Security Analysis of symmetric key and asymmetric key cryptography

Akash Sirohi[1], Kavita[2], Sahil Verma[3]

[1] Research Scholar, Lovely Professional University
[2,3] Associate Professor, Department of Computer Science and Engineering,
Lovely Professional University, Phagwara, India

ABSTRACT:

Nowadays technology spread like a spider web, which has both some advantages and disadvantages (like every coin has two sides) the one side (advantage) is that everything comes on the internet and the other side(disadvantage) is of securities issue which is growing at a faster rate. So to safeguard our data over the internet we use the process of cryptography in which original text is converted into ciphertext (transform text) refers to as encryption and ciphertext are converted into an original text called decryption. There are several techniques for encryption. In this paper, we discuss the difference between the several public-key cryptography and private-key cryptography techniques on the basis of security and find out the best way of encryption, after performing comparison we conclude that AES-192 and AES-256 is the best way for encryption.

INTRODUCTION:

The conversion of the original text into ciphertext (encrypted text) is called encryption and the conversion of ciphertext into an original text called decryption, the process of encryption and decryption is called cryptography. There are several algorithms for cryptography and these algorithms divided into two types one is symmetric and other is asymmetric cryptography. The process of cryptography in which one key is used for changing the original text to ciphertext (encryption) and ciphertext to original text (decryption) is called symmetric key cryptography and the process of cryptography in which two different keys are used called asymmetric key cryptography. The main problem in designing of encryption algorithms is the attacks done by a hacker or some unwanted attacks and the implementation cost also, but in this paper, we compare securities of algorithms against the unwanted attack and ignoring the cost of implementation. While comparing the security we neglect the running time and performance.

The remaining paper is divided into three sections such as section 2 gives the introduction of algorithms chosen, section 3 is the cryptanalysis of several algorithms and section 4 is the literature review.

ALGORITHMS:

1. Private key cryptography algorithms:
   1.1. Playfair cipher
   1.2. Hill cipher
   1.3. DES (Data encryption standard)
   1.4. Triple DES
   1.5. AES (Advance encryption standard)

2. Public key cryptography
   2.1 RSA (Rivest Shamir & Adelman)

Playfair cipher:

Playfair cipher is also known as Playfair square or Wheatstone-Playfair cipher, it is a private key cryptography (symmetric cryptography) technique. This technique proposed by CHARLES WHEATSTONE (Lord Playfair) in 1854[9]. In this technique pair of two letters is encrypted with the help of a 5*5 matrix by removing the duplicates letters from key and the position of I and j is the same. After removing the duplicates from key put the key in matrix row-wise and also the remaining alphabets. Then we make pairs of two letters of the original text and if the same letters occur then add the lowest occurrence frequency letters with them and then encrypt by intersection letters of row and columns.

Hill cipher:

This technique based on the linear algebra proposed by Lester s. hill in 1929[11]. This was the first technique that works on more than three symbols at a time.in hill, cipher key is in the form of m*m matrix where m is an integer

- Encryption:

  C=P*k mod26

- For decryption:

  P=C*k^-1 mod26 Where C=ciphertext,

P=plaintext K is in the form of a square matrix

P is in the form of a column matrix.

DES (Data Encryption Standard):

DES is used most widely and is one of the best technique in the world. It is a block cipher. This technique developed in 1970 at IBM and based on the design of Horst Feistel and reviewed by the National Bureau of Standards(NBS).DES is used to encrypt the block data of 64-bit and produces the cipher of 64bit, the key is the same for encryption and decryption which is 56-bit[8]. The plaintext of a 64-bit first divide in two parts having 32-bit each, then take the right part and apply the Feistel block process. After the Feistel XOR takes place between the output of permutation and the left part of text then the outcome becomes the right part for the next round and the right part becomes left part then repeats this process 16 times.

- Feistel Structure:
  I. Expansion
  II. XOR
  III. Substitution
  IV. Permutation

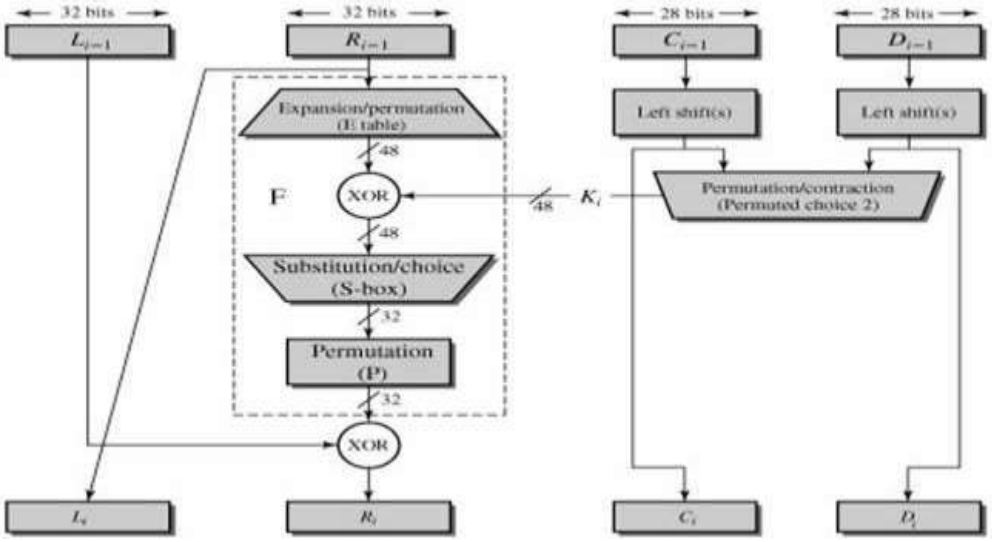

Figure1.1 DES (Feistel Structure)[13]

Triple DES:

It is a type of cryptography where block cipher is encrypted by applying the DES algorithm 3 times on it. It was published in 1995, it has sets of key or key bundles having 56-bit each(k1=k2=k3). It consists of 48 rounds(3 times of 16 rounds of DES).

- Encryption: C=Ek3(Dk2(Ek3(P)))[1][15].
  Where C=ciphertext and P=plaintext

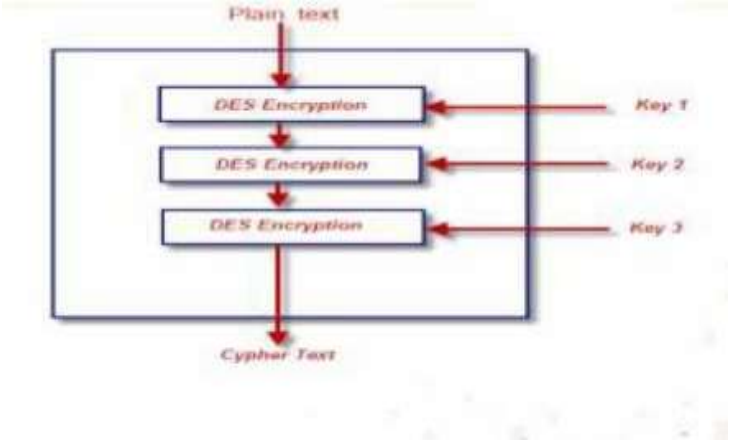

Figure 1.2: Triple-DES working[13]
For decryption : P=Dk1(Ek2(Dk3(C)))[15]

AES (Advance encryption standard):

Like DES, AES also a block cipher technique which is symmetric key cryptography, AES was proposed by Rijndael in October 2000[16].AES enhance security, AES is more advance then DES, in AES plaintext is of 128-bit, 192-bit and 256-bit having a key of the same length but there is a different number of rounds for different sizes of plaintext. 10 rounds for 128-bit, 12 rounds for 192-bit and 16 rounds for 256-bit[1]. There is a term called state means 4*4 matrix having plaintext.

Rounds	Size
10	128
12	192
16	256

- For every round there are 4 steps-

1.1. Sub bytes

1.2. Shift rows
1.3. Mix column
1.4. Add round key

- Final round

1.1 Sub bytes
1.2 Shift rows
1.3 Add round key

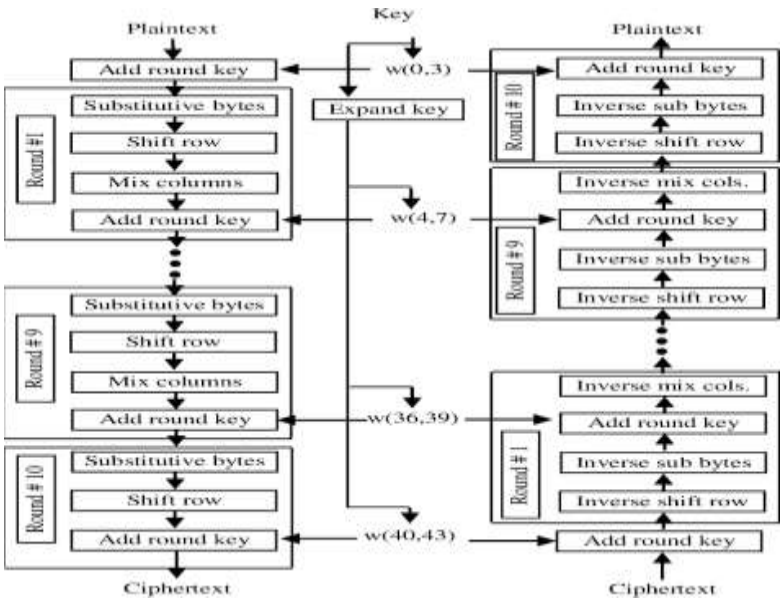

Figure 1.3, AES Working[13]

RSA (Rivest-Shamir-Adleman):

It is the first Asymmetric cryptographic technique or public key cryptographic algorithm which uses two keys for encryption and decryption.it was proposed by Rivest, Shamir, and Adleman and published in 1977.it depends on the two prime numbers, higher the numbers higher the security[5]. RSA contains four steps:

1 Key generation:
1.1 take two prime numbers p,q
1.2 n=p*q (n =length of a key) 1.3 λ(n)=(p-1)*(q-1)
1.4 gcd(e, λ(n))=1, 1<=e<=λ(n)
1.5 (d.e)mod λ(n) =1 , 1<=d<= λ(n)
2. Key distribution
2.1 Public Key (e, n)
3. Encryption
C=Me (mod n), where M=plaintext
4. Decryption M=Cd (mod n)

CRYPT ANALYSIS:

Playfair cipher:

The security of Playfair cipher is breaking if the attacker gets the plaintext and ciphertext or if he gets the ciphertext alone[9]. if the attacker has both text then the key can be generated easily and if he has ciphertext then there are two methods for breaking security:

- Brute force attack: in this technique, the key is searching by the gap between the occurrence of a pair of letters in the ciphertext and the known frequency of occurrence of letters. this method is used when ciphertext is of larger length. since Playfair cipher use 5*5 matrix, therefore, occurrence of matrix can

be of 25! which can be break easily manually.

- Shotgun hill-climbing method[10]: this method is used if the ciphertext is of smaller length, it has some steps.

Hill cipher:

The basic attack on hill cipher is a known-plaintext attack, if the attacker knows the plaintext and ciphertext then the key can be recovered because it is a linear process. another attack is if the attacker knew only ciphertext and this attack only possible for 2 by 2 matrix in practical.for 2 by 2 matrix use frequency occurrence of letters and try other combination of ciphertext digraphs until getting key[12].

K*P=Q MOD26

Q*P-1 (MOD 26)=K

Where Q is ciphertext and P is plaintext by guessing

DES(Data Encryption Standard):

DES has 16 rounds and key of length 56-bit and plain text is 64-bit, and each round has substitution and permutation so that breaking of DES is not so easy but can be a break.

- Brute force attack:
  It will always find the right solution with all possible key i.e 2^{56} approx 10 hours [2][8].
- Linear Cryptanalysis:
  DES can be a break with linear cryptanalysis with 2^{43} known plaintexts[14][2]. This technique points to the linear relationship between the ciphertext, plaintext, and key. Ciphertext=f(plaintext,key)

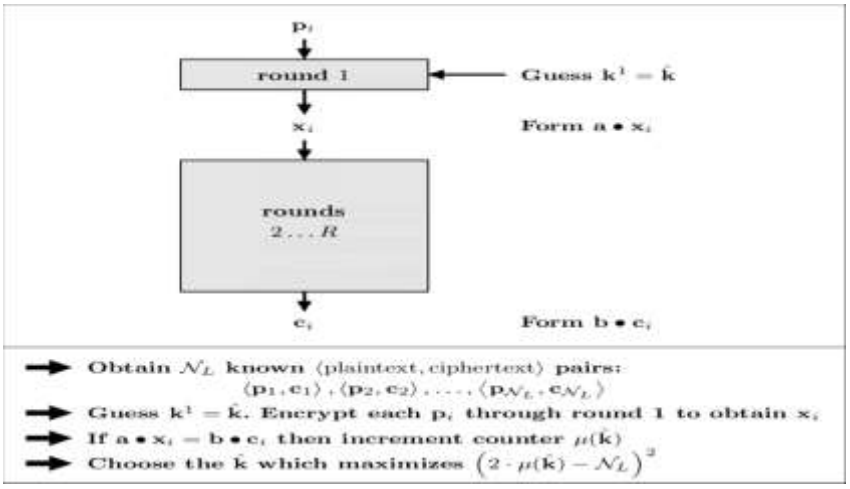

Figure 1.4: Linear cryptanalysis of DES[13]

- Differential Cryptanalysis:
  It can break DES with 2^{47} chosen-plaintext[14][2](full 16 rounds). this technique analyses the difference between the two plaintext message affects the differences between the corresponding ciphertexts.
- Improved Davies' attack[14]:
  Improved davies' attack can break the DES with 2^{52} known plaintexts.

Triple DES:

It has 3 independent keys that have a key of length 168-bit (3 DES keys of 56-bit), that's why it is more secure than basic DES. For breaking of triple-DES, there should be 2168 known- plaintext or chosen-plaintext but due to meet-in-the-middle attack the key2 reduce and effective key become 112-bit but when it is tested by NIST then effective security becomes of 80-bit, so it is declared as insecure in 2017 by NIST[15].

AES (Advance Encryption Standard):

AES is the most secure algorithm among all symmetric cryptography, it has 128-bit, 192-bit, and 256-bits length of the key and for high security 192 or 256-bits length of the key is used.

- Brute-force attack:
  Its security can be breaking by brute-force attack but it is practically possible only for 128-bits of key.192-bits and 256-bits can not be break by brute force in a lifetime.
- Related-key attack:
  Initially, it can break the AES with complexities 2^{119}, later it was improved with 2^{96} but this is not possible in practice[16].
- Structural attack:
  A most effective attack on substitution is a square attack, but this attack not successful in 192 and 256-bits in practically.
- Algebraic attack:
  In this attacker attack on the GF (2^8), 8 quadratic equations are generated i.e. there are 255 or 256 cases which is not possible for 192-bit and 256-bit[17].

Since none of the attacks compromise the full AES, therefore AES is the most secure algorithms specially 192 and 256-bits which are not compromised till now.

RSA (Rivest-Shamir-Adleman):

RSA uses the prime numbers in encryption and its security depends on those prime numbers only i.e. greater the prime numbers greater the security.

- Factoring:
  In this method, the main problem is created if two chosen prime number is multiplied and this is done in RSA. This method can break RSA in theory but not in practice[2]. Factoring can be done by various methods:
  1.1 Trial Division
  1.2 Pollard's p-1method
  1.3 Pollard's rho method
  1.4 Elliptic curve method
- Side channel analysis[5]

RSA can be a break for small prime numbers but can not be a break for larger prime numbers.

LITERATURE REVIEW:

- Monika Agarwal et al.[1] represented how the security of data becomes a major issue and how can we secure data by cryptography with the best techniques so that our data become secure and this paper provides the depth analysis of symmetric key cryptography about their performance and security. This paper explains the security comparison between symmetric and asymmetric key cryptography, this paper also explains the complexity of techniques. According to this paper, it is concluded that symmetric key cryptography is much secure and faster than asymmetric key cryptography.
- Prerna Mahajan et al.[2] provides the depth analysis of encryption techniques of symmetric and asymmetric keys of cryptography.in In this paper they analysis on DES, AES, and RSA for security and performance-related issue. According to this paper, we can conclude that AES takes less time for execution then RSA and all other algorithms and much more secure than all other encryption techniques.
- Poorna Chander [4] discusses the various security issues on network and cryptography techniques. This

paper also provides depth analysis of the security of techniques by doing cryptanalysis, The cryptanalysis of technique provides a clear look of security means how much secure techniques is. This paper deals with all types of encryption techniques means symmetric and asymmetric and attacks also. This paper concludes that symmetric key(AES) is more secure than asymmetric key cryptography because AES has more round and highly complex although RSA is also highly secure and its security depends on prime numbers

- Prof. Mukund et al.[3], explained about the function of cryptography in network security when transmission of data take place via wireless network, data security is the main aspect and with the help of cryptography confidentiality, integrity and authentication can be applied to data for security. this paper involves all best techniques of cryptography like DES, AES, RSA, MD5, SHA, HASH . This paper concludes that with the help of cryptography the data which is transmitted over the network can be secure and network security can be increased.
- Sangyub lee et al[5] checked the security of RSA with the help of device which is embedded with an analysis attack. They recover the secret key by collision analysis attack on Miller-Rain with the help of prime value. The device used for implementation has 512-bit modular exponentiations on ARM Cortex-M4 microcontroller recommended by FIPS 186-4.by the analysis attack on 512-bit they recover the secret key prime number with three failure. This paper concludes that RSA security is based on the prime numbers i.e higher the prime numbers higher the security so we have to use higher prime numbers for more security of our data.
- Ving Shi et al.[6] explained AES is used for edge computing which handles the sensitive data. According to this paper, the side-channel attack is the main concern for edge computing.in this paper, they find a relation between the "Euclidean distance between traces" and "Hamming distance between values" to determine the chosen plaintext and compromise the data security then AES is used for security. AES is one of the best techniques of cryptography for security because AES-192 and AES-256 are not compromised until now. This paper concludes that AES is best for security of data because after applying the AES the side-channel attack is not able to compromise the security and its success rate drop to 10%.
- Zilong Jiang[7], discusses the AES-192 security against multiple impossible differentials attack, the two types of attack for impossible differential for 4-rounds AES and 7-round AES with the same plaintext. The attack on the substitution method of AES for more security since these attacks are impossible in reality. This paper concludes that the time and space complexity of AES-192 is compromised by these attacks. The time, space and data complexities become $2^{109.2}$ 7- round AES encryption, $2^{86.5}$ bytes, and $2^{106.3}$ chosenplaintext.
- Isnar sumartono et al.[8] represented that for securing the data over the internet or network some cryptography techniques are required for security, in this paper, they encrypt the data by DES. DES has 16 rounds and 64-bit plaintext and 64-bit key initially. This paper concludes that DES can secure the data because in DES substitution algorithm is used and it has 16 rounds so it is difficult to break the s- box of 16 rounds. A brute force attack needs more than 10 hours to compromise the key.

CONCLUSION

In this paper, some cryptographic techniques were introduced and their security was compared. Among them some are private key cryptography (symmetric) having the one key for encryption and decryption and RSA is public key cryptography (asymmetric). According to a literature review, we can conclude that the more complex techniques more will be security since AES is more complex among all, therefore, AES is more secure for cryptography. RSA also has lots of computation and never easily breakable because of its multiplications of prime numbers and public key cryptography treated as more secure than private key cryptography but AES has more complex and that's why it is the more secure techniques and AES-192 and AES-256 not compromise until

now.

REFERENCES

[1] Monika Agarwal and Pradeep Mishra: a comparative survey on symmetric key encryption techniques, International journal on computer science and engineering, vol. 4, May 2012.

[2] Prerna Mahajan & Abhishek sachdeva: Performance and security analysis of DES, AES and RSA, IEEE Access,vol.6, October 2014.

[3] Mukund R.joshi, Renuka Avinash karkade : Network security with cryptography, International journal of computer science and mobile computing, vol.4 , January 2015 .

[4] Poorna Chander V: Security issues on cryptography and network security, international journal of computer science and information technology, vol. 7 ,issue 3, October 2016.

[5] Sangyub lee, Sung min cho,Heeseok kim and Seokhie hong: a practical collision-based power analysis on RSA prime generation, IEEE Access, vol. 7, April 2019.

[6] Ying shi and An wang : Adaptive chosen-plaintext collision attack on masked AES in edge computing, IEEE Access, vol. 7, May 2019.

[7] Zilong Jiang: Multiple impossible differentials attack on AES-192, IEEE Access, vol. 7, September 2019.

[8] Isnar sumartono and Andysah putera utama siahaan : Encryption of DES algorithm in information security, International journal for innovative research in multidisciplinary field, vol. 4, issue-10, October 2018.

[9] https://en.wikipedia.org/wiki/Playfair_cipher

[10] https://www.commonlounge.com

[11] https://en.wikipedia.org/wiki/Hill_cipher

[12] http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-hill-cipher

[13] http://www.google.com/images

[14] https://en.wikipedia.org/wiki/Data_Encryption_Standard#Security_and_cryptanalysis

[15] https://en.wikipedia.org/wiki/Triple_DES

[16] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[17] http://www.math.wisc.edu/~boston/nover.pdf