IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011
ISSN (Online): 2231-5268
www.ijcsms.com

Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures

Yogesh Kumar[1], Rajiv Munjal[2], Harsh Sharma[3]

[1]Sr. Lecturer in CSE Deptt, BPR College of Engg Gohana (Sonipat)
yogs_crsce@yahoo.com

[2]lecturer in CSE Deptt., CBS Group of institution (Jhajjar),
rajiv.munjal@rediff.com

[3]Lecturer in CSE Deptt, BPR College of Engg Gohana (Sonipat)

Abstract

Internet and networks application are growing very fast, so the need to protect such application are increased by using cryptographic methods. The two widely accepted and used cryptographic methods are symmetric and asymmetric. The DES ideally belongs to the category of symmetric key cryptography and RSA belongs to the category of asymmetric key cryptography. This paper comprises of brief description of RSA and DES cryptography algorithms and their existing vulnerabilities along with their countermeasures. Besides this, there is a theoretical performance analysis and comparisons of symmetric and asymmetric cryptography.

Keywords: *Asymmetric Key, Rivest-Shamir-Adleman(RSA), Data Encryption Standard(DES),Symmetric Key.*

1. Introduction:

Many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. The key should be distributed before transmission between entities. Keys play an important role. If weak key is used in algorithm then everyone may decrypt the data. Strength of Symmetric key encryption depends on the size of key used. For the same algorithm, encryption using longer key is harder to break than the one done using smaller key. There are many examples of strong and weak keys of cryptography algorithms like RC2, DES, 3DES, RC6, Blowfish, and AES. RC2 uses one 64-bit key .DES uses one 64-bits key. Triple DES (3DES) uses three 64-bits keys while AES uses various (128,192,256) bits keys. Blowfish uses
various (32-448); default 128bits while RC6 is used various (128,192,256) bits keys [1-4]. But main problem with this is secure transmission of key over the malicious network. Asymmetric key encryption or public key encryption is used to solve the problem of key distribution. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption
(E.g. RSA and Digital Signatures). Because users tend to use two keys: public key, which is known to the public and private key which is known only to the user. There is no need for distributing them prior to transmission. However, public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices [1].

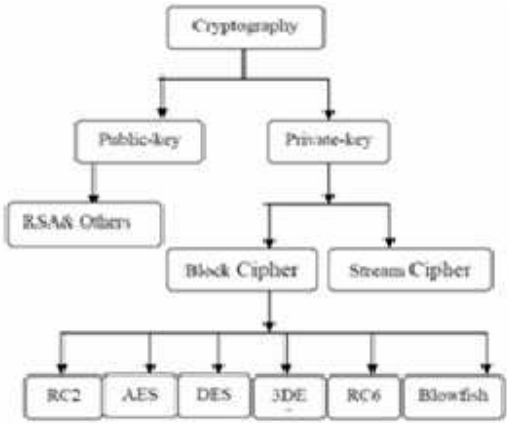

Fig 1

Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [2].The most common classification of encryption techniques can be shown in Fig. 1

Brief definitions of the most common symmetric encryption techniques are given as follows:

DES: (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and

IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011
ISSN (Online): 2231-5268
www.ijcsms.com

Technology).DES is (64 bits key size with 64 bits block size) . Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block
cipher [3],[4].

3DES is an enhancement of DES : It is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods [3].

RC2 is a 64-bits block cipher with a variable key size that range from 8 to 128 bits. RC2 is vulnerable to a related-key attack using 234 chosen plaintexts [3].

Blowfish is block cipher 64-bit block - can be used as a replacement for the DES algorithm. It takes a variable-length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish is unpatented, license-free, and is available free for all uses. Blowfish has variants of 14 rounds or less. Blowfish is successor to Two fish.

AES is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. it encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices [2]. Also, AES has been carefully tested for many security applications.

RC6 is block cipher derived from RC5. It was designed to meet the requirements of the Advanced Encryption Standard competition. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. Some references consider RC6 as Advanced Encryption Standard [4].

The other type of cryptography is the greatest and perhaps the only true revolution in the entire history of Cryptography. Public key cryptography provides a radical departure from all that has gone before. The two major reasons which made Public key cryptography algorithms more reliable in the areas of confidentiality key distribution and authentic. These algorithms are based on mathematical calculations rather than substitution and permutations like the symmetric cryptosystem. These algorithms use two keys in contrast to symmetric algorithms which uses only one key. These public key cryptosystem evolved from an attempt to attack two of the most difficult problems of key distribution and the other problem was associated with the digital signatures for the purpose of authenticity of data and message.

Public key algorithm relies on one key for encryption and a different but related key for decryption. It is computationally infeasible to determine key given only the knowledge of cryptographic algorithm and the encryption key. The two keys in Public key cryptographic algorithm are referred as public and private key. Invariably the private key is kept secret and is only known to the user that holds it. The most important public key cryptographic algorithm is RSA which have accepted and wisely used now a days. [3][4].

2. Description of Asymmetric cryptographic algorithm (RSA) Along with existing vulnerabilities and their countermeasures:

2.1 RSA:

RSA scheme is a block cipher in which the plain text and cipher text are integers between 0 and n-1 for some n. That is, the block size must be less than or equal to log2(n); in practice, the block size is 2k
bits, where $2^k < n <= 2^{k+1}$. Encryption and Decryption are of the following form, for some plain text M and cipher text $C = P^e \bmod n$ and $P = C^d \bmod n$.

Both the sender and the receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public key encryption algorithm.

The public key consists of n, the modulus, and e, the public exponent. The private key consists of n, the modulus, which is public and appears in the public key, and d, the private exponent, which must be kept secret.

We are now ready to state the RSA scheme. The following are the steps to generate the public and the private keys. Choose two large prime numbers p, q such that p is not equal to q, randomly and independently of each other.

Compute n = p * q

Compute the quotient Ø (n) = (p-1) (q-1)
Choose an integer e such that 1< e <Ø (n)
which is co prime to Ø (n)
Compute d such that d*e (mod Ø (n) = 1

Finding the large prime numbers is usually done by testing random numbers of the right size with probabilistic primarily tests which quickly eliminate virtually all non-primes. p and q should not be 'too close'. Further more if p-1 and q-1 has only small prime factors, n can be factored quickly and these values of p and q should therefore be discarded as well. It is important that the secret private key d should be large enough [3][4].

IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011
ISSN (Online): 2231-5268
www.ijcsms.com

2.1.1 RSA Encryption

RSA is a block cipher mechanism. So we divide the input binary text into 8 bit apart. We will convert the first 8 bit text into an integer form. After that we take a public key from key generator and perform encryption operation for that integer. For example 'M' is an integer then we encrypt 'M' by performing

$$C = P^e \bmod n$$

After calculating the value of C we will convert C into binary format. After that we will make binary value of C as 16 bit length and print that result in cipher txt. Now we will take another 8 bit text and repeat the above process.

2.1.2 RSA Decryption

Divide the input binary text into 16 bit apart. We have converted the first 16 bit text into an integer form. After that we take a private key 'd' from key generator and perform decryption operation for that integer. For example 'C' is an integer then we encrypt 'C' by performing

$$P = C^d \bmod n$$

2.2 Vulnerabilities and their countermeasures:

- RSA private keys are likely to be weak if their value is less than $N^{0.292}$ .It is believed that for secure implementation private exponent to be larger than $N^{0.5}$.
- The system(N,D,E) is likely to be insecure if (p-1), for the p that is one of the factors of N, is a product of small primes.
- If p and q that are used to generate N are too close to each other, then Fermat's factoring is possible, making the system highly insecure. Thus, the difference between the two primes should be at least $N^{0.25}$.
- When RSA is implemented with several key pairs ,the implementer often choose to use the same N for all key pairs, thus saving computation time. However, since the private and public exponents together always assist in factoring N, every single member of the system will be able to factor N with his key pair and use that result to invert any public exponent to the corresponding private exponent. So it is necessary to generate a new N value for each key pair. [5][6]

3. Description of Symmetric cryptographic algorithm (DES) Along with existing vulnerabilities and their countermeasures:

3.1 DES:

DES is a block cipher. It encrypts data in in block of size 64 bit each. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.

3.1.1 DES Key Generation

The initial key consists of 64 bits. However, before the DES process even start, every eight bit of the key is discarded to produce a 56-bit key.

3.1.2 DES Encryption

DES Encryption is based on the two fundamentals attributes of cryptography: substitution and transportation. DES consists of 16 steps, each of which is considered as round. Each round performs the steps of substitution and transportation as:

In the first step, the 64-bit plain text block is handed over to an Initial Permutation(IP) function. The Initial Permutation is performed on plain text. Next, the IP produces two halves of permutated block; say Left Plain Text(LPT) and Right Plain Text(RPT)[2][3].Then, each LPT and RPT go through 16 rounds for encryption process. In the end, LPT and RPT are rejoined and a Final Permutation is performed on the combined block and result of this process produce 64-bit cipher text.

3.1.3 DES Decryption

DES Decryption process is same as encryption with some minor differences. The only difference between is the reversal of key portions. If original key K was divided into K1, K2, k3,…….k16 for the 16 encryption round, then for decryption , the key should be used as K16, K15, K14,……K1.[4]

3.2 DES vulnerabilities and their counter measures:

- DES algorithm suffers from Simple Relations in its keys. In DES, simple relationship is of complementary nature due to complementary relations between keys result in a complementary relationship between the resulting cipher text. This vulnerability reduces the algorithm strength by one bit.
- The DES algorithm is vulnerable to Linear Cryptanalysis attacks. By such an attack, the

IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011
ISSN (Online): 2231-5268
www.ijcsms.com

algorithm in its sixteen rounds can be broken using 2^{43} plaintexts. This vulnerability raises a notable risk when encrypting bulk data that may be predictable with keys that are constant.

- Eli Biham and Adi Shamir presented a differential attack, by which a key can be recovered in 2^{37} time using 2^{37} cipher texts taken from a pool after encrypting 2^{47}

Comparison:

Performance analysis and comparison of symmetric and asymmetric key cryptography:

Method	DES	RSA
Approach	Symmetric	Asymmetric
Encryption	Faster	Slow
Decryption	Faster	Slow
Key distribution	Difficult	Easy
Complexity	O(Log N)	O (N3)
Security	Moderate	Highest
Nature	Closed	Open
Inherent Vulnerabilities	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle attack
Vulnerabilities cause	Weak key usage	Weak implementation
Secure Services	Confidentially	Confidentially, integrity, non repudiation

3. Conclusions:

This paper presents a theoretical performance analysis of selected symmetric and asymmetric encryption algorithm. The selected algorithms are DES and RSA along with their working mechanisms. Severa1points are to be concluded. First, despite the key distribution, DES is more suitable to the application, which has the decryption as the highest priority. There is no doubt that, an asymmetric key cryptographic system provides high security in all ways.

Second; several loop holes are to be existed in their working systems due to probability of deadness occur is prevailed. However, corresponding to every vulnerability there is an alternative countermeasure but they are not so secure as the internet growing application demands. Due to the rapid advancement of technologies like Quantum Computing, these algorithms are not so longer safe.

4. References:

[1] Hardjono, "Security In Wireless LANS And MANS,"Artech House Publishers 2005.

[2] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309 .

[3] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength Against Attacks."I BM Journal of Research and Development, May 1994, pp. 243 -250.

[4] Atul khate, "Cryptography and Network Security, 2nd Ed," Tata Mcgraw hill, 2009, PP. 87-2004

[5] Dan Boneh and Glenn Durfee, "Cryptanalysis of Low-Exponent RSA"

[6] Benne De Weger, "Cryptanalysis of RSA with Small Prime Difference" June, 2002

[7] Eli Biham and Adi Shamir, "Differential Cryptanalysis of Full DES"

[8] Eli Biham, Alex Biryukov, "An Improvement of Davies Attack on DES", Journal of Cryptology, pages =461—467

[9] Results of comparing tens of encryption algorithms using different settings- Crypto++ benchmark- . Retrieved October 1, 2008

[10] S.Z.S. Idrus,S.A.Aljunid,S.M.Asi, "Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers," IJCSNS International Journal of Computer Science and Network Security, VOL.8, No.1, January 2008 ,PP 20-25.