Brute Force attack that was named as "Modified Double Mod RSA Tested with Brute Force Attack". Here authors says, in RSA, using of an extended Euclidean and Euler totient function to generate the private key with the help of public key and modulus. Through their research article authors double the RSA functionalities and provide security in increasing mode. Authors tested their double modulo function of RSA with Brute Force attack and got 20 to 30 percent of characters in plain text matched from the Brute Force attack.

E. Side Channel Analysis Attack

Generally the process of side channel analysis is works well through the technique of branch prediction analysis. On the RSA cryptanalysis, the branch predictor work is to test and decisive whether the conditional branch in the instruction flow is to be used or not. The main focus of branch prediction analysis attack is to use a spy to detect the private key. The research work was named as "The power of Simple branch prediction analysis" [15], with in the 10 iterations the authors can invent 508 out of 512 bits of an RSA key. Andrea Pellegrini and Valeria Bertacco [16] discovered the research article named as Fault Based Attack of RSA Authentication. Here the authors retrieve the keys with the help of varying the CPU power voltage limits.

1. ***Timing Attack:*** Timing attacks accomplished the timing variations between various cryptographic operations. Depends upon the input and value of the secret parameters the cryptographic algorithm take different amounts of time to perform the optimization and computation process. If the RSA private key operations work well and accurately in the timing point of view, in some cases the statistical analysis process is applied to rescue of private key. The mathematical operations of RSA cryptosystem are explained shortly here, the public exponent e is used for encryption and private exponent d for decryption. It uses modulus N which is a product of two large prime numbers. To encrypt the original message, calculate $C = M^e \bmod N$ where C is considered as an encrypted message. For decryption to calculate $M = C^d \bmod N$. The goal of attacker is to find private key d. for a timing attack the hacker needs to compute $C^d \bmod N$ from the carefully selected values of C. by analyzing the time variations; the attacker tries to rescue the private key d one bit at a time until the whole private exponent d is known.

Amuthan and praveena[17] proposed technology to secure RSA cryptosystem from the timing attack and the research article named as Securing RSA Algorithm against Timing Attack. The author uses two techniques for securing RSA, one is padding scheme called as OAEP (Optical Asymmetric Encryption Padding) is used before encryption to prevent chosen cipher text attack. The second one is randomness algorithm; it is used after

decryption to prevent non-fixed time computation in RSA [17]. Through this research, author increases the robustness of RSA against timing attack.

F. Records of Factorization in RSA Cryptosystem

TABLE I. RSA Key Size Hacked

Factorized Time in Year Wise	Factorized Key Size in Bits
1992	364
1993	397
1994	426
1996	430
1999	463
2000	512
2003	530
2004	576
2005	663
2010	768

The method of factorization playing the main role on RSA cryptosystem to leak of possible keys for hacking original plain text data, even not knowing by the data of authorized person. RSA was started to enhance the security in 1977, after the years of fifteen it has been lost the key by factorization threat. In earlier, the minimum of 364 bits of key size is hacked by the factorization threat on 1992. The level of 2048 bits of key, RSA cryptosystem provides more security from the point of factorization threat problem.

G. How still RSA Preferred for Secrets?

In RSA cryptosystem the key size of 1024bits is expectable to leak within 2015 to 2020. Compare to 1024bits, 2048bits takes four billion times longer to factorize the original key. The table below shows the measurement of RSA key strength.

TABLE II. RSA Key Strength

Strength Measurement	RSA Modulus Size [18]
80	1024
112	2048
128	3072
192	7689

From the above reference table, RSA has 80 bits of strength for 1024 modulus size and 2048 bits of RSA modulus size has the strength of 112bits approximately. Likewise, 7689bits of RSA modulus size has the strength of 192bits exactly. So compare the both RSA-1024 and RSA-2048, 32 times as hard to the fact the keys in RSA-2048. Finally, 2048bits of key size in RSA will be expected to the fact at 2040 to 2050 years. From till now, 2048 bits size of keys is more secure to transfer secret data confidentially.

In RSA, the computational cost with n bit of key size is big-Oh of n^2 for operations with public key and big-Oh of n^3 for private key operations. For RSA cryptosystem, memory space management is not a big constraint as a problem of storage capacity. Because in RSA, need to keep few sizes of keys in memory. RSA is provides secured data more and more with the help of large integers. Large integers are considered as too hard to factor.

H. Application of RSA in run-of-the-mill

Secure Socket Layer is one of the public key protocol developed by Netscape, it established perfect security for internet based communication with the help of TCP/IP, HTTP, and FTP etc. For online communication, message authentication and integrity is needed for every transaction. For the purpose of secure transaction, RSA is used to authentication process, which means exchange of keys is done between clients and server. For example, whenever the person wants to open a webpage starting like http://, the RSA Cryptosystem is used to validate the remote server's certificate. After that, RSA used for secured key exchange with the clients and server. There are three possible reasons for the popularity of RSA, Firstly RSA is freely available, anyone can use it for their security, secondly RSA uses same two functions for encryption and decryption as well as signature and finally RSA is applicable to any kind of data.

V. CONCLUSION

The contribution of this research paper is to concentrate on entire RSA in the aspect of cryptanalysis. In the cryptosystem, cryptanalysis plays a crucial aspect to enhance the security more and more. For the purpose of increasing security, plenty of research has going on. In cryptography particularly in public key system, RSA based research has placed in peak mode. The growth of attack against RSA is raised today. But still, RSA system has strongly secured to proceed the authenticated transactions. This paper covered all the attacks and countermeasures of RSA to hack secret keys. For RSA, the factorization threat has a vital role in hacking keys. The attacks named as, Brute Force attack, Timing attack, Side Channel analysis and Factorization threats are still continued to break keys of RSA. From the overview it is understood that RSA-2048 bits of key size are more secured for secret communications. Though many background works on attacks are done, still it is worthwhile for secured transactions and authentication.

REFERENCES

[1] Available: Http://en.wikipedia.org/wiki/cryptanalysis.
[2] Carlos Frederico Cid, "Cryptanalysis of RSA: A Survey", as part of the Information Security Reading Room, SANS Institute, pp: 1-10, 2003.
[3] Adamu Abubakar, Shehu Jabaka, Bello Idrith Tijjani, Akram Zeki, Haruna Chiroma, Mohammad Joda Usman, Shakirat Raji , Murni Mahmud, "Cryptanalytic Attacks on Rivest, Shamir, and Adleman (RSA) Cryptosystem: Issues and Challenges" Journal of Theoretical and Applied Information Technology, vol.61 No.1, PP: 37-43, March 2014.
[4] Robert Statica, "New Approach To Cryptanalysis of RSA", in CiteSeer ^{X},2003.
[5] Available: Http:// link.spriger.com/chapter/10.1007%2F978-3-642-36362-7_13.
[6] Don Coppersmith, "Small Solutions to Polynomial Equations and Low Exponent RSA Vulnerabilities", Journal of Cryptology (1997):10, PP: 233-260.
[7] Abderrahmane Nitaj, " Another Generalization of Wiener's Attack on RSA", in ACM Digital Library, AFRICACRYPT'08 proceedings of the Cryptology in Africa 1st International Conference on Progress in Cryptology, pp: 174-190,2008.
[8] Christophe Coupe, Phong, Nguyen, Jacques Stern, "The Effectiveness of Lattice Attacks Against Low-Exponent RSA", in Public Key Cryptography, PKC 1999. Lecture Notes in Computer Science, vol 1560, springer, Berlin, Heidelberg, pp: 204-218.
[9] Available: Http:// en.wikipedia.org/Wiki/ Correlation_Attack.
[10] Amar Pandey, "Correlation Attack on Stream Cipher", International Journal of Emerging Technology and Advanced Engineering, Vol 4, Issue 4, April 2014, pp: 864-869.
[11] Bernstein D.J.et al.(2013) Factoring RSA keys from Certified Smart Cards: Coppersmith in the wild. In: Sako k., Sarkar P.(eds) Advances in Cryptology – ASIACRYPT 2013. Lecture Notes in Computer Science, Vol 8270, Springer, Berlin, Heidelberg.
[12] Abderrahmane Nitaj, Mohamed Ould Douh, "A New Attack on RSA with a Composed Decryption Exponent", International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.4, December 2013.
[13] Abhishek Gupta, Vishal Sharma, "Modified Double Mod RSA Tested with Brute Force Attack", International Journal of Innovative Research and Development, Vol.3, Issue.5, pp: 815-818, May 2014.
[14] Onur Aclicmez, Cetin Kaya Koc, Jean-Pierre Seifert, "On the Power of Simple Branch Prediction Analysis".
[15] Andrea Pellegrini, Valeria Bertacco, "Fault-Based Attack of RSA Authendication", in ACM Library, pp: 855-860, March 2010.
[16] Amuthan Arjunan, Praveena Narayanan, Kaviarasan Ramu, " Securing RSA Algorithm Against Timing Attack", International Arab Journal of Information Technology, Vol. 13, No. 4, pp: 471-476, July 2016.
[17] Available: Http://crypto.stackexchange.com/questions/8687/security-strength-of-rsa-in-relation-with-the-modulus-size/8692#8692.

AUTHOR PROFILE

K. Berlin, received her M.Phil degree in Alagappa University, Tamil Nadu. Now she is pursuing her Ph.D (Computer Science) research in the same university. The field of her research is data security in cryptography. Four Research papers are published in Journals and Conferences.

S.S.Dhenakaran, a faculty member is working in the Department of Computer Science, Alagappa University, Tamil Nadu, India. He has acquired a doctoral degree in Computer Science and Engineering during 2008. Completed post graduation in mathematics during 1984, PG degree in computing during 2003. To his credit, he has more than 95 articles in international journal and conference. His field of research is Data Security using Cryptography. His familiar research fields are Optimization Techniques, Algorithms and Data mining.