A unique opportunity for you to be mentored by Amazonians

BeSA

Become a Solutions Architect

Batch 04

Week 5

05-Aug-2023

Week 05 – 05-Aug

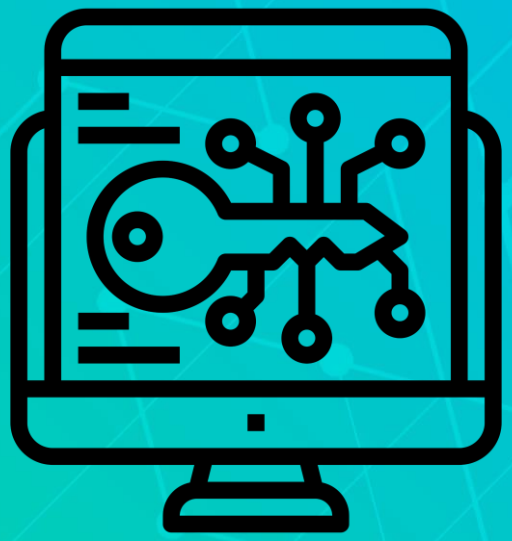
40
Minutes
Fundamentals Track
Encryption

40
Minutes
Specialist Track
Encryption Services
In AWS

Carel Grove

30
Minutes
A day in life of
AWS Account
Manager

Jonathan Nally

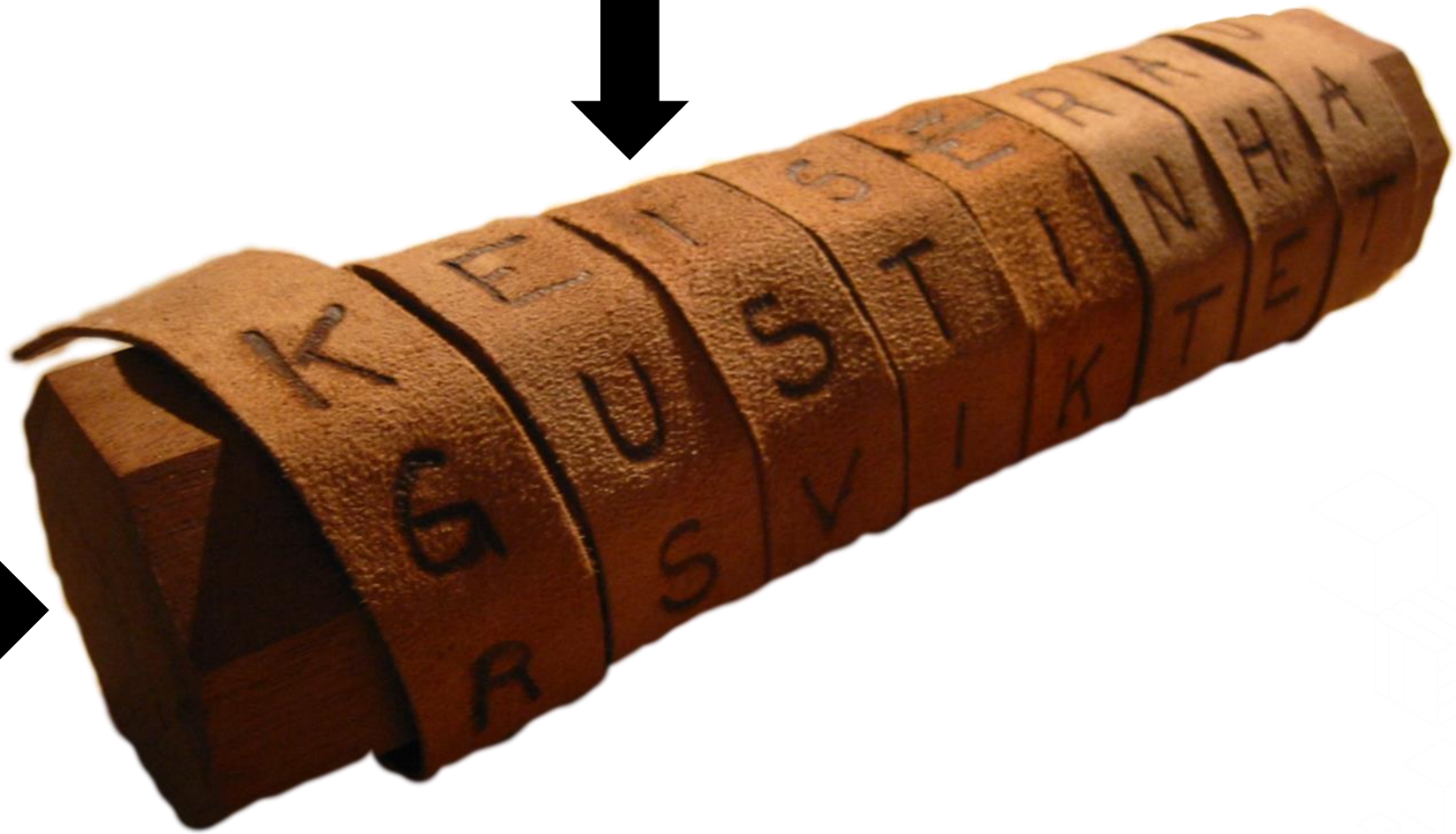


Encryption Basics

What is this?

- Scytale

Encrypted Message



Key

Encryption Analogy

Pin

4 5 8 2

Key

+ 1 - 1

4 5 8 2 (Plain Text)

+ 1 -1 + 1 - 1

5 4 9 1

Cypher Text

5 4 9 1

Decrypt

5 4 9 1

- 1 +1 - 1 +1

4 5 8 2

Key

+ 1 - 1

+ <Value> - <Value>

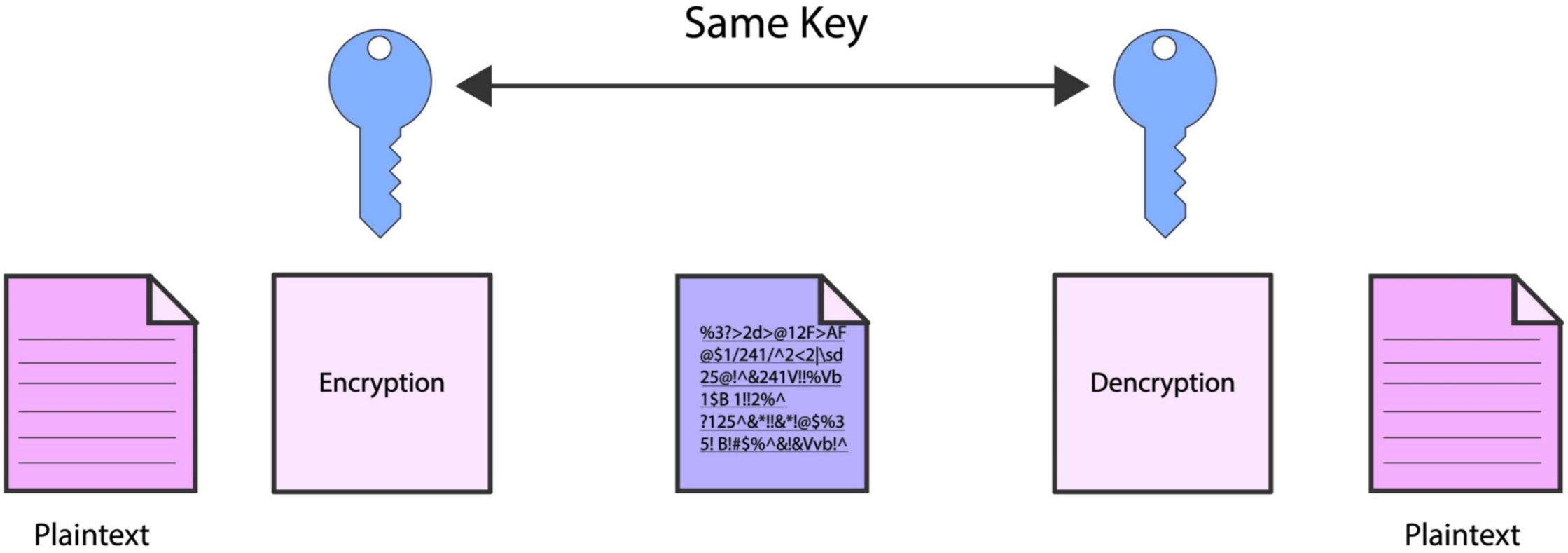
Algorithm

Value = 1

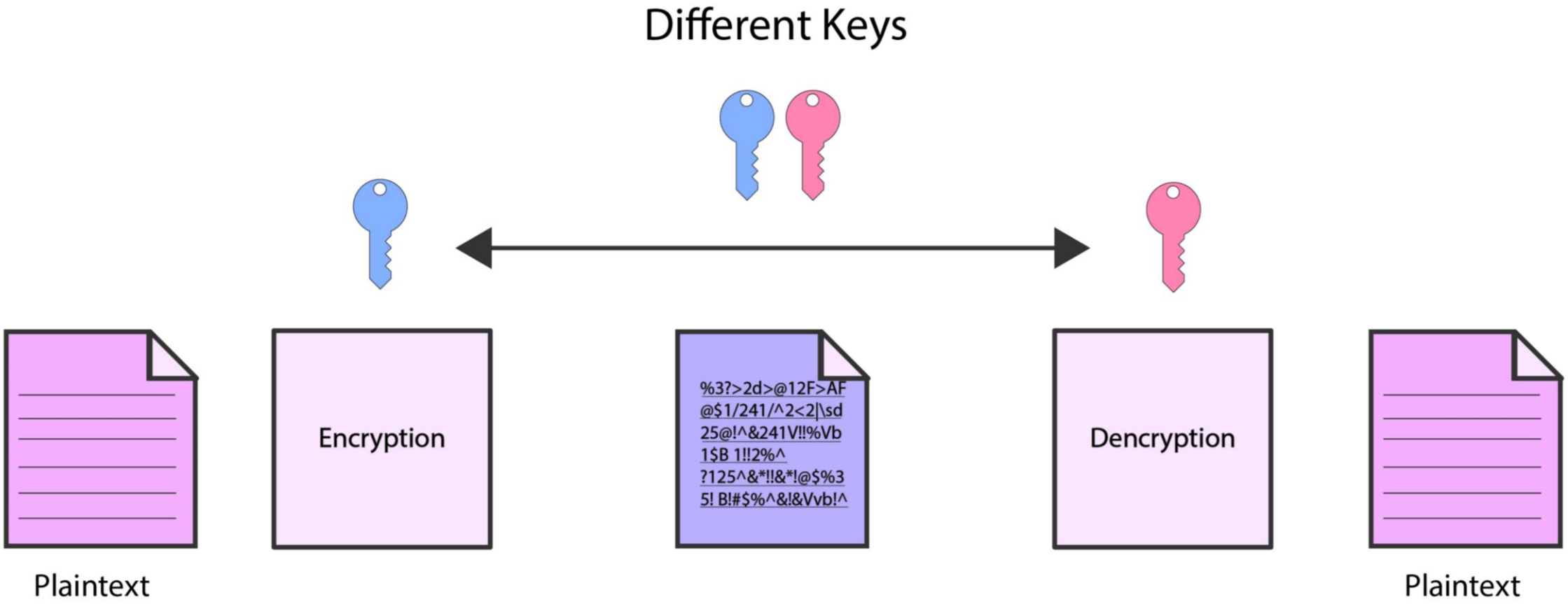
Key Material

Symmetric and Asymmetric Encryption

Symmetric Key Encryption



Asymmetric Key Encryption

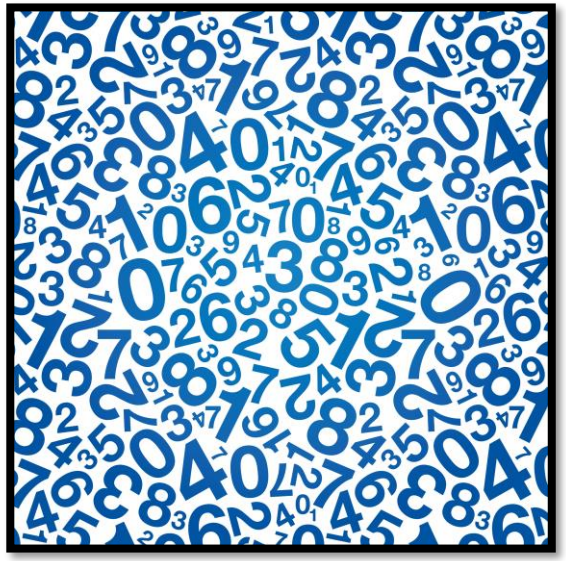


Symmetric Key Encryption vs. Asymmetric Key Encryption

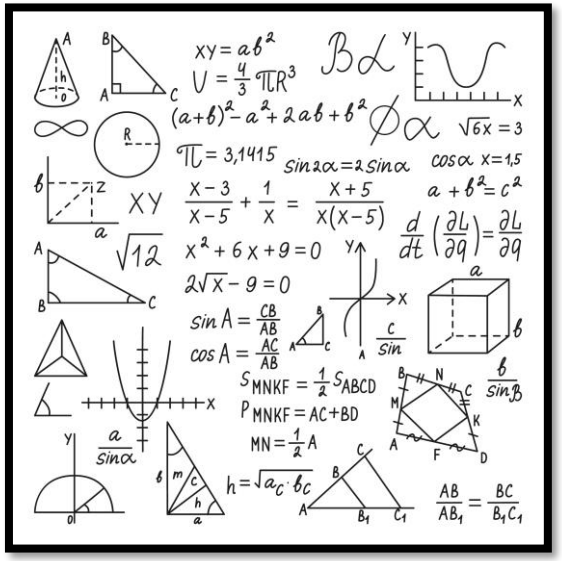
Symmetric Key Encryption	Asymmetric Key Encryption
Encrypts and decrypts data using a single key	Encryption and Decryption are accomplished using two distinct keys – Public Key and Private Key
Due to its simplicity, it is faster.	Due to its complexity, it is slower and requires more processing power.
Smaller key lengths, typically 128-256 bits	Longer key lengths E.g. Recommended RSA keys are 2048 bits
It is typically used for bulk data encryption	It is used in smaller data transactions, primarily to authenticate and create a secure communication channel before the actual data transfer.
Cipher text size is not much different from original plaintext	Cipher text is bigger than the plaintext
Not used in digital signatures	Preferred in digital signatures
Algorithms: DES, RC4, 3DES, AES, ChaCha20	Algorithms: DSA, RSA, Diffie-Hellman, ECDSA, ECDH

How a key pair is generated?

Large Random Number



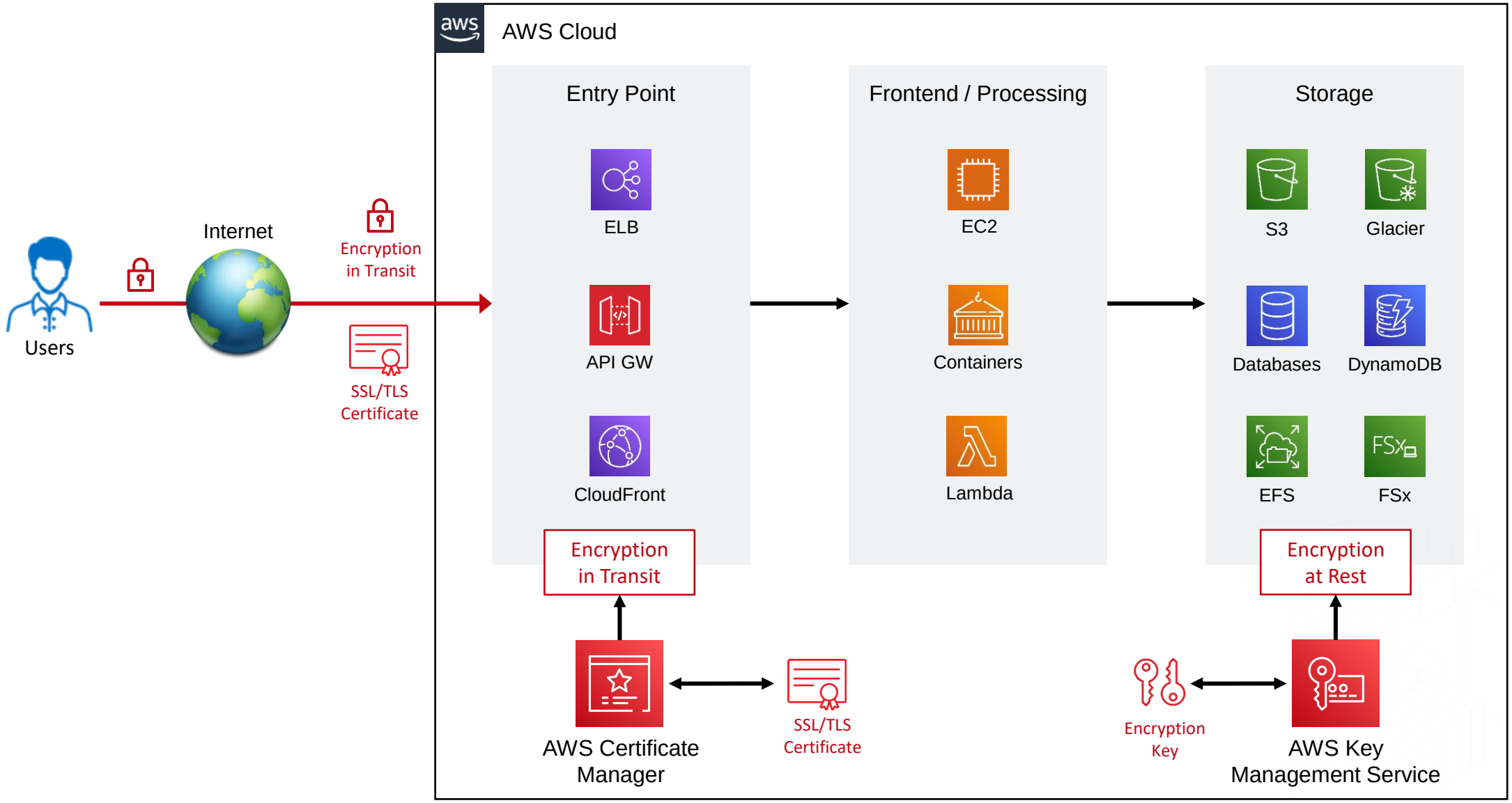
Key Generation Program



Keys

Encryption in AWS

Encryption in Transit / Encryption at Rest



AWS Certificate Manager

AWS Certificate Manager

- Easily provision, manage, and deploy public and private SSL/TLS certificate

Provision, Manage & Renew Certificates

Private Certificate Authority (CA)

Free for ACM integrated services

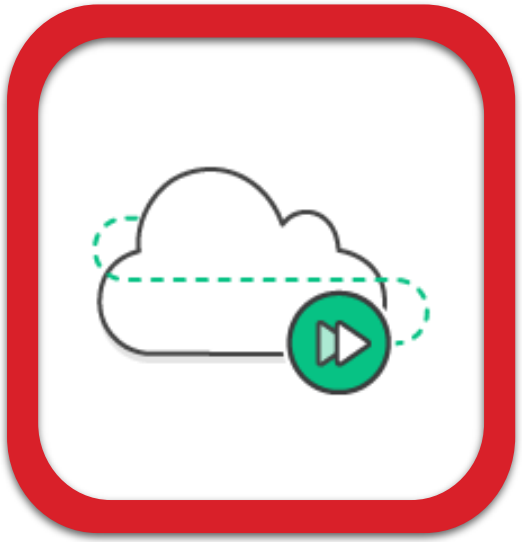
Import 3rd Party Certificates

- AWS Certificate Manager supports a growing number of AWS services.

AWS Key Management Service (KMS)

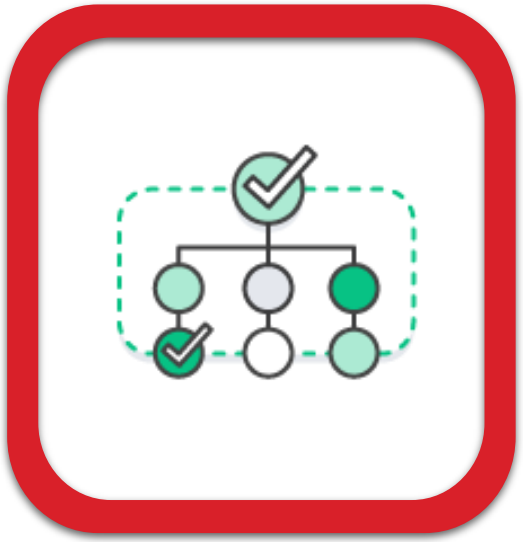
AWS Key Management Service

- Easily create and control the keys used to encrypt or digitally sign your data.



Fully
managed

Built-in
auditing



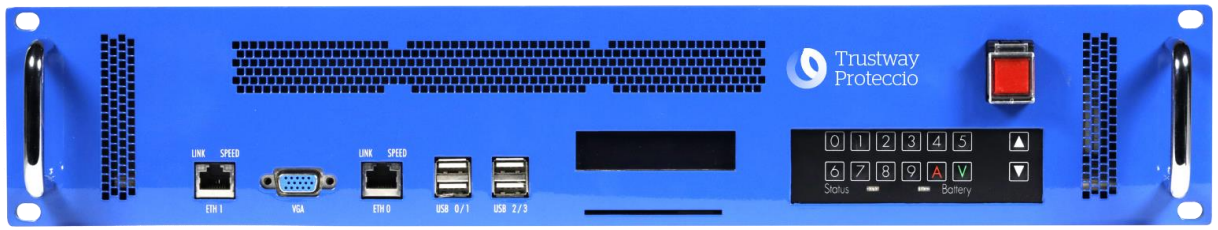
Compliant with
PCI, HIPAA and more

Supports Custom
Key Store

- AWS KMS service stores key material on a device called HSM (Hardware Security Module).

What is a Hardware Security Module (HSM)?

- Hardware Security Module (HSM) is a physical device which is designed to store keys safely.



Envelope Encryption

I HIDE DOOR KEY