



Networkforyou

Subscribe to our
YouTube Channel



Networkforyou



Welcome

To

Network for you

Cryptography Concepts:



Email us:
networkforyou4@gmail.com

1 of 7

WhatsApp Us : +918143809578



Cryptography Concepts:

- Cryptography is the practice of securing information and communications through the use of codes so that only those for whom the information is intended can understand it and process it.
- The prefix **"crypt" means "hidden"** and suffix **"graphy" means "writing"**.
- In cryptography, the techniques which are used to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it.

Cryptography



Here are some of the key concepts in cryptography:

Plaintext: The original message that is to be encrypted.

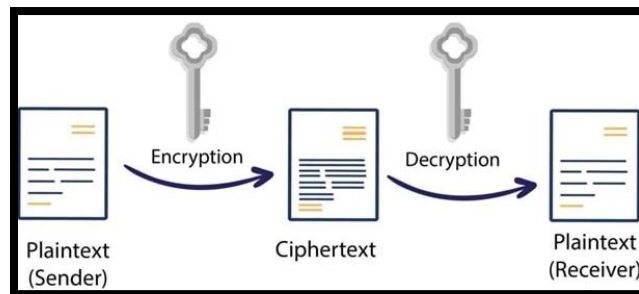
Ciphertext: The encrypted message that is the result of applying an encryption algorithm to the plaintext.

Encryption algorithm: A mathematical procedure that is used to **transform plaintext into ciphertext**.

Decryption algorithm: A mathematical procedure that is used to **transform ciphertext back into plaintext**.

Key: A secret value that is used by the encryption and decryption algorithms.

Salt: A random value that is used to make the encryption process more secure.



Email us:
networkforyou4@gmail.com

2 of 7

WhatsApp Us : +918143809578



Let see some example online this is link we use to check.

<https://www.cryptool.org/en/cto/caesar>

Symmetric and Asymmetric Encryption:

- Symmetric and asymmetric encryptions are two different types of encryption that are used to protect data.
- **Symmetric encryption uses the same key for both encryption and decryption**, while **asymmetric encryption uses two keys: a public key and a private key.**
- Symmetric encryption is the most common type of encryption.
- It is relatively fast and efficient, and it can be used to encrypt large amounts of data.
- However, symmetric encryption requires that the key be shared between the sender and receiver, which can be a security risk if the key is compromised.
- Asymmetric encryption is slower than symmetric encryption, but it is more secure.
- This is because the public key can be shared with anyone, while the private key is kept secret.
- This means that only the person with the private key can decrypt the data that was encrypted with the public key.

The Simple Lockbox Model

Symmetric cryptography

One of us puts our package in a box and locks it. We both have the same key, so the other one can unlock it.



Asymmetric cryptography

I have given you an open box, but I keep hold of the key. You can put something in it and close it, but only I can unlock it once closed.



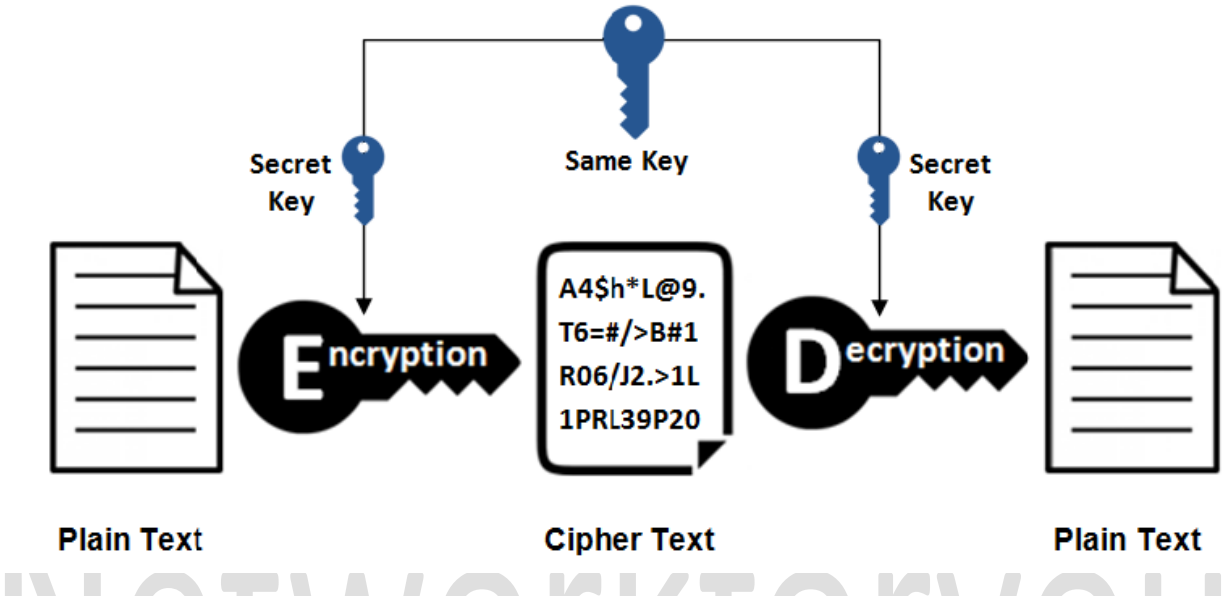
Email us:
networkforyou4@gmail.com

3 of 7

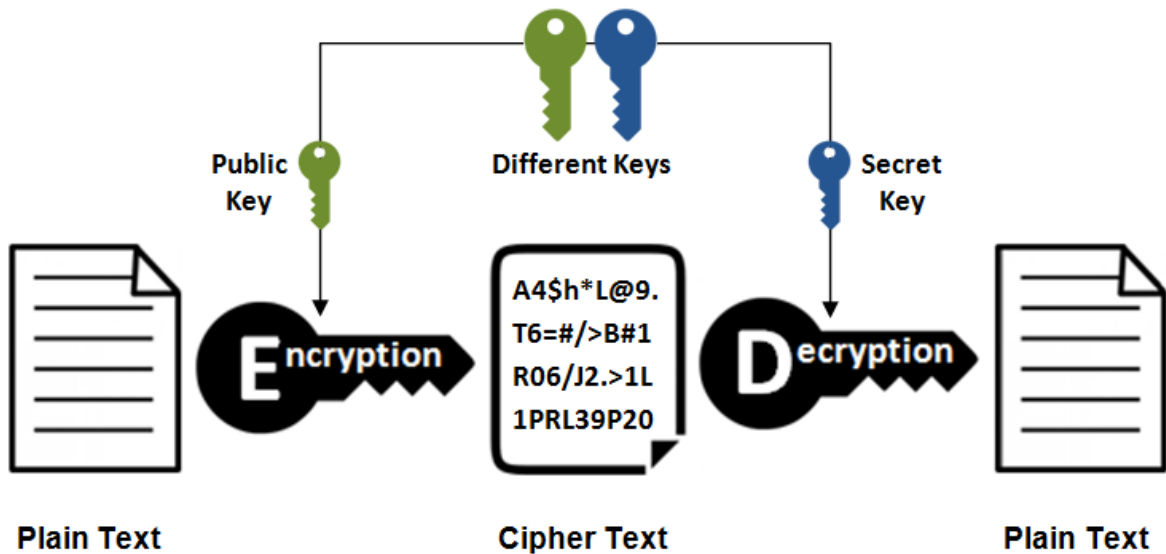
WhatsApp Us : +918143809578



Symmetric Encryption



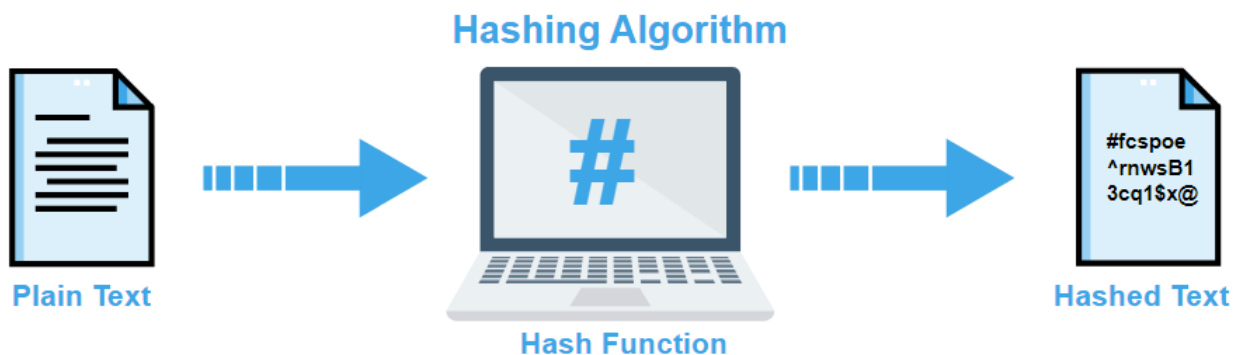
Asymmetric Encryption





Describe Hash:

- Cryptographic hash function is kind of algorithm that can be run on a piece of data.
- The produced value is called checksum, digest, message digest or hash value.
- It is string value, which is the result of calculation of a Hashing Algorithm.
- Hash is a number that is generated from the text through a hash algorithm.
- Hashing is one-way function that scrambles plaintext to produce unique message digest.
- There is no way to reverse the hashing process to reveal the original data or message.
- Hash Values have different uses main uses is to protects the integrity of your data.
- Protects data against potential alteration so that your data is not changed one bit.
- Sender sends the data and digest; receiver takes data & runs its own hash to create digest.
- Receiver then compares digests, if the two digests are same, then data is not manipulated.
- Two methods commonly available MD5 (Message Digest) and SHA (Secure Hash Algorithm).



MD5 Hashing:

- Hashing is the technique to ensure the integrity.
- MD5, which stands for Message Digest algorithm 5.
- The Message Digest (MD5) is a cryptographic hashing algorithm.
- MD5 hash is typically expressed as a 32-digit hexadecimal number.
- MD5 or message digest algorithm will produce a 128-bit hash value.
- Input data can be of any size or length, but the output size is always fixed.
- MD5 algorithm generates a fixed size (32 Digit Hex) MD5 hash.
- The hash is unique for every file irrespective of its size and type.

Email us:
networkforYou4@gmail.com

5 of 7

WhatsApp Us : +918143809578



SHA Hashing:

- SHA, stands for Secure Hash Algorithm, is cryptographic hashing algorithm.
- SHA used to determine the integrity of a particular piece of data.
- The Secure Hashing Algorithm comes in several flavors.
- SHA-1 and SHA-2 are two different versions of that algorithm.
- SHA1 produces a 160-bit (20-byte) hash value.
- SHA2 has option to vary digest between 224 bits to 512 bits.
- SHA224 produces a 224-bit (28-byte) hash value.
- SHA256 produces a 256-bit (32-byte) hash value.
- SHA384 produces a 384-bit (48-byte) hash value.
- SHA512 produces a 512-bit (64-byte) hash value.

HMAC:

- HMAC stand for Hash Message Authentication Code, Hash with plus secret key.
- HMAC use hash algorithm on data plus secret key that only sender & receiver know.
- Therefore, both parties with secret keys can calculate and verify their hash values.
- This prevents a man in the middle attacks by making it very difficult to modify data.
- This prevents a man in the middle attacks making it difficult and create a new hash.

For MD5 and SHA Hashing Demo, use HashCalc and WinMD5 free application:

Link to download Hashcalc:

<https://www.slavasoft.com/hashcalc/>

Link to download WINMD5 free:

<https://www.winmd5.com/>

Email us:
networkforyou4@gmail.com

6 of 7

WhatsApp Us : +918143809578



The screenshot shows a Windows desktop with three overlapping windows. The top window is HashCalc, a utility for calculating various file hashes. The 'Data' field contains the file path 'C:\Users\User\Desktop\What is the command to cor...'. The 'MD5' checkbox is checked, and the resulting hash '294cee9b20ed128bd645a7e282113822' is displayed in the output field. Below it, the 'CRC32' checkbox is also checked, showing a value of '0860f190'. The middle window is WinMD5Free v1.20, which has a file selected: 'Desktop\What is the command to configure a VPN on an ASA firewall.docx'. It shows the 'Current file MD5 checksum value' as '294cee9b20ed128bd645a7e282113822'. The bottom window is a smaller WinMD5Free dialog box with an information icon and the text: 'Original: 294cee9b20ed128bd645a7e282113822', 'Current: paste its original md5 value to verify', and 'NOT Matched!'. An 'OK' button is at the bottom.

Email us:
networkforyou4@gmail.com

WhatsApp Us : +918143809578