Data Protection

Encryption

- Encryption is the process of scrambling or enciphering data so it can be read only by someone with the means to return it to its original state
- Two types of Encryption
  - **Symmetric**
  - **Asymmetric**

Symmetric Encryption

From: Computer Security Principles & Practice (3rd Edition)

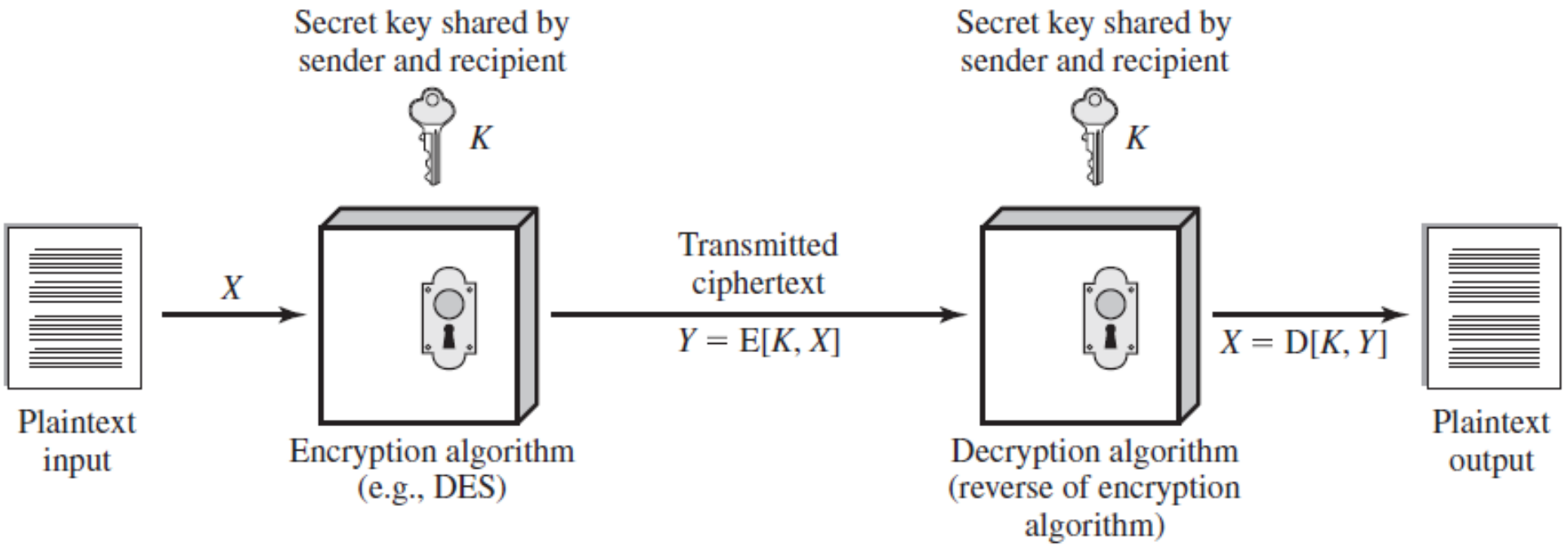


Figure 2.1 Simplified Model of Symmetric Encryption

Symmetric Encryption Algorithms

From: Computer Security Principles & Practice (3rd Edition)

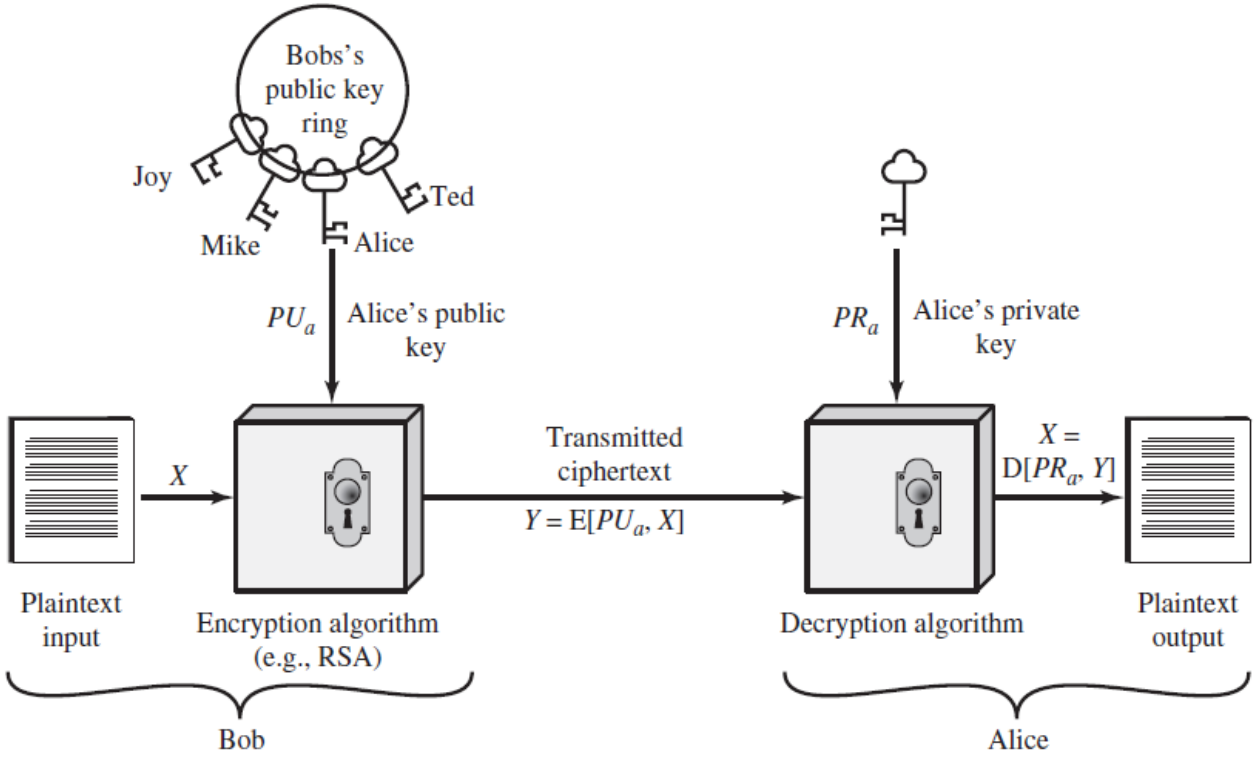
Table 2.1 Comparison of Three Popular Symmetric Encryption Algorithms

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

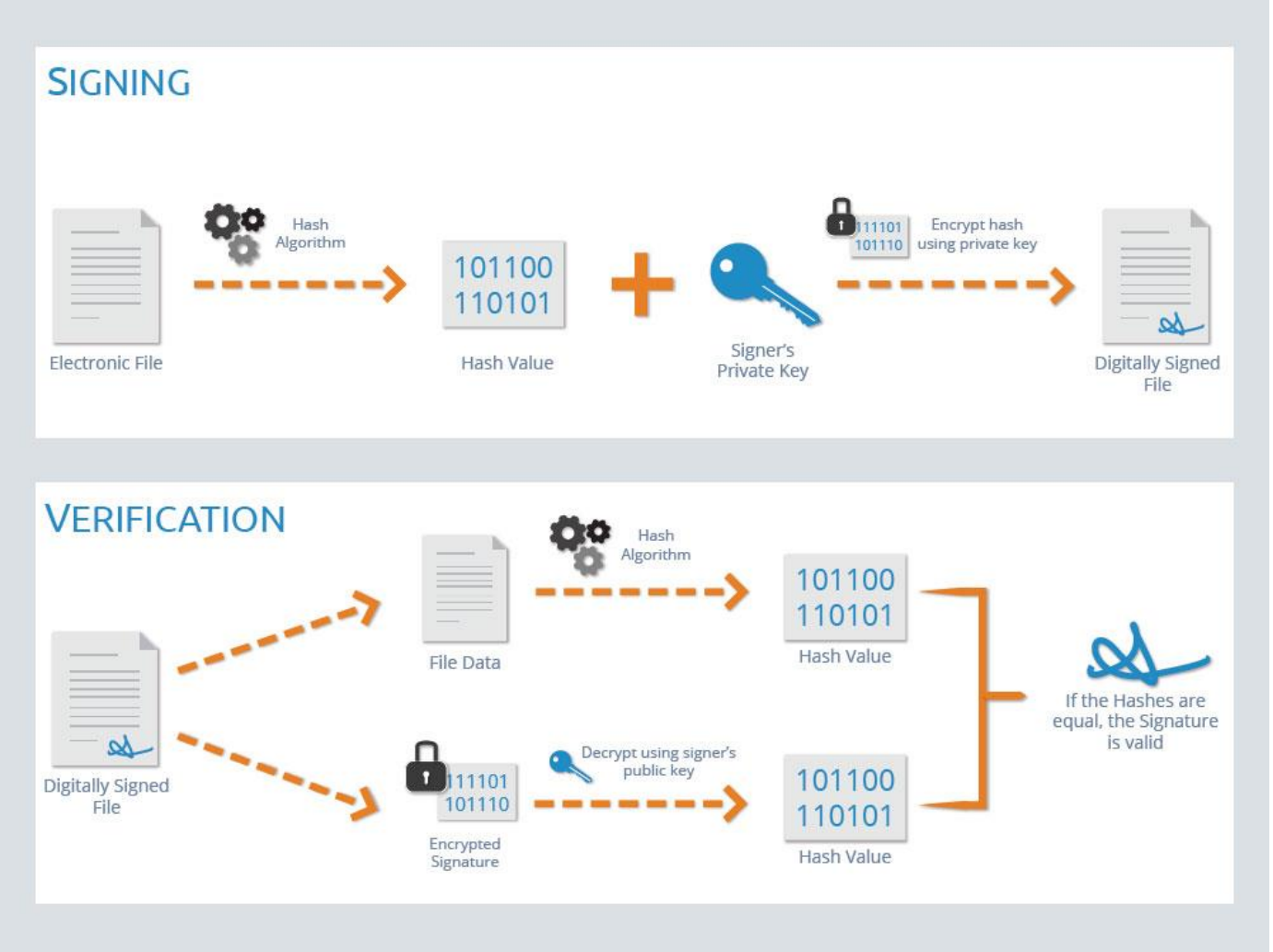
Encryption with Public Key

From: Computer Security Principles & Practice (3rd Edition)



(a) Encryption with public key

Digital Signature



Public Key Certificates

From: Computer Security Principles & Practice (3rd Edition)

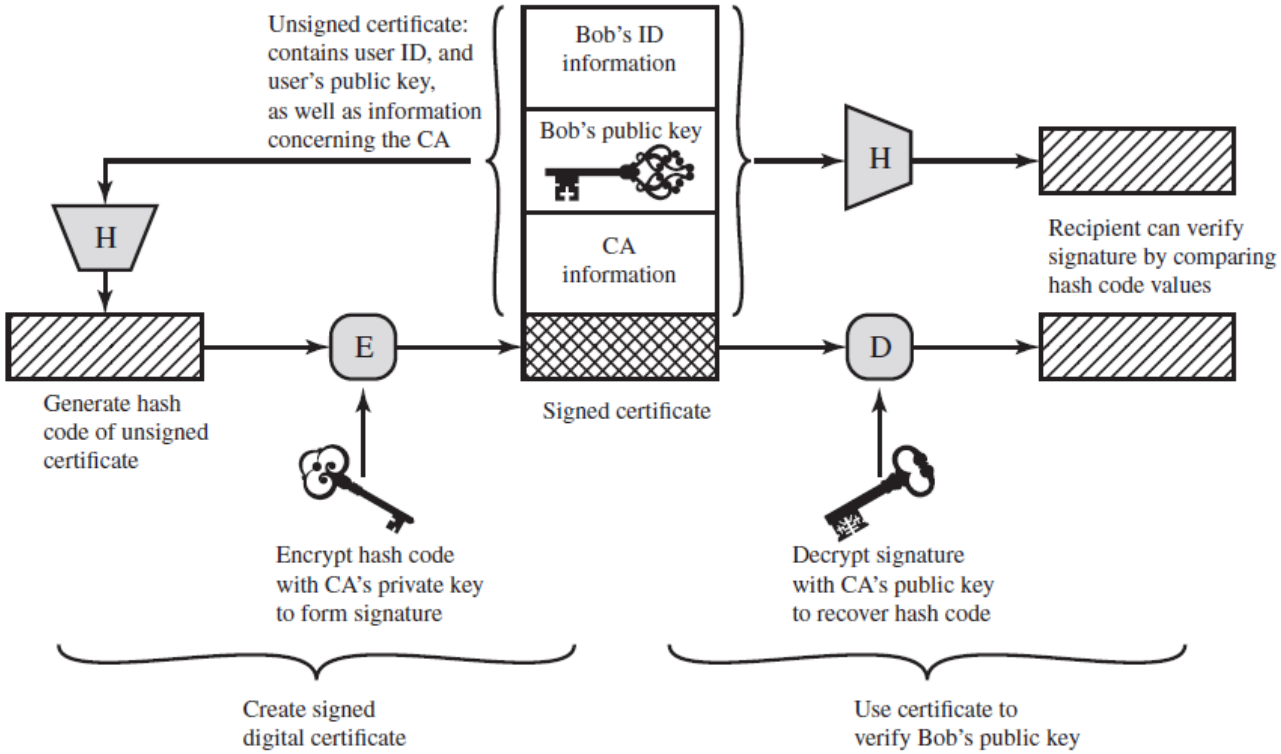


Figure 2.7 Public-Key Certificate Use

Hardware Security Module (HSM)

- A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing
- These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server
- HSMs may have features that provide tamper evidence such as visible signs of tampering or logging and alerting, or tamper resistance which makes tampering difficult without making the HSM inoperable,
- They may have tamper responsiveness such as deleting keys upon tamper detection

AWS CloudHSM

- AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.
- With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs.
- CloudHSM offers you the flexibility to integrate with your applications using industry-standard APIs
- It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups

KMS

- Key Management System
- Create and Control Encryption Keys
  - **These keys are used to encrypt our data**
- Integrated with other AWS Services
  - **S3, EBS, RDS,RedShift etc**

KMS Features

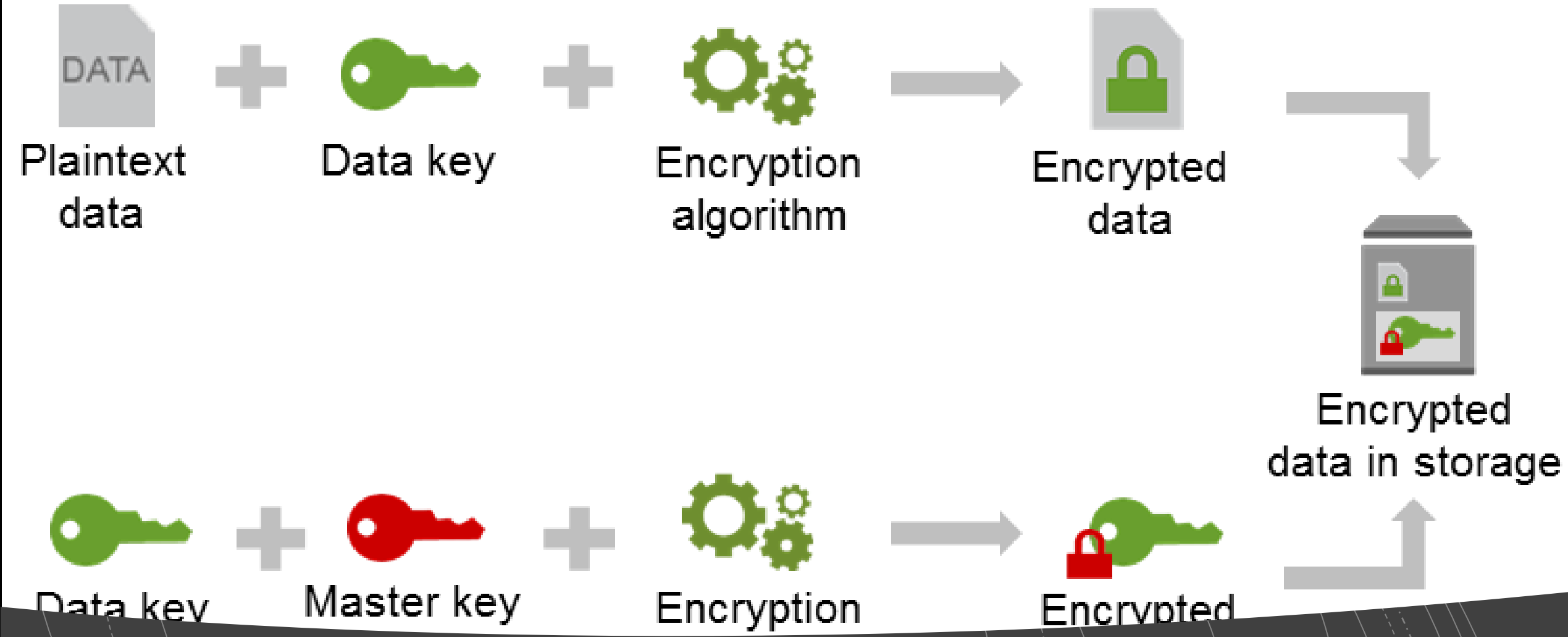
- Create Master Keys
  - **These cannot be exported out of the service**
- Encrypt, Decrypt, Re-Encrypt using Master Keys
- Generate Data Encryption Keys
  - **Both plain text and encrypted**
  - **Used to encrypt data**

Terminology

- Customer Master Key (CMK)
  - **Can protect upto 4KB of data**
  - **CMK does not leave KMS unencrypted**
- Data Keys
  - **Used to encrypt data**
  - **Plain text and encrypted data key**
  - **Plain text used to encrypt data. Encrypted data key stored with data**

Envelope Encryption

- Envelop Encryption used to protect data
- Plain text is encrypted using unique data key
- Data key is then encrypted and stored with data



Envelop Encryption

Image Source: AWS Documentation

Encryption in S3

- Server-Side Encryption (SSE)
  - **SSE – S3**
    - S3 Manages Data and Master keys
  - **SSE – C**
    - Customers manage their own keys
  - **SSE – KMS**
    - Keys managed by KMS
- S3 Encryption Client
  - **Encrypt in application and upload to S3**

Thanks

CloudSiksha