Survey on Modular Attack on RSA Algorithm

Satish N. Chalurkar[1] , Nilesh Khochare[2] , B.B.Meshram[3]

[1]Computer Department, VJTI
Matunga(E),Mumbai,India
satishchalurkar1@gmail.com

[2]Computer Department,VJTI
Matunga(E),Mumbai,India
nileshkhochare@gmail.com

[3]Head of Computer Department
VJTI,Mumbai,India
bbmeshram@vjti.org.in

Abstract

This paper is devoted to the analysis of various cryptanalysis attack .This cryptanalysis attack mainly happens on the encrypted message which is to be passed over communication channel.The cryptanalysis attack is used to get the key from the encrypted message. Mod operation in the RSA algorithm plays an important role to break this algorithm.The Side Channel attack which include Timing attack and power analysis is used to break the RSA algorithm. There are various types of symmetric algorithm are discussed in this paper ,which is to be used to break the encrypted message.

Keywords: *Cryptanalysis, Kerckhoff's Principle, Attack Scenarios, RSA Algorithm, Attacks on RSA.*

1. Introduction

Cryptanalysis is the study of methods for obtaining the meaning of encrypted information, without access to the secret information that is normally required to do so. Typically, this involves knowing how the system works and finding a secret key. In non-technical language, this is the practice of "**code breaking"** or "**cracking the code".**

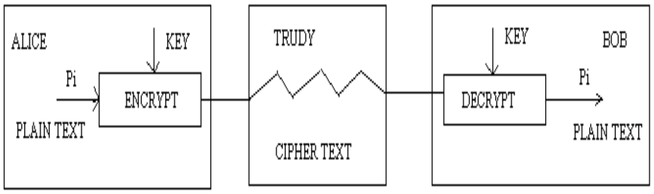
"Cryptanalysis" is also used to refer to any attempt to circumvent the security of other types of cryptographic algorithms and protocols in general, and not just encryption. Even though the goal has been the same, the methods and techniques of cryptanalysis have changed drastically through the history of cryptography, adapting to increasing cryptographic complexity, ranging from the pen-and-paper methods of the past, through machines like Bombes and Colossus computers in World War II, to the computer-based schemes of the present. The results of cryptanalysis have also changed - it is no longer possible to have unlimited success in code breaking, and there is a hierarchical classification of what constitutes an attack.

The paper starts with introduction; gives information about some related work in the section II .Section III discusses various attacks on RSA algorithm. The paper concludes with section IV.

2. Related Work

In cryptographic system, Sender knows plain-text and key to encrypt the message.i.e. to get the cipher-text. Similarly, Receiver knows the cipher-text and key to decrypt the message.i.e.,to get the plain-text. But, the cryptanalyst only knows cipher-text. His main aim to get the key for reading the encrypted message.

2.1 Who Knows What?



- Trudy knows the ciphertext
- Trudy knows the cipher and how it works
- Trudy might know a little more
- Trudy does not know the key

2.2 Block Cipher and Stream Cipher Cryptanalysis

1. Definition of Block Cipher

Block ciphers encrypt information by breaking it down into blocks and encrypting data in each block. A block cipher encrypts data in fixed sized blocks (commonly of 64 bits).

2. Definition of Stream Cipher

A stream cipher consists of a state machine that outputs at each state transition one bit of information. This stream of output bits is commonly called the running key. The state machine is nothing more than a pseudo-random number generator.

2.3 Attack Scenarios

In the case of block ciphers, the task of the adversary Trudy consists in recovering unknown parts of the plaintext, or better yet, recovering the secret key. Different attack scenarios can be distinguished depending on what information Eve can obtain, and to what extent she can interfere in the communication between Alice and Bob.
There are two main types of cryptanalysis attack.

1. Active attack

2. Passive attack

1. Active Attack
This type of attack will make the changes in the message when the key is get from the message. Cryptography provide the various services to the system such as integrity, authentication, privacy and non-repudiation. The attacker can change the services of the messages.

2. Passive Attack
This type of attack will does not make the changes to the message. But the attacker can view the message after getting the key. The attacker cannot change the services of message.

Here, there are the subtypes of the active and passive attack.

1. Man-in-the-middle attack:
This is the type of active attack. This differs from the above in that it involves tricking individuals into surrendering their keys. The cryptanalyst/attacker places him or herself in the communication channel between two parties who wish to exchange their keys for secure communication (via asymmetric or public key infrastructure cryptography).
The cryptanalyst/attacker then performs a key exchange with each party, with the original parties believing they are exchanging keys with each other. The two parties then end up using keys that are known to the cryptanalyst/attacker. This type of attack can be defeated by the use of a hash function. The attacker can changes the services of the message.

2. Known-Plaintext Attack:
A known-plaintext attack requires Trudy to have access to (parts of) the plaintext corresponding to the captured cipher text blocks. Using this information, the cryptanalyst attempts to deduce the key used to produce the cipher text.

3. Ciphertext-Only Attack:
This type of attack only assumes that Trudy (cryptanalyst) is capable of capturing encrypted blocks. The cryptanalyst has no knowledge of the plaintext. This requires accurate guesswork as to how a message could be worded. It helps to have some knowledge of the literary style of the cipher text writer and/or the general subject matter.

4. Chosen-Plaintext Attack:
It is also known as differential cryptanalysis . Some attacks only succeed when the plaintexts have a specific form. In order to mount such attacks, Trudy must find a way to influence the encrypted plaintexts.

5. Adaptively Chosen-Plaintext/Ciphertext Attack*:*
In order to mount one of the attacks described above, Eve will typically need to obtain the encryptions or decryptions of a whole series of chosen blocks.
When the choice of a certain block depends on the results obtained from previous blocks, the attack is called adaptive.

6. Brute-force attack:

This type of attack is a passive attack. The attacker can try all the possibilities of the key until the message is not broken. this is the very slow attack. Suppose that message is encrypted using the 56-bit key then the attacker can try all the possibilities up to 2^{55} bit. the next extension to the Brute-force attack is the Dictionary attack.in the Dictionary attack ,it will try also same possibilities but take only those key bit whose chances of success is more.

7. Timing/differential power analysis*:*

This is a new technique made public in June 1998, particularly useful against the smart card that measures differences in electrical consumption over a period of time when a microchip performs a function to secure information.

This technique can be used to gain information about key computations used in the encryption algorithm and other functions pertaining to security. The technique can be rendered less effective by introducing random noise into the computations, or altering the sequence of the executables to make it harder to monitor the power fluctuations

2.4 Kerckhoff's Principle

In most situations, it is fairly hard to keep an encryption or decryption algorithm completely secret: either Alice or Bob have to design and implement their own algorithm, or they have to trust a designer not to disclose the algorithm to others.

- Moreover, for each correspondent Alice wants to communicate with, she will need a different algorithm.
- The solution to this problem is to introduce a secret parameter and to construct parameterized encryption and decryption functions, in such a way that DK'(EK(P)) does not reveal anything about P as long as
- Instead of repeatedly having to design new secret algorithms, it now suffices to agree on a secret value for K, called the *key*.
- Typically, this key is a short binary string of 80 to a few hundred bits. Since the security of the resulting system only relies on the secrecy of the key, the functions E and D can as well be publicly shared.
- The principle that the full disclosure of an encryption algorithm should not affect its security as long as the key is secret is known as Kerckhoffs' principle.

2.5 Algorithm

Cryptanalysis Attack based on the following algorithm:
The above cryptanalysis attack is based on the following algorithm.
Cryptanalysis typically involves studying how resistant a cipher is against distinguishing attacks and key-recovery attacks.

- Distinguishing attacks are those that show that a cipher's structure exhibits some identifiable no randomness that allows someone to differentiate between a black box containing the cipher EK and a black box containing a random permutation
- Key-recovery attacks are those where a cryptanalyst strives to obtain the secret key K; thus any ciphertext can be decrypted back to the plaintext.
- The most naive key-recovery attack is the exhaustive key search, which involves guessing all possible values of K by brute force and, for each guess, verifying via trial decryption of the ciphertext if the guessed value is correct.

3. Discussion

RSA Algorithm uses MOD operation. The most important aspect of this algorithm is that we have to calculate the value of 'e' or 'd'.Here, We have discussed RSA algorithm, method for solving MOD problem and some common attacks on RSA algorithm.

3.1 Solving MOD problem

RSA Algorithm uses the MOD operation. The following algorithm gives the method in which we can solve any MOD problem.

M^e mod n (Given)
Step 1: e=expand in binary

Step 2: d=1 (Initially)
until bits are exhausted

Step 3:d=d*d mod n

Step 4: if (bi=1)
d=d*m mod n

Step 5: else goto Step 3.

Problem: 543^{16} mod 719

1	0	0	0	0
1/54	59	605	54	40

3.2 RSA Algorithm

RSA is a worldwide de facto standard and can be used for encryption, digital signatures and key exchange. The name RSA is derived from the last names of its three inventors:Rivest,Shamir and Adleman.It has become the most popular asymmetric algorithm, beyond the wildest expectations of its inventors.
The RSA Algorithm has the following steps.

Step 1: Select any p and q.The Value of p and q be any Prime number.

Step 2: n=p*q
z=(p-1)*(q-1)

Step 3:Choose 'd' in such a way that
GCD (d,z)=1

Step 4: e*d mod z=1
Public Key=k_u={e,n}
Private Key=K_r={d,n}

Step 5:Encryption
E(P)=C
P^e mod n=C

Step 6:Decryption
D(C)=P
C^d mod n =p

To Find the value of ‘e’ or ‘d’ , The Following Algorithm is used.
Right = Left -Q.Right
Y_{new} = x $_{old}$-Q.y_{old}
If(y_3=1)
Ans:y_2 iff (y_2>0)
If (y_2<1)
Ans:y_2 +z

The RSA Problem is Solved in the following Section:
Given=17
q=7
d=5
To Find:e=?
1. p=17 ,q=7

2. n=p*q
Z=(p-1)*(q-1)
=(17-1)*(7-1)
=96

3.d=5

4.(e*d) mod z=1

x_1 x_2 x_3	y_1 y_2 y_3	Q=[x_3/y_3]
1 0 z	0 1 d	
1 0 96	0 1 5	19
	0 -19 1	

Ans: e=y_2+z
e =-19+96
e =77

3.3 Attacks against RSA

Through the basic algorithm is secure, there are attacks on how RSA is implemented.
1. Forword search attack: If message space is predictable, attacker can decrypt C simply by encrypting all possible messages until a match with C is obtained.
2. Common modulus attack: If everyone is given the same modulus ‘n’ but different (e,d) pair, then under certain conditions, it is possible to decrypt the message without d.
3. Low encryption exponents: When encrypting with low encryption exponents (e.g., e = 3) and small values of the m, (i.e. $m < n^{1/e}$) the result of m^e is strictly less than the modulus n. In this case, cipher texts can be easily decrypted by taking the eth root of the cipher text over the integers.
4. RSA has the property that the product of two cipher texts is equal to the encryption of the product of the respective plaintexts. That is $m_1^e m_2^e=(m_1m_2)^e$(mod n) Because of this multiplicative property a chosen-cipher text attack is possible.

4. Conclusions

RSA algorithm is used for encryption, digital signature and key exchange. Kerckhoff’s principle states that, “Security of a cryptosystem must not depend on keeping the algorithm secret. The security depends only on keeping the key secret”. The various cryptanalysis attacks including passive and active attack can break the cryptosystem. The attacker can used modulus operator to break the RSA algorithm. Most attacks on RSA come from poor configuration or bad implementations.

References

[1] Nachiketh R. Potlapally, Anand Raghunathan, Srivaths Ravi,Niraj K. Jha, and Ruby B. Lee,” Aiding Side-Channel Attacks on Cryptographic Software With Satisfiability-Based Analysis”, IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 15, NO. 4, APRIL 2007

[2] Mohammad Zahiduf Rahaman and Mohammad Akram Hossain “Side Channel Attack Prevention for AES Smart Card”

[3] Johan Hastad and Mats Naslund ," The Security of All RSA and Discrete Log Bits".

[4] Mollin," RSA and Public-Key Cryptography" Journal of the ACM, Vol. 51, No. 2, March 2004

[5] David Wagner ,University of California at Berkeley,"Cryptanalysis of a Provably Secure CRT RSA Algorithm"

[6] Ellen Jochemsz and Alexander May," A Polynomial Time Attack on RSA with Private CRT-Exponents Smaller Than $N^{0.073}$ ",International Association for Cryptologic Research 2007

[7] Ramesh Karri, Kaijie Wu, Piyush Mishra, and Yongkook Kim, **"**Concurrent Error Detection Schemes for Fault-Based Side-Channel Cryptanalysis of Symmetric Block Ciphers", IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, VOL. 21, NO. 12, DECEMBER 2002

[8] Leo Dorrendorf,Zvi Gutterman The Hebrew University of Jerusalem and Benny Pinkas University of Haifa" Cryptanalysis of the Random Number Generator of the Windows Operating System" ,ACM Transactions on Information and System Security, Vol. 13, No. 1, Article 10, Publication date: October 2009.

[9] Raphael C.-W. Phan, Member, IEEE, and Mohammad Umar Siddiqi "A Framework for Describing Block Cipher Cryptanalysis", IEEE TRANSACTIONS ON COMPUTERS, VOL. 55, NO. 11, NOVEMBER 2006