SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY

Vibhuti sharma[1],Sushma Yadav[2]

[1,2]Raj Kumar Goel Institute of Technology for Women, (India)

ABSTRACT

Internet applications are increasing rapidly, so there is a need to protect such applications. These applications can be protected by the use of cryptography. Cryptography is a method used for secure transfer of massages over a network. The cryptography method used are private key cryptography (symmetric) and public key cryptography (asymmetric). Symmetric key cryptography includes DES whereas asymmetric key cryptography includes RSA. This paper includes the description about RSA and DES and about the various vulnerabilities and their countermeasures. Also it comprises about the comparisons and performance analysis of the two methods i.e, symmetric and asymmetric.

Keywords: Asymmetric Key, Rivesi-Shamir-Adleman (RSA), Data Encryption Standard (Des), Symmetric Key.

I. INTRODUCTION

For the purpose of security of information the encryption algorithms used are:
Symmetric (private) and Asymmetric (public) keys encryption. In symmetric keys encryption or secret key encryption, a single key is used for the purpose of encryption and decryption. The key is being shared by both sender and receiver. The key is being used is most important in encryption and decryption. If the key that is being used is week then the chances of attack increase. The key that is being used is the strength of symmetric key encryption. Some of the strong and weak keys of cryptography algorithms such as RS2 , DES, 3DES, RC6, blowfish, and AES. 64-bit key is used by RS2 and DES both whereas there 64-bit keys are used by triple .the main drawback of symmetric key encryption is the secure transmission of massages over a malicious network i.e, the problem of key distribution.
The problem of key distribution is solved using Asymmetric key Encryption. Two keys are used in Asymmetric: public key for encryption and private is known only to user.

Description of the most common symmetric encryption techniques

DES

Des is a 64-bit block size and 64-bit size. At the time, many attacks and method recorded the weakness of DES, which prove it to be an insurance block cipher.

3DES: is an important over of DES : it consists of 64 bit block size and 192 bits key size in this standard the encryption method applied 3times to DES which increase the encryption level and the average safe time.

RC2:is a 64-bit symmetric block cipher having a variable key size that range from 8 to 128 bits .RC2 is vulnerable to a related-key attack

Blowfish is block cipher 64-bit block which is used as a replacement for DES algorithm .It takes as input a variable -length key which ranges from 32bits to
448bits (default 128 bits).It is license-free and available free for all uses. It consists
Of 14 rounds or less

AES is a block cipher .It has a variable key length of 128, 192, or 256bits.itencrypt data blocks of 128 bits in 10, 12 and 14 rounds based on the key size. AES encryption is fast; it can be implemented on several platforms mostly in smalls Devices.

RC6 is block cipher which is derives from RC5 .It was designed to fulfill the requirement of the Advanced Encryption Standard competition .RC6 has a block Size of 128 bits and keys size of 128, 92 and 256 bits.

Public key cryptosystem is more reliable in the areas of confidentiality and authenticity. This type of cryptosystem is based on mathematics calculations instead of substitution and permutation as in symmetric cryptosystem .In thisAlgorithms two key are used i.e. one for encryption and decryption. Public keyIs used for encryption and private key is used for decryption of data. ThisCryptosystem evolves due to the problems associates with the digital signature For the purpose of authenticity of data .The keys used in public cryptosystem are private key and public key .Private key is kept secret by the user and publickey is known to all the most common algorithms used for public key cryptosystem is RSA.

II. DESCRIPTION OF RSA ALONG WITH EXISTING VULNERABILITIES AND THEIR COUNTER MEASURES

2.1 RSA

It is a block cipher where the plain text and cipher text lies between 0 and
n-1 for some n, where n is an integer .It means ,the block size must be less
than or equal to log2(n);in this, the block size is of 2k bits, where$2k<n<=2k=1$.

The form of encryption and decryption are as follow, for some plan text M and cipher text C=PE mod n and P=CD mod n. the value of n must be known by the both sender and receiver.

The sender knows the value of e, and only the receiver knows the value of d. thus, this is known as a public key encryption algorithm. The public key includes n, the modulus, and e, the public exponent. The private key includes n, the modulus, which is public and appears in the public key, and d, the private exponent, which should be keep secret.

the RSA scheme is as follow:

select two large prime number p ,q in such a way that p is not equal to q, randomly and independently of each other.
Compute n=p*q
Calculate the quotient(n)=(P-1)(q-1)
Select integer ales than (n) and
Relatively prime with (n).
Compute d such that d*e(Mod(n))=1
Publish the public key pair PU={e,n}
Publish the private key pair PR={d,n}

RSA Encryption

It is a block cipher. In this the input binary text is divided into 8 bit apart. Firstly the first 8 bit text is converted into an integer form. After that a public key is a taken from key generator and then encryption operation is perform for that integer .taken an example 'M' is an integer then we encrypt 'M' by following

C=P*mod n

We calculate the value of C and after that we will covert c into a binary format .now we will make binary value of Cas 16 bit length and record that result in cipher txt.

RSA Decryption

In a decryption process, the input binary text is divided into 16 bit apart. The first 16 bit text is already converted into an integer form. After that a private key 'd' is taken from key generator and decryption operation will be performed for that integer. Take an example 'C' is an integer then we encrypt 'C' by following

P=C mod n

DES

it is a -block cipher. It encrypts data in the blocks of size 64 bits each. The same algorithm and key are used for both encryption and decryption , with some differences. The length of the key is 56 bits.

DES Key Generation.The initial key generation is of 64 bits. Before , the DES process starts, every eight bits of the key is discarded so as to produce a 56 bit key.

DES Encryption

DES Encryption is based on the two concepts of cryptography i.e., substitution and transportation techniques. DES consists of 16 rounds. The step of substitution and transportation is performed on each step as follow:

In the first step, the 64 bit plain text block passes through an initial permutation function. Initial permutation is performed on the block of plain text. Now, the initial permutation function produces two halves of the permulated block i.e,left plain text(LPT) and right plain text(RPT). Then, each of the LPT and RPT goes through 16 rounds of the encryption process. At the least, LPTand RPT are joined a final permutation is performed on the resulted block and thus produces 64 bit cipher text.

DES DECRYPTION

DES decryption process is same as that of encryption process but with some changes. The only difference between the two is the reversal of key portions. If original key K was divided into sub keys K1,K2,K3…..K16 for the 16 encryption rounds, then for the decryption, the keys are used in reverse order i.e, K16 ,K15,K14……K1

DES vulnerabilities and their counter measures:

DES algorithm suffers from some simple Relationships in the keys.in DES, simple relationship is of complementary nature due to which complementary relations between the keys resulted in a complementary relationship between the keys resulted complementary relationship between the obtained cipher text. The DES algorithm is mostly vulnerable to Linear Crypto analysis attacks. By such an attack, the Algorithm can be

broken down using plaintexts in its 16 rounds. This vulnerability may lead to a risk while encrypting bulk of data may be predicated with keys that are constant.

III. COMPARISON

Comparison of symmetric and asymmetric key cryptography on the basis of performance analysis:

1. The approach used in DES is Symmetric while in RSA, asymmetric approach is used.

2. In DES, encryption and decryption is faster while in RSA, it is slow.

3. Key distribution is very difficult in DES while in RSA, distribution of keys is easy.

4. DES has a complexity O(Log N) while in RSA complexity is O(N3).

5. Security is moderate in DES while in RSA security is highest.

IV. CONCLUSION

This paper presents the performance analysis of the asymmetric and asymmetric Encryption algorithm. The algorithms are DES and RSA along with their working mechanisms. Several Points are concluding. First, despite of the key distribution, DES is more suitable for the applications, whose highest priority is decryption. Asymmetric key cryptography system provides higher security in all ways. Second, several loops holes exists in their working system. Corresponding to every vulnerability there is an alternative countermeasure but they are not so secure as the internet application demands are increasing day by day. Due to the rapid advancement of technologies like quantum computing, these algorithms are no.

REFERENCES

[1] ALBERT, A. A "Some mathematical as- pects of cryptography," presented at the AMS 382nd Meeting, Manhattan, Kans.,

[2] Nov 22, 1941. BERLEKAMP, E. R. Algebrazc coding theory, McGraw-Hill, New York, 1968. HOFF77 BRANSTAD, D. 3."Hellman's data does not support his conclusion," IEEE Spectrum 16, 7 (July 1979), 41 HORO74 BRIGHT, H S, AND ENISON, R L. "