International Journal of Engineering & Scientific Research **(IJMRA Publications)**
Vol. 6 Issue 4, April 2018,
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.esrjournal.com Email: esrjeditor@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Network Security and Cryptography

ANJU DEVI

Department of Computer Science and IT

GNG College, Santpura, Yamuna Nagar

Corresponding Author Email Id: anjugngit@gmail.com

Article Received: 3rd March, 2018 Article Revised: 18th March, 2018 Article Accepted: 28th March, 2018

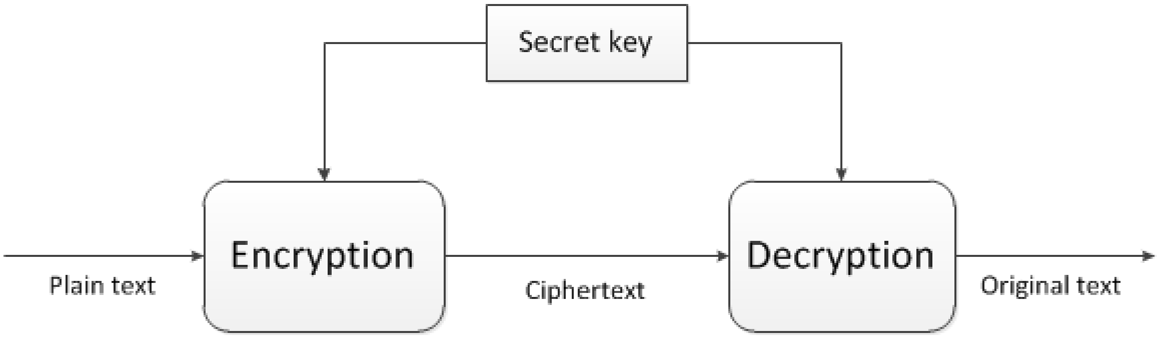
Abstract

In this world, large amount of data are transferred daily over a network. Our main aim of data transmission over the network will not be accessed by unauthorized users. Security is main concept to secure the transmission data over network. We use network security and cryptography to protect the data. Network security covers to public and private network, that's used in everyday in government sectors, transaction communication etc. In this paper, we define the various types of security aspects like: confidentiality, non- repudiation, integrity etc. Cryptography-based security technologies commonly use one or more of these functions to provide network and information security. There are various types of techniques are used in cryptographic, symmetric and asymmetric key .In symmetric key cryptography Advanced encryption standard (AES) and Data encryption standard (DES) comes under it and RSA (Rivest Shamir Adleman) and DSA(Digital Signature Algorithm) comes under asymmetric key cryptography. The difference between these algorithms are : key, block size and speed. The performance of all the algorithms are different. And the message are encrypted and decrypted by the mathematics expressions

Keywords: Security, cryptography, Symmetric, Asymmetric key

Introduction

The most common and simple way of protecting a network resource is to assign a unique name and a corresponding password. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. It is a combination of key and algorithms. Key can be public or private. With the help of encrypt key or decrypt key we can secure our transmission data. Encryption is the process of converting plain text into cipher text. Decryption is in reverse order, which is used to convert cipher text back to plaintext.



We can secure the data through the symmetric and asymmetric key. In symmetric key ,only one key is used. But in asymmetric key, public and private key both are used. There are various techniques and mechanisms are used for protection of data.

Basic Concepts:

Cryptography The methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message to its original message

Plaintext The original message form.

Cipher text The converted message

Cipher An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods

Key Some critical information used by the cipher, known only to the sender& receiver

Encipher (encode) The process of converting plaintext to cipher text using a cipher and a key

Decipher (decode) the process of converting cipher text back into plaintext using a cipher and a Key

Code An algorithm for transforming an intelligible message into an unintelligible using a code-book

Security Services

It enhances the security of data processing and transferring. There are various types of aspects to secure the data :

Data Integrity

When sender sends the message to receiver then unauthorized users cannot modify or change the message. Verification the original contents of information have not been corrupted. Without integrity. Therefore, many cryptosystems use techniques and mechanisms to verify the integrity of information. For example, an intruder might covertly alter a file, but change the unique digital thumbprint for the file, causing other users to detect the tampering by comparing the changed digital thumbprint to the digital thumbprint for the original contents.

Data Confidentiality

Unauthorized person cannot be understand the message except who is the actual receiver. For example, unauthorized users able to intercept information, but the information is transmitted and stored as cipshertext and is useless without a decoding key that is known only to authorized users.

Authenticity

Only authorized persons can access the data or to do communication with each others, unauthorized are not allow to communication. cryptosystems use various techniques to authenticate both the sender and receiver of information.

Non repudiation

Non repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent and receive, the receiver or sender can prove that the alleged sender or receiver in fact sent the message.

Access Control

It is the process of preventing an unauthorized use of resources. This goal controls who can have access to the resources

6.Availability

Requires that computer systems be available to authorized parties when needed.

Basic Terminology of Cryptography

Millions of peoples are used computer for many purposes such as: shopping, education, banking, in every field, it is used etc.

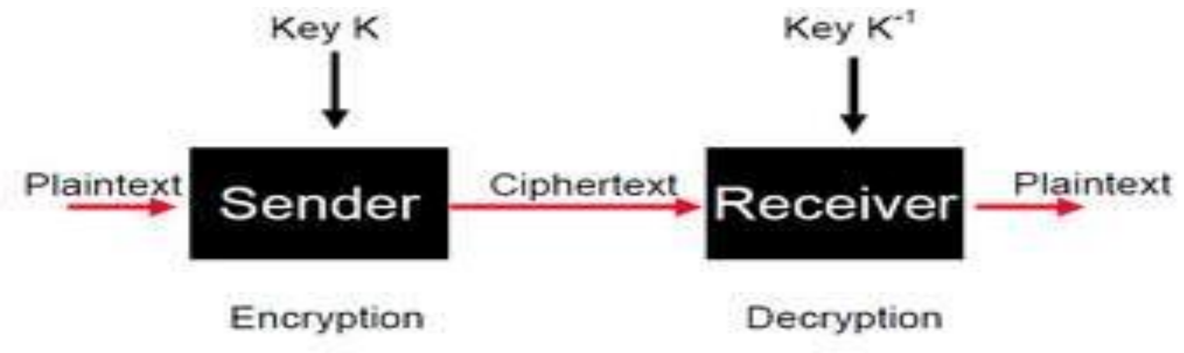
Privacy is main issue in these applications, how are we need to make sure that an unauthorized person cannot read or modify the messages.

Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data.

For example, sender sends the message before encryption or it is receive after decryption.

The information are transmitted and nobody can understand , is called cipher text,except the recipients.

Many algorithms are used to transform plain text into cipher text.



Cipher algorithm is used to transform plaintext to cipher text, This is called encryption.

Network security refers to the activities designed to protect the usability, integrity, reliability and safety of data during their transmission on a network.

There are two types of cryptography

Symmetric Key

Asymmetric Key

Symmetric Key Cryptography

Symmetric key cryptography is also known as private-key cryptography. Secret key can be held by one person or information transferred between the sender and the receiver. If private key cryptography is used to send secret messages between two person , both the sender and receiver must have a copy of the secret key. Because encryption and decryption are used same private key.If one side loses the key then there are no guarantee of message received securely or we can say message cannot be secure. It is also known as secret key cryptography.There are two types of symmetric key divided:

1.Traditional

2.Modern

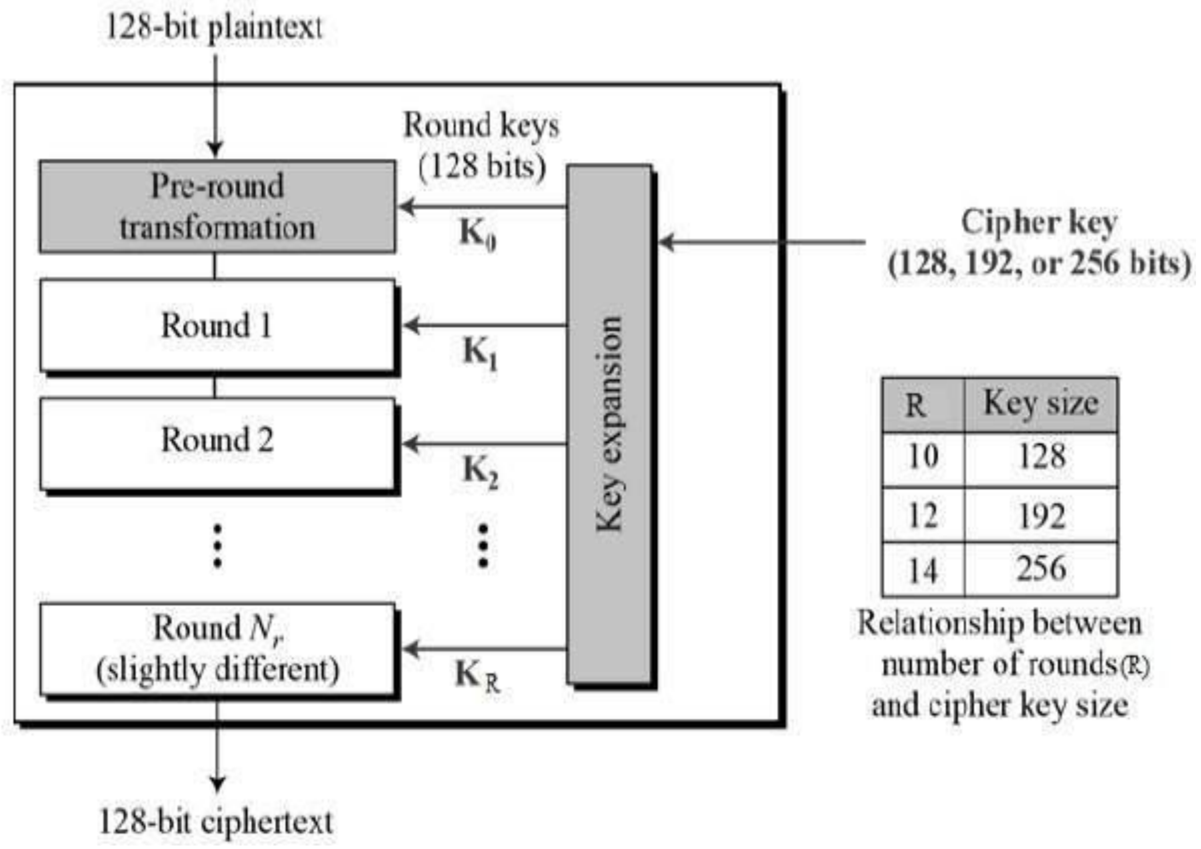
In traditional key ,based on byte or character oriented .It is further divided into substitutional cipher :monoalphabetic and polyalphabetic and transpositional.

In modern key,based on bit oriented :simple modern cipher,rotational cipher,substitution box,p-box.

In comlex modern ciphers of two technics :AES and DES

AES

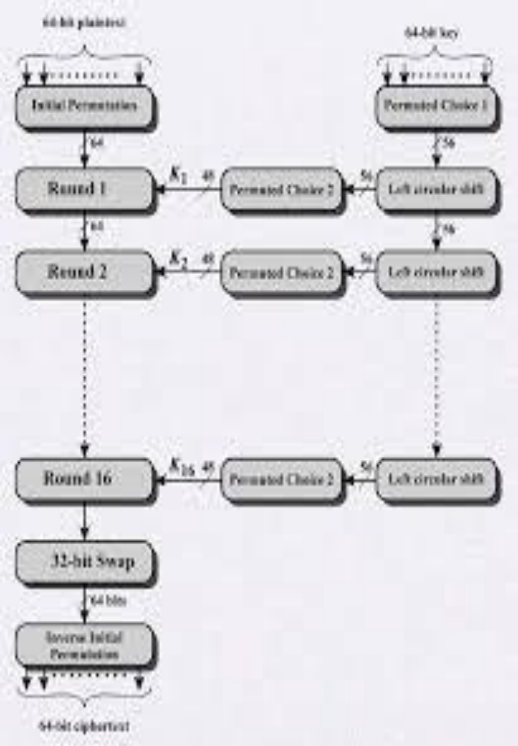
AES technics comes under the symmetric key cryptography,same key are used both the sides.It is designed by NIST (National Institute o Standard & Technology) .AES technique is fast,flexible and higher secure.It is a variable block bit and bit is 128,192 and 256 bits round respectively 10,12 and 14.



R	Key size
10	128
12	192
14	256

DES

DES technics also a type of symmetric key cryptography .It is designed by IBM and USA govt. standazied.It takes 64 bits plaintext and 56(64) bits as a key.It produce the 64 bit ciper text.DES works on same key on both the side to encrypt or decrypt of messages, both sender and receiver must know & use the same private key.



Asymmetric Key Cryptography

In the asymmetric key cryptography there are two key are used and also known as public key system.One key to encrypt the data and another to decrypt the data.

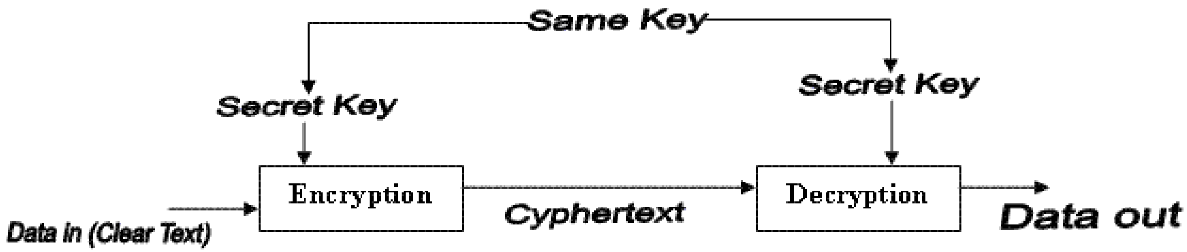
Using this method, the sender and receiver are able to authent`icate one another as well as protect the message. Asymmetric cryptography has two primary use cases: authentication and confidentiality. Using asymmetric cryptography, messages can be signed with a private key, and then anyone with the public key is able to verify that the message was created by someone possessing the corresponding private key. This can be combined with a proof of identity system to know what entity (person or group) actually owns that private key, providing authentication.

Encryption with asymmetric cryptography works in a slightly different way from symmetric encryption. Someone with the public key is able to encrypt a message, providing confidentiality, and then only the person in possession of the private key is able to decrypt it.

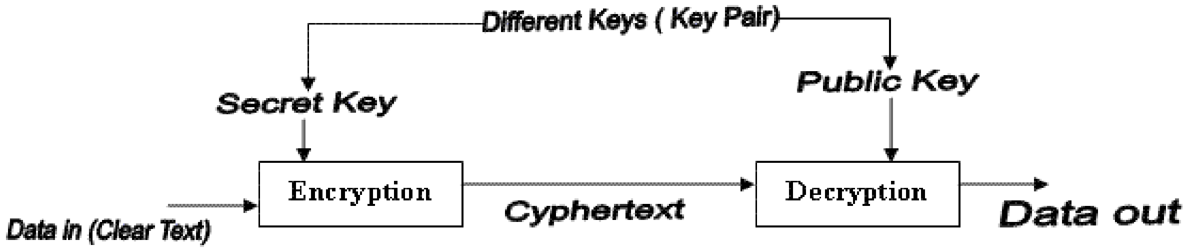
There are various algorithms comes under it like:

RSA (Rivest Shamir Adleman)

DSA(Digital Signature Algorithm)



Symmetric Encryption



Asymmetric Encryption

RSA: We used two keys Private and public keys

Set: e=public key

d=private key

Steps for choosing key by sender:-

1.Sender chooses the two very large prime number of 1024 digits.

2.It will multiple these two numbers to get ‘n’, which will act as modulus for encryption and decryption.

n = p*q

3.It calculates Z that is

Z=(p-1)(q-1)

4.It chooses the random integer ‘e’ and then calculates the ‘d’,by given equation

d*e=1mod z

It announces ‘e’ and ‘n’ to public and d and z are private.

For encryption we use public key

For decryption we use private key

Cipher text(c)=(plaintext)^e mod n

Plaintext=(ciphertext)^d mod n

This is an simple example using numbers by using RSA algorithms:

1. select primes numbers and values : p=11, q=3 and m is the message and its value is 7

2. n = pq = 11*3 = 33
3. z= (p-1)(q-1) = 10*2 = 20

4. Choose e=3
Calculate the value of e by using this equation:

d*e=1 mod z

7*e=1 mod 20

:. e=3

5.Now we want to encrypt the message:

Cipher text = plaintext ^ e mod n

=7^3 mod 33

Hence the cipher text is 13

Now we want to decrypt the message:

Plain text=cipher text ^ d mod n

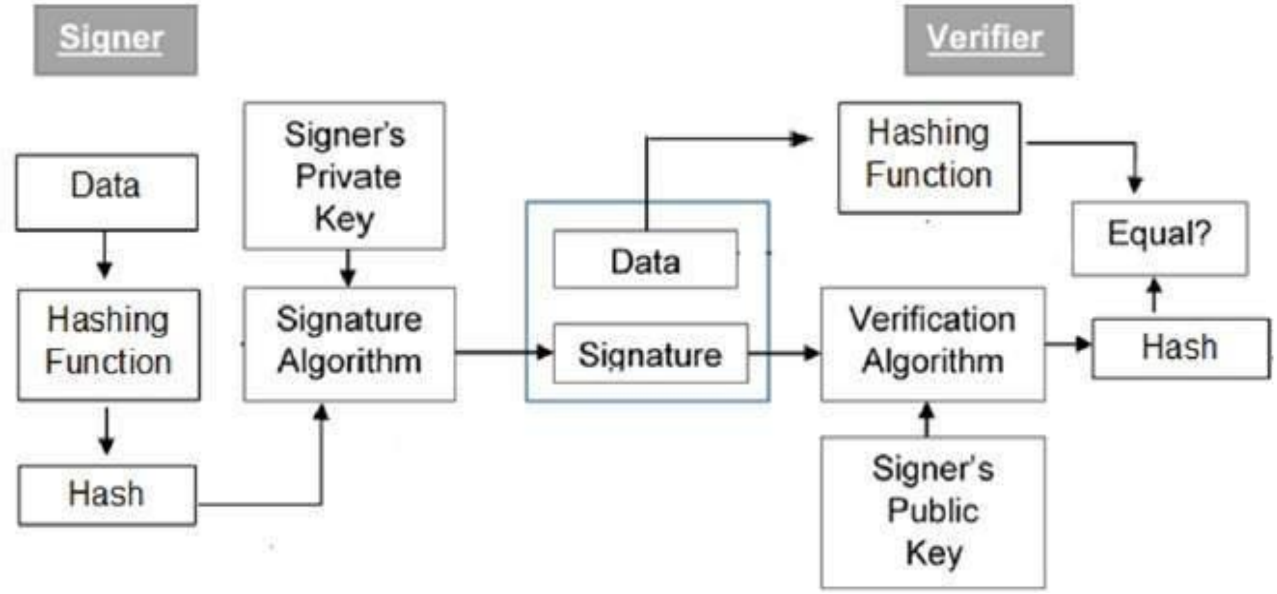
=13^7 mod 33

Hence the plain text is 7

so we can break down a potentially large number into its components and combine the results of easier, smaller calculations to calculate the final value.

DSA

DSA stands for Digital Signature Algorithms. Out of all cryptographic, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security. Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer. The private key used for signing is referred to as the signature key and the public key as the verification key. Signer side feeds the data to hash function and then generate the hash of data. Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output. Verifier run same hash function on received data to generate hash data. For verification, this hash value and output of verification algorithm are compared. If both are same then digital signature are valid otherwise invalid.



CONCLUSION

Network Security and cryptography is the main role in data security because it is responsible for securing all information passed through networked computers. We have studied various cryptographic techniques to increase the security of network. Cryptography , principles authorized and confidently are most important for these we can communicate or exchange the information between users ,no one can read or modify the message without exactly receiver. To protect our data or information various types of techniques are used like : aes , des, rsa etc.

.

References:

[1] Murat Fiskiran , Ruby B. Lee, ―Workload Characterization of Elliptic Curve Cryptography and other Network Security Algorithms for Constrained Environments‖, IEEE International Workshop on Workload Characterization, 2002. WWC-5. 2002.

[2] https :// www.techopedia.com/definition/1773/decryption

[3] https://en.wikipedia.org/wiki/Cryptography

[4] https://www.techopedia.com/definition/25403/encryption-key

[5] Daemen, J., and Rijmen, V. "Rijndael: AES-The Advanced Encryption Standard, Springer, Heidelberg, March 2001.

[6] The Research of Firewall Technology in Computer Network Security, 2009 Second Asia-Pacific Conference on Computational Intelligence and Industrial Applications by Xin Vue, Wei Chen, Yantao Wang, College of Computer and Information Engineering Heilongjiang Institute of Science and Technology Harbin, China.

[7] 'Data encyption standard', FIPS PUB 46, National Bureau of Standards,Washington, DC Jan. 1977

[8] Coron, J. S. , " What is cryptography?", *IEEE Security & Privacy Journal, 12(8), 2006, p. 70-73.*

[9] SIMMONS, G.J.: 'Symmetric and asymmetric encryption', *ACM Comput. Surveys*, 1979, **11,** pp. 305-330

[10] www.google.com