Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 10, October -2017

Key Based Cryptanalysis of DES, AES and RSA and analysis of RSA using Randomization

GauranshKalla[1], Shalini Kumari[2], Aarti Dadheech[3]

[1] Computer Science Department, M.B.M. Engineering College Jodhpur
[2] Computer Science Department, M.B.M. Engineering College Jodhpur
[3]Computer Science Department, M.B.M. Engineering College Jodhpur

Abstract - *Network security means providing Confidentiality, Integrity, and Authentication of sensitive data while storing, processing or transmitting. The network needs security against attackers and hackers. Network Security includes two basic domains. The first is the information security i.e. to protect the information from unauthorized access, alteration and loss. And the second is devices security i.e. to protect data stored in devices and to resist hackers. Data security can be provided by using encryption system, and for encrypting any of the two types of keys can used namely, Public Key and Private Key. Public Key is the key used to encrypt a plain text and which is available for everyone and Private Key is the key used to decrypt the cipher text in order to make it readable and it is kept private as the name suggests. Cryptanalysis basically depends on key and algorithm. Even after knowing the encrypting algorithm it is not feasible to break the code. But, for any encrypted form, by any means if key could be found it becomes easy to decode. Complexity of Brute force attack depends on the key length. As longer key gives greater search spaces, it will take much more time to break the code. After a point brute force becomes impractical as it may lead to extensive search spaces.*

As per current scenario it is necessary to send a key in a secured manner which ensures privacy even if the channel is unsecured one and as we know internet is not a perfect secured channel. This makes it important, cryptosystems to be more powerful to work against cryptanalysis.

In this paper, we have discussed how to speculate the key in efficient way and hence reduce the complexity of breaking the code encrypted using most well-known modern algorithms DES, AES and RSA.

I. INTRODUCTION

The information and network are highly affected by the intruders who try to get into the systems in order to damage or steal the confidential matters. There is need of establishing strong security measures against attackers and hackers. Here network security not only means security in a single network rather in any network or network of networks.

II.

Now our need of network security has two main aspects, one is securing information i.e. electronic bits and bytes and other is the need of devices security i.e. physical equipment.

III.

On internet or any network of an organization, thousands of important information is exchanged regularly. This information can be accessed, modified and misused by an unauthorised third party.

In order to conduct safe communication the most important aspect one looks for is security. It is desired that a message should be read only by the person it has been sent for and no one else. For this purpose many techniques and methods are being used, available and introduced. With techniques, methods are introduced to crack them. Hence this area is one of the vital research areas.

Hence network security has become essential and vital there-fore terms like cryptography, cryptosystem, encryption, de-cryption, etc come into context. A cryptosystem is a com-bination of cryptographic algorithms needed to implement a particular security service, most commonly for achieving confidentiality. Typically, a cryptosystem consists of three algorithms: one for key generation, one for encryption, and one for decryption.

Encryption is the art of converting a plaintext(readable form) into a ciphertext(non-readable form) and reverse of it is called decryption. Now, there are two commonly used methods to implement this cryptosystem. First one is called Symmetric Key Cryptosystem i.e. only one key is used for encryption and decryption, this key is called Private key as it is kept secret and no one else knows about it except for the sender and receiver. Second method is called Asymmetric Cryptosystem i.e a pair of keys is used, one is called Public Key which is used to encrypt the data and the Public key is known to everyone but the main part is that for decryption we use a different key known as Private key, only the person having Private key can decrypt the ciphertext send and read it.

In this paper we are going to study some most well-known modern cryptography algorithms and indicate their possible

weaknesses. Finally various possible attacks are studied so that stronger security algorithms can be built and must present in future to continue securing information over the network.
Enigma, a machine for generating ciphertext, used during World War II, was breakable due to a flaw in it. Some common phrases were used in messages so they were decoded easily and that lead to guessing the key for the rest of the messages. After this, the search for a key was restricted based on some parameters which reduced the number of searches as well as time.Further, enigma breaking machine was made to searchin context with relevant scenario, resulting into less time consumed to break a code.

Similarly every cryptosystem has possibility of some flaws that make them vulnerable towards attacks. Before proceeding, dis-cussion about the nature of cryptosystems has been explained below:

A. DES :

DES stands for Data Encryption Standard. It is a symmetric key encryption used to encrypt data i.e. it uses the same PRIVATE KEY for encryption and decryption. It was first designed by IBM in 1975 and standardized in January 1977. DES is a block cipher that means the key is used to encrypt the data in blocks and not bit by bit. Each block size is of 64 bits and encryption is done by combination of permutation and substitution. For decryption the user just need to reverse the steps followed in encryption. DES has a key length of 56 bits.

B. AES :

AES stands for Advanced Encryption Standard. It is also a symmetric key encryption used to encrypt data i.e. it uses the same key for encryption and decryption. It was designed by Joan Daemen, Vincent Rijmen in 1998.AES is also a non fiestel block cipher. The block size in AES is 128 bits and the key size used in this encryption method can be any of 128 bits, 192 bits and 256 bits depending upon the number of rounds. There are N rounds in this cryptosystem and N depends on the key size user wants to use.

C. RSA

RSA cryptosystem was first described in 1977 by Ron Rivest,Adi Shamir and Leo Adleman(Hence the name RSA). It is a asymmetric key encryption that means there are two different keys used, one for encryption and other one for decryption. Key used for encryption is called public key which is known to everyone and the key used for decryption is called private/secret key as it resides with the receiver and is secured. It is most widely used algorithm and gets its security from Prime factorization.
User of RSA first need to choose two large prime numbers and these prime numbers should be kept private. Even if someone tries to break the encryption of RSA only the person having these two prime numbers can attempt to do so, breaking of RSA is known as RSA PROBLEM. RSA is comparatively slow process and that is why it is not so commonly used to encrypt the data rather it is used to encrypt the password of data files and then share it with others. Key size of RSA can be 1024 to 4096 bits

IV. ROLE OF KEY

A key plays vital role in cryptanalysis. To break the code the most important element needed is a key. In most cases, only a known key can decrypt the required text.

A. DES : -
1976: For a very small class of weak keys, DES can be broken with complexity 1.
1976: For a very small class of weak keys, DES can be broken with complexity 1.
1980: A time/memory tradeoff can break DES faster at the expense of more memory.
1982: For a very small class of semi-weak keys, DES can be broken with complexity 1.
1985: A meet-in-the-middle attack can break 6-round DES with complexity 252.
1987: the Davies Attack can break DES with complexity 256.2 ,slightly worse than brute force.
1990: Differential cryptanalysis can break DES with 247 chosen plaintext (full 16-round).
1993: Linear cryptanalysis can break DES with 243 known plaintexts.
1994: Differential-linear cryptanalysis can break 8-round DES with 768 chosen plaintexts plus 246 a brute-force search.
1994: the Davies attack can be improved, and can break DES with 252 known plaintexts.

Weakness of DES: It is apparent that DES is the weakest among all due to its smaller key length. Hence a small key size can be considered as one of the weak point of using DES algorithm for security purpose.

B. AES :

Several times different approaches have been applied to attack the code encrypted using AES. Some of such attacks are mentioned here:

1. XLS Attack in 2002 by Nicolas and Josef
2. Second attack was by Alex Biryukov, Dmitry Khovra-tovich, and IvicaNikoli in 2009 and brought down the complexity of this algorithm
3. This attack was made on AES-256 on 30 June 2009, but only able to break down till 10 rounds. therefore was not applicable to full AES

Weakness of AES: The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the plaintext into the ciphertext. The number of cycles of repetition is as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each con-taining four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext into the original plaintext using the same encryption key. The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/orinformation must be reviewed and certified by NSA prior to their acquisition and use.

C. RSA

RSA is most secured method till date. Breaking RSA with very large numbers is considered to be impractical. But in public key cryptography the problem is that everyone is aware of the algorithm which such cryptosystem follows. So the attack could be done on some of the elements of algorithm that may also lead us towards deducing possible key.
Weakness of RSA :

1) Brute force m: For small messages one could simply try to encrypt every possible message block, till a match is found with one of the cipher text blocks. This will make RSA or public key cryptography with small numbers insignificant to use. So it is necessary to use RSA with very large prime numbers.
2) Guess the value of d : To decrypt a cipher text encrypted using RSA one may start by guessing the private key d. It can be assumed that its value will remain somewhere in between 1 to n. Now, the com-plexity of breaking it depends upon the size of n. For comparatively smaller value of n it is easy to get the value of d and for somewhat very large number it seems impractical.Calculating value of d in d.e = 1 mod (n), time complexity can be reduced by some extent if d is selected randomly. Randomize Algorithm can be used to choose the value of d (from 1 to n). This will take at least less number of choices for d in order to break the code. It is possible that d may be related with the public key e. Once that relation has been formulated, finding or choosing the value d will be easy.
3) Pair (e, (n)): Its known that value of e is somewhere in between 1 to (n) and also (e, (n)) are co-prime. This information will give somewhat less pairs. Finding all such possible pairs and fetching them while calculating value of d will reduce the time complexity.
4) Factorization: In RSA with very large numbers, fac-toring takes an unreasonable amount of time in order to break the code. Factoring large number has not been proven equivalent to that of breaking the RSA algorithm. There may be another easier method that provide values of p and q or (n). As (n) ranges from n/2 till n-1, to guess a value of (n) is more efficient rather than calculating it by taking different values of p and q.

Improvement of RSA: Above study arises the possibility of breaking RSA in future which will make this cryptosystem weak. A way to improve RSA algorithm is to associate some values with the message to make it more unintelligible and increase the complexity of breaking it a little more than existing.

V. Conclusion

No matter how strong the cryptosystems pretends to be, there must be some flaw in them that make them weak or vulnerable towards cryptanalysis. DES is the most vulnerable cryptosystem due to small key length. AES to some extent is able to

survive attacks on key when the length is of 72 bits or more. RSA till now passed the attacks when the key length is of large numbers but it is possible to break this cryptosystem by reducing possibilities of choosing a private key value.
This paper suggests few methods of guessing the possible key of RSA, these techniques identifies the shortcomings of the algorithm and can be used to design a better cryptosystem. Moreover stronger and non-breakable keys can be designed in the future. Further research can be performed in this area to prove the practicalities of the techniques.

Acknowledgement

We would like to thank our HOD Dr. Anil Gupta Dept. of Computer Science, MBM Engineering College, for his guidance without which we would not be able to write this paper. A special thanks to Dr. Rajesh Purohit Dept. of Com-puter Science, MBM Engineering College, for his motivation. We are grateful to our friend MrsArpitaChoudhary, MBM Engineering College, for her support.

References

[1] P. Princy, "A Comparison of Symmetric Key Algorithm DES, AES, BLOW-FISH, RC4, RC6: A Survey, Volume 6 No. 05 May 2015
[2] Monika Agrawal, Pradeep Mishra, "A Comparative Survey on Symmetric Key Encryption Technique", Vol. 4 No. 05 May 2012
[3] Jing Li, Attack on DES
[4] Carlos Cid, Sean Murphy and Mathew Robshaw, "Algebraic Aspects of the Advanced Encryption Standard", ISBN 0-387-24363-1, 2006
[5] Bruce Schneier, AES Announced, October 15, 200
[6] Nikoli, Ivica, Distinguisher and Related-Key Attack on the Full AES-256", Advances in Cryptology CRYPTO 2009
[7] Bruce Schneier, Another new AES Attacks, Schneier on Security, A blog covering security and security technology, Retrieved 2010-03-11
[8] Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, Adi Shamir, Key Recovery Attacks of Practical Complexity on AES Variants with upto 10 Rounds, original on 28 January 2010
[9] Behrouz A. Forouzan, Cryptography and Network Security, 2007, Special Indian Edition

