CLOUD CRYPTOGRAPHY PRESENTAITON

AHTESHAM SARWAR AG-6068

KHAWAR AZEEM AG-6067 NABEEL UR REHMAAN AG-6078

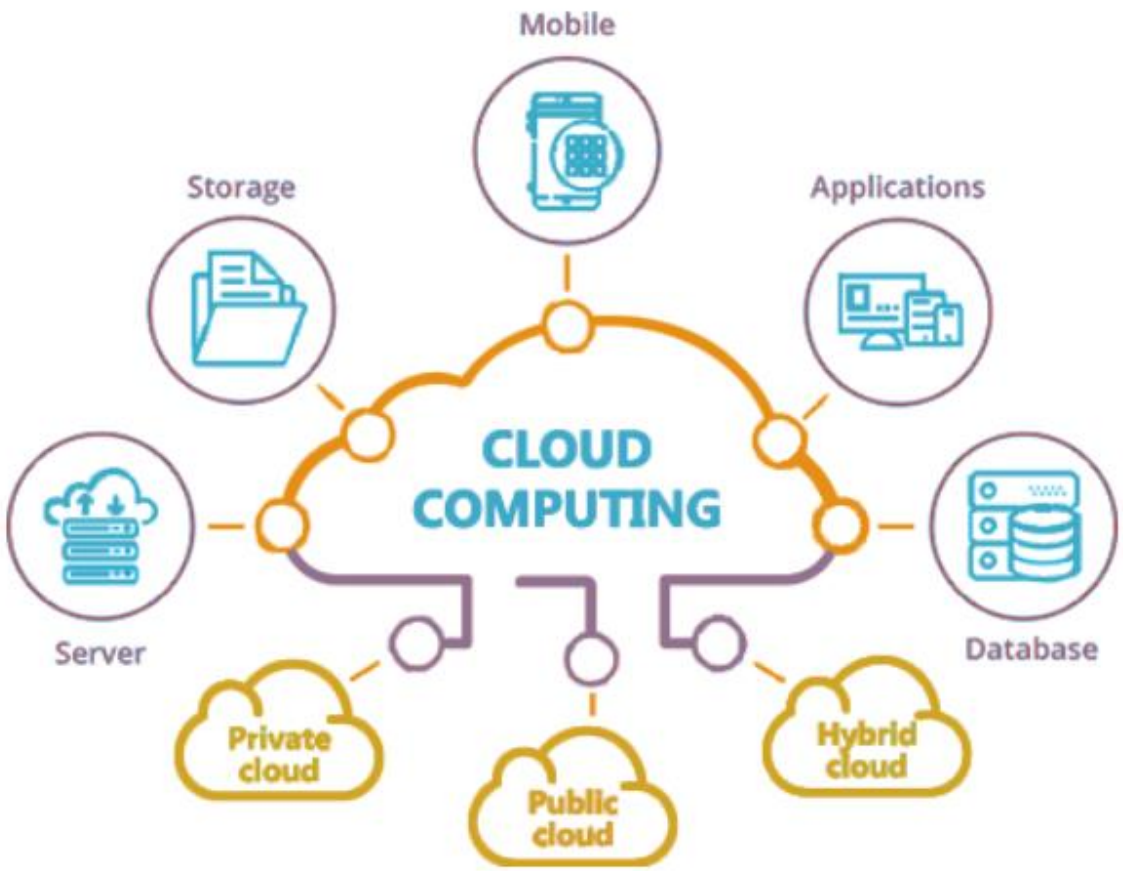
CLOUD CRYPTOGRAPHY

BASIC TERMINOLOGIES:

Cloud:

"The cloud" refers to servers that are accessed over the Internet, and the software and databases that run on those servers.

Cloud servers are located in data centers all over the world. By using cloud computing, users and companies do not have to manage physical servers themselves or run software applications on their own machines.

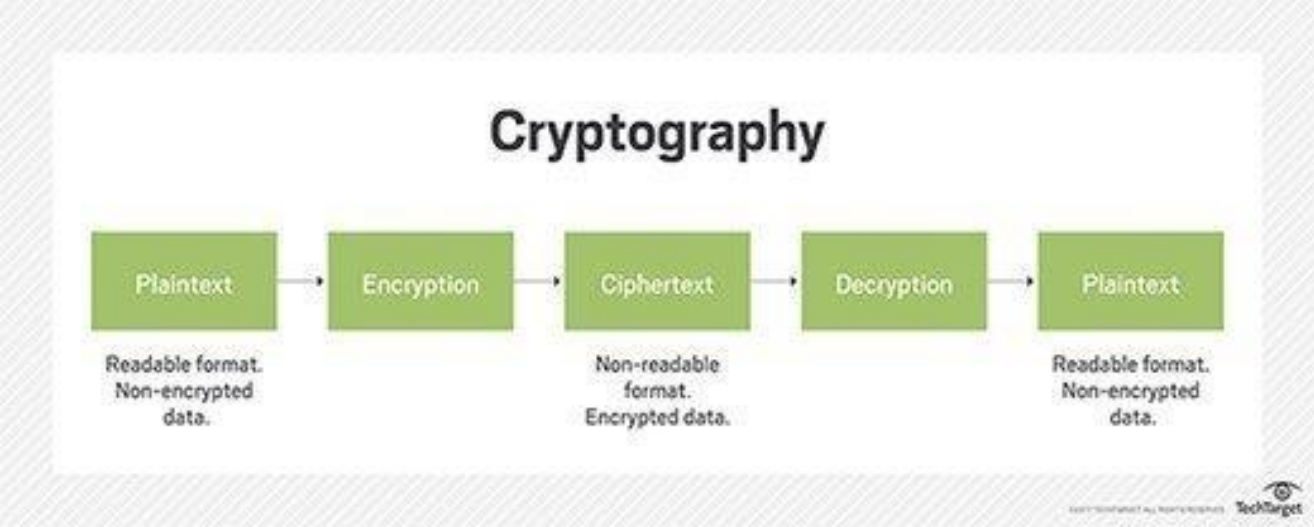


Cryptography:

The term is derived from two Greek words “kryptos”, which means “hidden, secret” and “graphein”, which means “to write”.

Cryptography or Cryptology is the practice and study of techniques for secure communication in the presence of adversarial behavior.

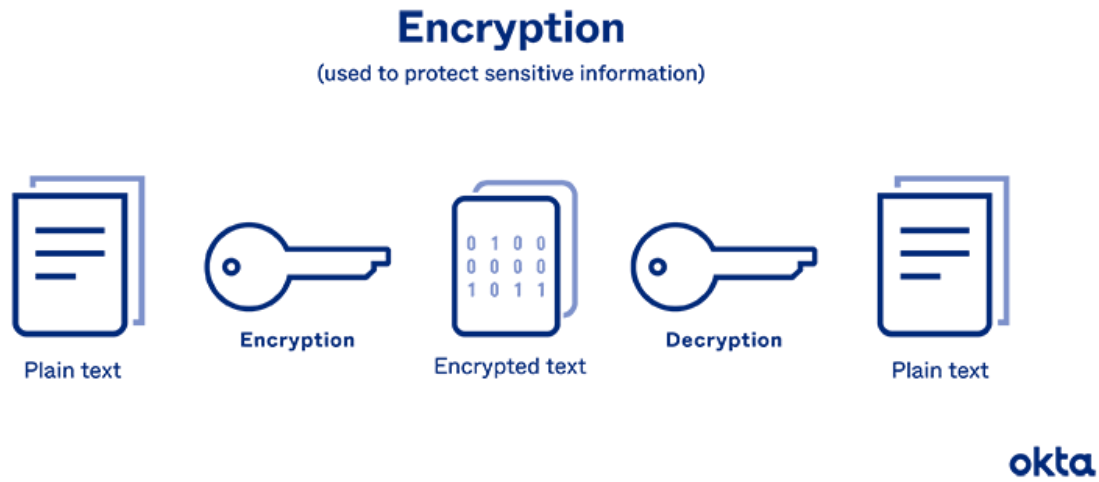
More generally, cryptography is about constructing and analyzing protocols that prevent third parties and public from reading private messages.



Encryption:

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of a **cryptographic key**: a set of mathematical values that both the sender and the recipient of an encrypted message agree on.

Although encrypted data appears random, encryption proceeds in a logical, predictable way, allowing a party that receives the encrypted data and possesses the right key to decrypt the data, turning it back into plaintext. Truly secure encryption will use keys complex enough that a third party is highly unlikely to decrypt or break the ciphertext by **brute force** — in other words, by guessing the key.



What is Cloud Cryptography?

- Cloud Cryptography is encryption that safeguards data stored within the cloud.
- The basic aim of using such a method is authentication.
- Adds a strong layer of protection to secure data to avoid being breached, hacked or affected by malware.
- Permit users to access shared cloud services securely and conveniently.

- **Secures sensitive data without delaying the delivery of information.**

Why Cloud Cryptography?

Cloud computing without cryptography is not much safe. All the data stored on cloud and communicating is in plain text, not encrypted. Anyone who tries to intercept the data during communication, can read and modify it. There is no privacy for user. Sensitive data is not safe. In order to overcome these issues, we need Cloud Cryptography.

How does cryptography in cloud work?

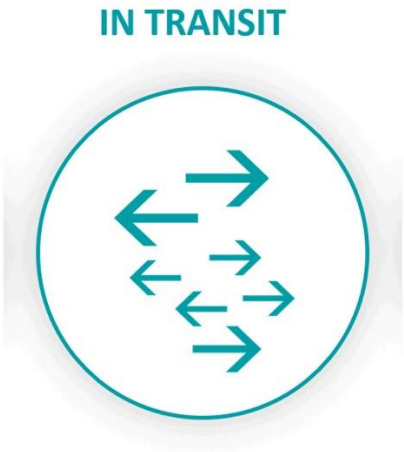
Cloud cryptography is based on encryption, in which computer and algorithms are utilized to scramble text into ciphertext. This ciphertext can be converted into plaintext by using an encryption key, by decoding it with a series of bits.

There are two primary ways of encryption to secure the data:

1. **Information in-transit**
2. **Information at-rest**

1. Information in-transit:

When the information is moving through different connections (email, apps, or even browsers), it is information in transit.



- ## Encryption in-transit:

  Encryption-in-transit, whereby messages are encrypted on the sender′ s end, delivered to the server, decrypted there, re-encrypted, and then delivered to the recipient and decrypted on their end. Encryption-in-transit protects information during transmission, but using it allows the intermediate link in the chain — the server — to see the content. Depending on how trustworthy its owners are, that can be an issue.

- ## End-to-End Encryption:

  Senders and receivers send messages, where they are the only one who can read them.

  In E2EE, the data is encrypted on the sender′ s system or device, and only the intended recipient can decrypt it. As it travels to its

destination, the message cannot be read or tempered by anyone e.g., ISP, ASP or hacker.

2. Information at-rest:

It is when the information storage is in the cloud, computer hard drive, mobiles, and apps electronically.

- ### File-Based Encryption (FBE):

  File encryption occurs when at rest, data is encrypted so that if an unauthorized person tries to intercept a file, they will not be able to access the data it holds.

- ### Full-Disk Encryption (FDE):

  When any files are saved on an external hard drive, they will be automatically encrypted. This is the key method to secure hard drives on the computers.

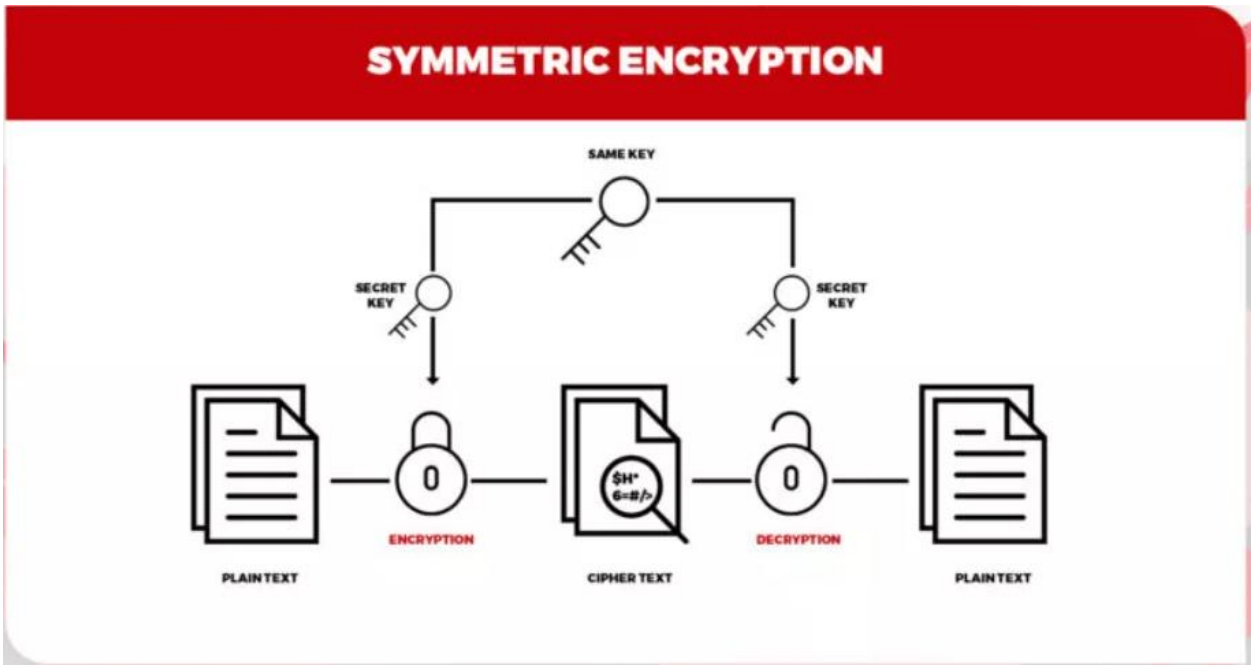
How the data on the cloud be secured by Cryptography?

Cloud Cryptography brings same level of security to cloud services by securing the stored data using encryption. It can protect sensitive cloud data without delaying data transmission. Many organizations define various cryptographic protocols for their cloud computing to keep balance between security and efficiency. The cryptographic algorithms used for Cloud Security are:

1. Symmetric Key Cryptographic Algorithm
2. Asymmetric Key Cryptographic Algorithm
3. Hashing

1. Symmetric Key Cryptographic Algorithm:

This algorithm provides authentication and authorization to data because the data is encrypted with a unique single key cannot be decrypted with any other key. It also requires a safe method to transfer the key from one party to another. This takes little computing power and works very well in encryption.

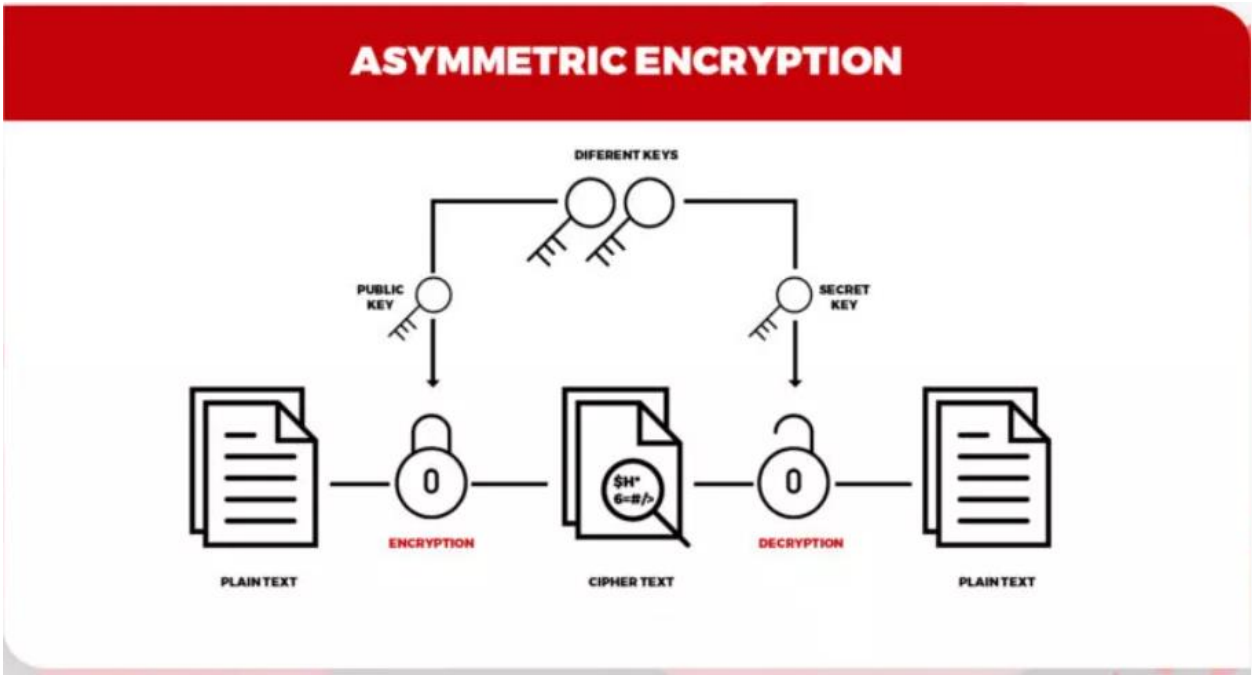


Some popular symmetric algorithms used in cloud computing are - Data encryption standard (DES), Blowfish, Advanced encryption standard (AES), Triple DES, etc.

2. **Asymmetric Key Cryptographic Algorithm:**

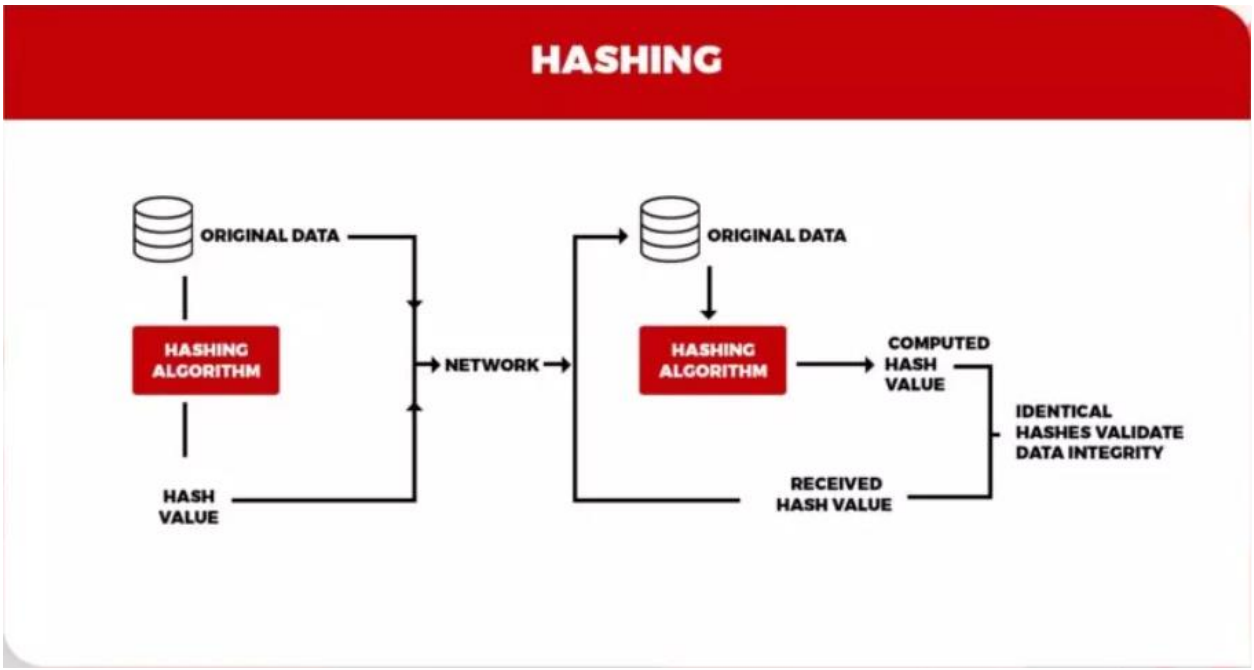
It utilizes different keys for encryption and decoding. Here, every beneficiary requires a decoding key. This key is referred to as the recipient's private key. Here, the encryption key belongs to a particular individual or entity. This sort of algorithm is considered the most secure as it requires both keys to get to a piece of explicit data. Secure but slower than symmetric key cryptographic algorithm.

Popular Asymmetric Key algorithms are RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptography).



3. **Hashing:**

Hashing is the process of converting the information into key using a hash function. The original information cannot be retrieved from the hash key by any means. Generally, the hash keys are stored in the database and they are compared to check whether the original information matches or not. They are generally used to store passwords for login. Some examples of hashing algorithm are MD5, SHA256.



Advantages of Cloud Cryptography:

- The main advantage of cloud cryptography is privacy. The data stays private for users because the details will be confidential, and the risk of fraud by unauthorized users reduces.
- Organization immediately receive notification if an unauthorized person tries to modify the data. The users who have cryptographic keys are granted access.

- Secure the data during transmission
- Cloud encryption permits organizations to be proactive for their defense against data breaches and cyber-attacks.
- Receivers of data have the ability to identify if the data received is corrupted, permitting an immediate response and solution to the attack.
- Encryption is one of the safest methods to store and transfer the data as it complies with the restrictions imposed by the organization such as FIPS, FISMA, HIPPA or PCI/DSS.

Disadvantages of Cloud Cryptography:

- Cloud Cryptography only grants limited security to the data which is already in transit.
- It needs highly advanced systems to maintain encrypted data.
- The system must be scalable enough to upgrade which adds to the involved expenses.
- Overprotective measures can create difficulties for organization when recovering the data.

Research Paper:

Name: Secure Cloud Data Storage Using Hybrid Cryptography

Date: April, 2022

Authors: Nidhi Kumari, Prof. Vimmi Malhotra

Journal: iJRASET (International Journal for Research in Applied Sciences and Technology)

Abstract:

Nowadays a huge number of organizations use the cloud for storing Big data. And some of the sectors have sensitive data, for example, Military, Agencies, Colleges, Industries, etc. The data can be retrieved when the user requests it. And others can also access the data. Cloud computing provides a lot of features with affordable prices and knowledge accessibility by using the Internet. Security is the main concern in the cloud computing environment as clients store secret information with cloud providers, but sometimes these providers may not be trustful. Splitting data in a safe approach while protecting data from an untrusted cloud is still a demanding topic. In this paper we ensure the right approach for data security and privacy, using Blowfish, and RSA/SRNN algorithms.

References:

- https://www.geeksforgeeks.org/an-overview-of-cloud-cryptography/
- https://www.cloudflare.com/learning/ssl/what-is-encryption/
- https://en.wikipedia.org/wiki/Cryptography
- https://www.cloudflare.com/learning/cloud/what-is-the-cloud/
- https://peoplactive.com/cryptography-in-cloud-computing/
- https://www.arpatech.com/blog/what-is-cloud-cryptography/
- https://www.researchgate.net/publication/359732789_Secure_Cloud_Data_Storage_Using_Hybrid_Cryptography