COMPARATIVE STUDY OF PRIVATE AND PUBLIC KEY CRYPTOGRAPHY ALGORITHMS: A SURVEY

Priti Bali[1]

[1]*Assistant Professor, Computer Science Department, D.A.V. Institute of Management, Haryana, India*

Abstract

Internet has revolutionized many aspects of our daily lives. Nowadays Internet is used for millions of applications. Many people depend on Internet for several activities like on-line banking, on-line shopping, on-line learning and on-line meetings etc. Huge amount of data travels over the network. Security of data over the network is a critical issue. Making a network secure involves a lot more than just keeping it free from programming errors. Network Security refers to the protection of valuable data against Interception, Interruption, Modification, Fabrication and Non-repudiation. Computer networks are inherently insecure so to protect data over the networks we need some mechanism. Cryptography came into existence to ensure data security. There are various threats to data: Backdoors, denial-of-service attack, direct-access attack, eavesdropping, exploits, indirect-attacks and social engineering and human-error. Cryptography provides protection against security threats. Cryptography means secret writing, the content of original text is scrambled to produce coded text and job of intruders becomes difficult. Secret-writing is the strongest tool of cryptography which protects the data. Cryptography is used to ensure confidentiality, integrity and availability of data by using private and public key cryptography algorithms. Private and Public key algorithms are used to transform original (readable) messages into unreadable jumbles. This paper describes the comparison of Private (symmetric) and Public (asymmetric) key algorithms.

Keywords: *Plain Text, Cipher Text, Key, Encryption, Decryption, Intruder, Cryptanalysis, Cryptology, Cryptosystem, Cryptography, DES, RSA.*

---***---

1. INTRODUCTION

Use of Internet is growing rapidly. So, providing security to the data over networks has become a critical issue nowadays. Data over networks is insecure; it should be disclosed only to the intended recipients not to everyone. Data is more prone to attacks while transmitting in the network. Cryptography came into existence to provide solutions to all the issues of network security. Cryptography provides security to data while it is in network. It makes the messages immune to various attacks by converting the original message into coded message. Encryption is a process which is used for converting the original message into disguised message at the sender end. Various cryptography algorithms (private and public) are available which are used for concealing the content of message from all except the sender and the receiver.

1.1 Basic concepts of Cryptography

Plain text: Plain text is the message that a person wants to communicate. It is the original message which is to be encrypted at the sender end.

Cipher text: Cipher text is the message that is not comprehensible to anyone. It is the coded message which is to be decrypted at the receiving end.

Intruders: Intruders alter the message with wrong intentions. Intruders intercept, interrupt and fabricate the original messages and send their own disguised messages.

Encryption: Encryption is the process of converting Plain text into Cipher text. It requires Encryption algorithm and a key. The best method for protecting the confidentiality of information transmitted over wireless networks is to encrypt all wireless traffic. The most effective way to secure wireless network from intruders is to encrypt, or scramble, or disguise, communications over the network. Most wireless routers and access points have a built-in encryption mechanism [1].

Decryption: decryption is the process of converting Cipher text into plain text. It requires Decryption algorithm and a key.

Key: Key operates on the plain text and converts it into cipher text. The real secrecy of cryptography is in the key. It is used for both processes: Encryption Process and Decryption Process. Key could be a number, function or an algorithm. Keys perform the transformations. For example: ABC (plain text) becomes DEF (cipher text) by applying a key. (The key is: shift all the letters by 3)

Cryptanalysis: Cryptanalysis means “code breaking”. Art of breaking cipher text is known as cryptanalysis.

Cryptology: The art of formulating ciphers (cryptography) and breaking ciphers (cryptanalysis) is collectively known as cryptology.

Cryptography: Cryptography means "code making", it is a process of converting plain text (original message) into cipher text (coded message). This message transformation is done to make messages secure and immune to attacks over the network.

Cryptosystem: The system which is used to implement cryptography is known as cryptosystem.

1.2 Cryptography provides Protection against the following Security Threats:

Interception: Interception happens when an unauthorized user gain access to valuable data. In this case, the protection is aimed to ensure confidentiality of the data.

Interruption: Interruption happens when data become unavailable, unusable or destroyed. In this case, the protection is aimed to ensure availability of data.

Modification: Modification means some unauthorized user has altered the data. In this case, the protection is aimed to ensure integrity of data.

Fabrication: Fabrication happens when an unauthorized person inserts forged data in a file. In this case, the protection is aimed to ensure authenticity of data.

Non-Repudiation: Non-Repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Non-Repudiation can be achieved by the use of digital signatures, confirmation services, time stamps and unique biometric information [2].

Cryptography is used for controlling all the security threats. Secret-writing (coded/cipher text) is the strongest tool because well-disguised data cannot be read, modified and fabricated easily. Different types of algorithms are used for converting Plain text (original message) into Cipher text (coded message).

1.3 Cryptography Algorithms can be classified into Two Categories:

- Private key cryptography algorithms
- Public key cryptography algorithms

1.3.1 Private Key Cryptography Algorithms:

Private Key algorithms are also known as symmetric key algorithms. In symmetric key algorithms, encryption and decryption processes are performed using the same key. It is also known as conventional encryption and decryption [3]. In private key algorithms, encryption and decryption keys are mathematically related (usually inverse of each other). Private key algorithms are efficient and take less time to encrypt messages. These algorithms are used to encrypt and decrypt long messages because size of key is small.

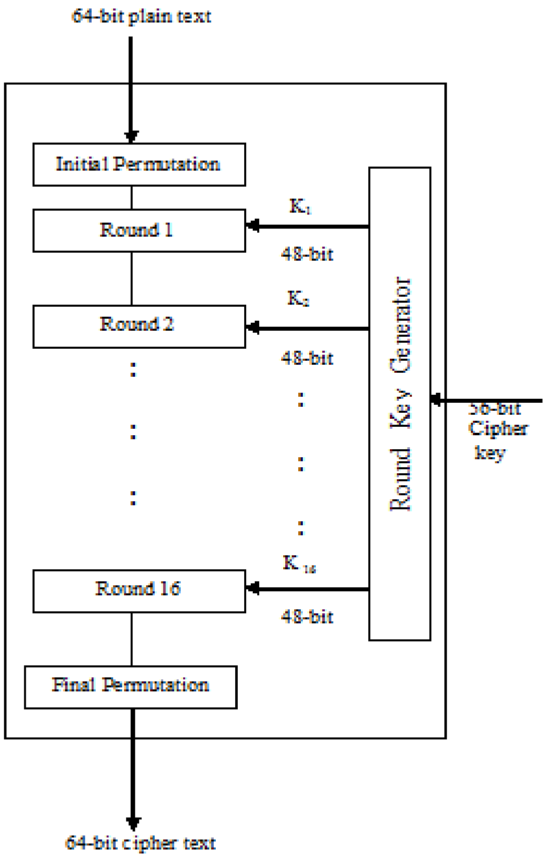
1.3.2 Public Key Cryptography Algorithms

Public key algorithms are basically used for key distribution. Public key algorithms are also known as asymmetric key algorithms. In asymmetric key algorithms two keys are used: A private key and a public key. Public key is used for encryption and private key is used for decryption. Public key is known to public and private key is only known to user. So there is no need to distribute the keys before transmission [4]. In this type of algorithms it is very difficult to derive one key from the other (means decryption key is very difficult to derive from the encryption key). In asymmetric algorithms, public keys are used to encrypt the message and private keys are used to decrypt the message.

2. DES (DATA ENCRYPTION STANDARD)

DES was designed by IBM in 1977. DES is a Private (symmetric) key cryptography algorithm. In DES, size of input block is 64-bits and key is 56-bits long. Same key is used for encryption and decryption. DES comprises various operations: mixing of bits, substitution, exclusive OR, S-boxes, straight permutation and expansion permutation [5].

Structure of DES algorithm:



[6] *Source: International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*

Steps involved in DES algorithm are:

(i) Inputs of DES are 64-bits plain text and 56-bits key. Output of DES is 64-bits cipher text. In DES, block of plain text is converted into block of cipher text.

(ii) Processing of block: Transposition is applied to 64-bits plain text. This process is called keyless initial permutation.

(iii) Processing of key: 64-bits key provided by the user is reduced to 56-bits by removing the parity bits (8, 16, 24, 32, 40, 48, 56 and 64). Split the key into two halves of 28-bits each. After this, circular left shifts are applied on both halves. Then by applying compression permutation 56-bits key is reduced to 48-bits. This 48-bits key is used for encryption. This component is called key processor sub component. It provides different set of 48-bits for 16 rounds means all the 16 complex round ciphers use a different key derived from the original key.

(iv) Split the block produced in step (ii) into two halves of 32-bits each.

(v) Expansion permutation is applied to one half to increase its size to 48-bits.

(vi) XOR operation is applied to 48-bits of plain text produced in step (v) and 48-bits fetched from key processor sub component in step (iii).

(vii) Output of step (vi) is fed into the S-box which reduces the 48-bits block into 32-bits block.

(viii) Output of step (vii) is subjected to straight permutation for changing the order of bits.

(ix) Again XOR operation is applied to the output of step (viii) and other half of the block produced in step (iv).

(x) The two data halves are then swapped and become the input for the next round

(xi) Cipher text is obtained after completing 16 rounds and by applying final permutation (reverse of initial permutation) [7].

For decryption, same process is used but in reverse order. DES algorithm is widely used for better security. Security depends heavily on S-boxes.

3. RSA (RIVEST, SHAMIR, ADLEMAN) ALGORITHM:

RSA was discovered in 1978. RSA is a Public (asymmetric) key cryptography algorithm; it is named after the initials of its discoveres, Ron Rivest, Adi Shamir and Len Adelman in 1977. It is the most popular asymmetric key cryptographic algorithm which is used to provide both secrecy and digital signature. It uses the prime numbers to generate public and private keys based on mathematical calculations and multiplying large numbers together [8]. Steps involved in RSA algorithm are generation of public and Private keys, Encryption Process, Decryption Process.

Generation of Public and Private Keys

Following steps are used for generating keys:
Choose any two prime numbers say p & q. (p & q cannot be divided by any other number except 1 and itself). Calculate n, n = p x q. Calculate another number Ø also known as Euler's totient function. Value of Ø = (p-1) x (q-1). Now assume a number e such that d x e = 1 (mod Ø). The value of e should lie between 1 and Ø. Number e should be a prime number. Number e and Ø should be co-prime means e and Ø are not divisible by any other number except 1 or in other words g.c.d. of e and Ø should be 1. Now calculate the value of d by using extended Euclidean algorithm's table method. After calculating the value of d, public keys (e and n) are announced to the public and private keys (d and Ø) are kept secret.

Encryption process:
Now anyone can send a message by using public keys (e and n). Plain text (Original message) is converted into Cipher text (scrambled message) by using the following formula:

$$C = P^e \text{ (mod n)}$$

Decryption process:
Cipher text is converted into Plain text by using private key d. Cipher text (scrambled message) is converted into Plain text (original message) by using the following formula:

$$P = C^d \text{ (mod n)}$$

Modular exponentiation is used for Encryption and Decryption process.

RSA algorithm requires complex computation and hence it is very slow. In Public key algorithms, the underlying modular exponentiation and factoring large numbers into prime numbers depend on multiplication and division, which are inherently slower and requires a lot of processing power.

4. COMPARISON OF PRIVATE AND PUBLIC KEY CRYPTOGRAPHIC ALGORITHMS:

Conceptual comparison of DES and RSA:

Factors	DES (Private Key Algorithm)	RSA (Public Key Algorithm)
Message Length	Suitable for long messages	Suitable for short messages
Data rate	Fast	Slow
Requirement of memory space	Less memory space required	More memory space required
Encryption Process	Fast	Slow
Decryption Process	Fast	Slow
Type of algorithm (or cryptography)	Symmetric	Asymmetric
Speed of computation	Fast	Slow
Complexity	O(logN)	O(N3)
Security	Moderate	Highest
Nature	Closed	Open

Vulnerabilities (or weaknesses)	Brute Forced, Linear and Differential cryptanalysis attack	Brute Forced and Oracle attack
Cause of vulnerability	Weak key usage	Weak
Secure services	Confidentiality	Confidentiality, Integrity, Non-repudiation
Job of intruder (or Hacker)	Easy Deduction of key is based on guesses and knowledge of language. Key could be derived by Hit and trial or by recognizing patterns or by combination of guesses, strategy and mathematical skill.	Difficult
Block size	64 bits	Minimum 512 bits
Power consumption	Low	High
Rounds	16	1
Throughput	Very high	Low
Confidentiality	High	Low
Software Implementation	Fast (DES is at least 100 times faster than RSA)	Slow
Hardware Implementation	Fast (DES is between 1,000 and 10,000 times faster (depending on the implementation) than RSA)	Slow
Encryption and Decryption algorithm	Different	Same
Cryptanalysis method	Differential method	Product factorization

Key-Based comparison of DES and RSA:

Factors	**DES (Private Key Algorithm)**	**RSA (Public Key Algorithm)**
Relationship between Encryption and Decryption Keys	Encryption and Decryption keys are inverse of each other. $P = D(K, E(K, P))$	Encryption and Decryption keys come in pairs. $P = D(K_D, E(K_E, P))$
Derivation of Decryption key from Encryption key	Easy	Difficult (almost impossible)
Key Distribution	Problematic (not as popular as RSA)	Simple (widely used for key distribution)
Type of key	Private or Secret	Public
Key Size	56 bits	>1024 bits
Key transportation (or transmission)	Key transportation is necessary because sender and receiver both use the same key.	Key transportation is not necessary (the biggest advantage of public key cryptography is the secure nature of private key, it never needs to be transmitted or revealed).
Sharing of key (or key exchange)	Difficult (in the world of Internet, the communicating parties may never meet and converse except over the network so how do they share key and communicate).	Simple (problem of key sharing can be solved by using RSA because it uses two keys: public and private. Public key is announced by the receiver and is available on the web page of receiver).
Ways used for key sharing	Telephone lines are used which are prone to eavesdropping.	Public key is available on the web page of the receiver. Sender uses this public key to encrypt the message.
Key disclosure	Key is not disclosed publicly.	Key is disclosed on the web.
Key management	Difficult	Easy
Key deposit	Needed	Needed

Comparison of DES and RSA on the basis of Encryption and Decryption Time:

S. No.	Algorithm	Packet Size (KB)	Encryption Time (Sec)	Decryption Time (Sec)
1	DES	153	3.0	1
	RSA		7.3	4.9
2	DES	118	3.2	1.2
	RSA		10.0	5.0
3	DES	196	2.0	1.4
	RSA		8.5	5.9
4	DES	312	3.0	1.6
	RSA		7.8	5.1
5	DES	868	4.0	1.8
	RSA		8.2	5.1

[9] *Source: International Journal of Science and Research (IJSR)*

From the above table it is clear that RSA takes more time for Encryption and Decryption than DES. Hence, Public key algorithms are slower than Private Key algorithms.

5. CONCLUSIONS

Security of any algorithm is highly based on the length of the key being used. Private and public key algorithms have their own advantages and disadvantages. Private key algorithms require less memory than Public key algorithms. Computation speed of Private key algorithms is much faster than Public key algorithms. Because of the amount of computations involved, Public key algorithms are very slow and are useful only for specialized tasks. Private key encryption is 10,000 times faster than the Public Key encryption because in Public Key algorithms, the underlying modular exponentiation and factoring large numbers into prime numbers depend on multiplication and division, which are inherently slower and requires a lot of processing power than the bit operations (addition, exclusive OR, substitution and transposition, shifting columns, shifting rows) on which Private key algorithms are based. Therefore, cryptographers use Private key algorithms for frequent tasks where slow operation is a major problem and Public key algorithms are reserved for specialized, infrequent uses, where slow operation is not a problem. Key distribution is simple in public key algorithms whereas it is complex in Private key algorithms.

So, for providing better services, combination of Private and Public key algorithms can be used. Hybrid (means combination of Private and Public key algorithms) scheme can be used to provide better security in networks. For an instance, firstly use Public key algorithm for key distribution and then send data securely by using Private key algorithm. Public key algorithms are more often used as a solution to the key-management problem. For short messages, only public key algorithms can be used and for long messages, combination of Private and public key algorithms can be used for sending data securely. This combination of Private and Public key algorithms often capitalizes on the best features of each.

REFERENCES

[1]. Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, “Wireless Network Security: Vulnerabilities, Threats and Countermeasures”, International Journal of Multimedia and Ubiquitous Engineering, Vol. 3, No. 3, July, 2008.

[2]. Mrs.V.Umadevi Chezhian, Dr. Ramar, Mr. Zaheer Uddin Khan, “Security Requirements in Mobile Ad Hoc Networks”, International Journal of Advanced Research in Computer and Communication Engineering, ISSN 2278 – 1021, Vol. 1, Issue 2, April 2012.

[3]. Gurpreet Singh, Supriya, “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security”, International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013.

[4]. Dr. Prerna Mahajan, Abhishek Sachdeva, “A study of Encryption algorithms AES, DES and RSA for security”, Global Journal of Computer Science and Technology, Volume 13 Issue 15 Version 1.0 Year 2013.

[5]. Dr. Sudesh Jakhar, Aman Kumar, Sunil Makkar, “Comparative Analysis between DES and RSA algorithm”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, ISSN: 2277 128X**,** July 2012.

[6]. Shaymaa Mohammed Jawad Kadhim Manjusha Joshi, Dr. Shashank Joshi, “Provide the Security to a Web Service by using DES Cryptography Algorithm”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013 ISSN: 2277 128X, figure2.

[7]. Prashanti.G, Deepthi.S, Sandhya Rani.K, “A Novel Approach for Data Encryption Standard Algorithm”, International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013.

[8]. Mohit Marwaha, Rajeev Bedi, “Comparative analysis of Cryptographic Algorithms”, International Journal of Advanced Engineering Technology, IV/III/July-Sept.,2013/16-18, E-ISSN 0976-3945.

[9]. B. Padmavathi, S. Ranjitha Kumari, “A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique”, International Journal of Science and Research (IJSR) India Online ISSN: 2319-7064, Volume 2 Issue 4, April 2013, Table2.

BIOGRAPHIE

Priti Bali is working as an Assistant Professor in D.A.V. Institute of Management, Faridabad.