COMPX527 Lecture 9.2

Cloud Data Security

Data Security Controls in Cloud

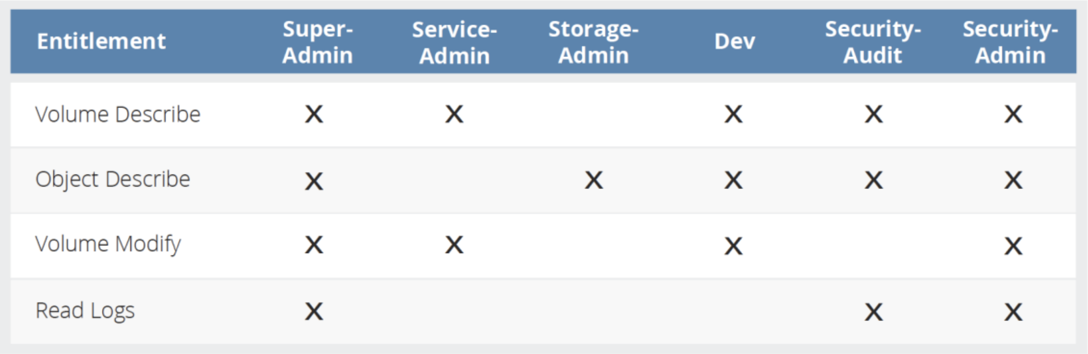
- Policies & Access Control
- Encryption
- Tokenization

Policies and Access Control

Once Data Identification and Classification has been done, high level policies need to be defined to describe who has access to what data

Policies and Access Control

- Access controls should be implemented with a minimum of three layers:
- Management plane:
  - These are the controls for managing access of users that directly access the cloud platform's management plane.
- Public and internal sharing controls
  - If data is shared externally to the public or partners that don't have direct access to the cloud platform, there will be a second layer of controls for this access.
- Application-level controls
  - As you build your own applications on the cloud platform you will design and implement your own controls to manage access.
- Create an entitlement matrix

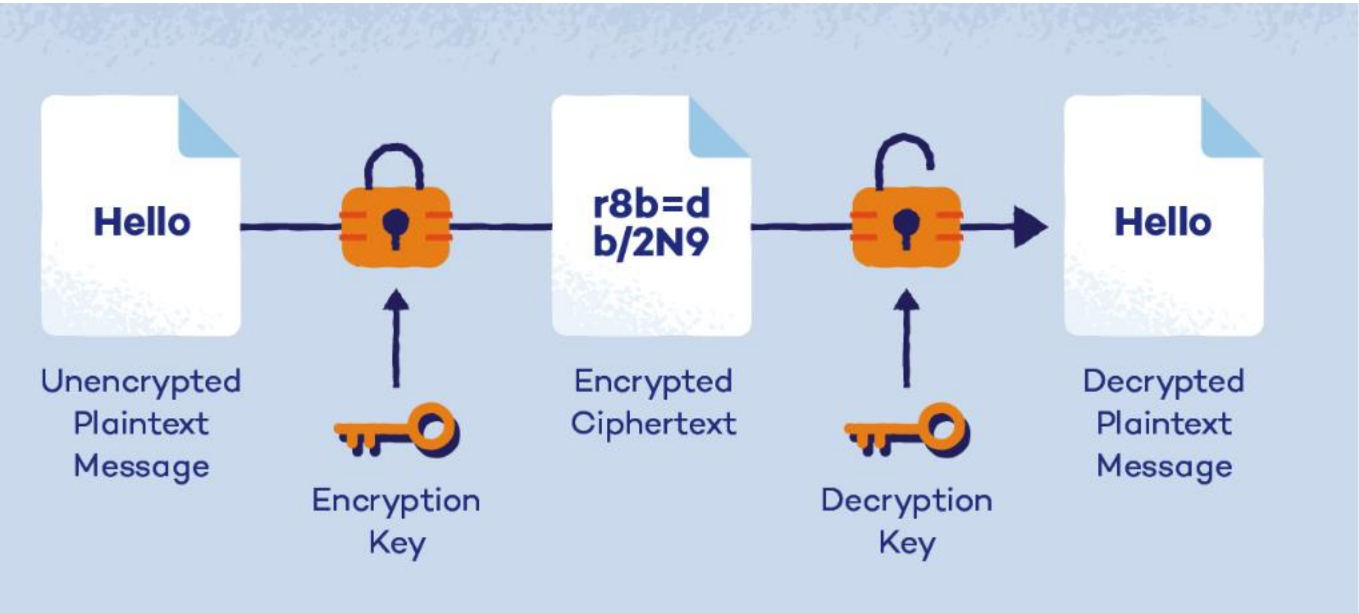


Entitlement	Super-Admin	Service-Admin	Storage-Admin	Dev	Security-Audit	Security-Admin
Volume Describe	X	X		X	X	X
Object Describe	X		X	X	X	X
Volume Modify	X	X		X		X
Read Logs	X				X	X

010
101
101
010
ENCRYPTION

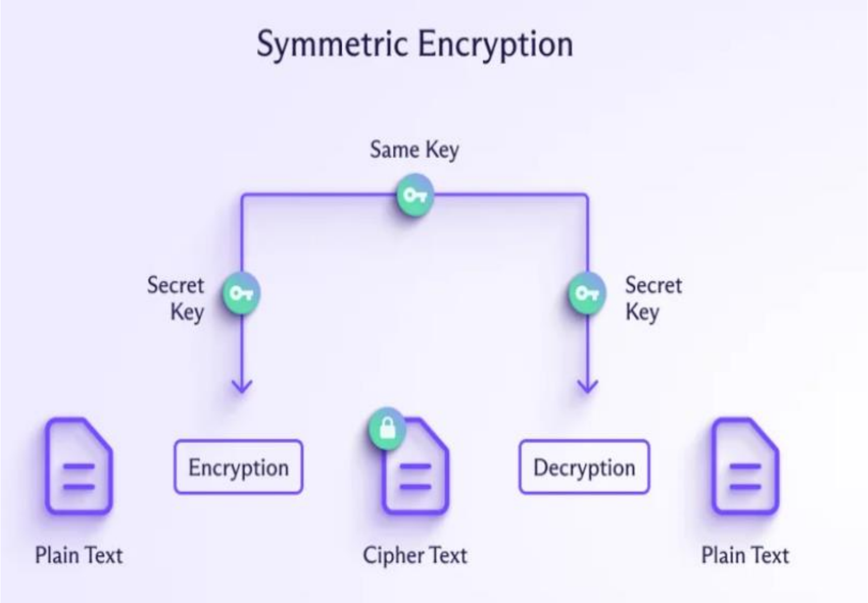
Encryption

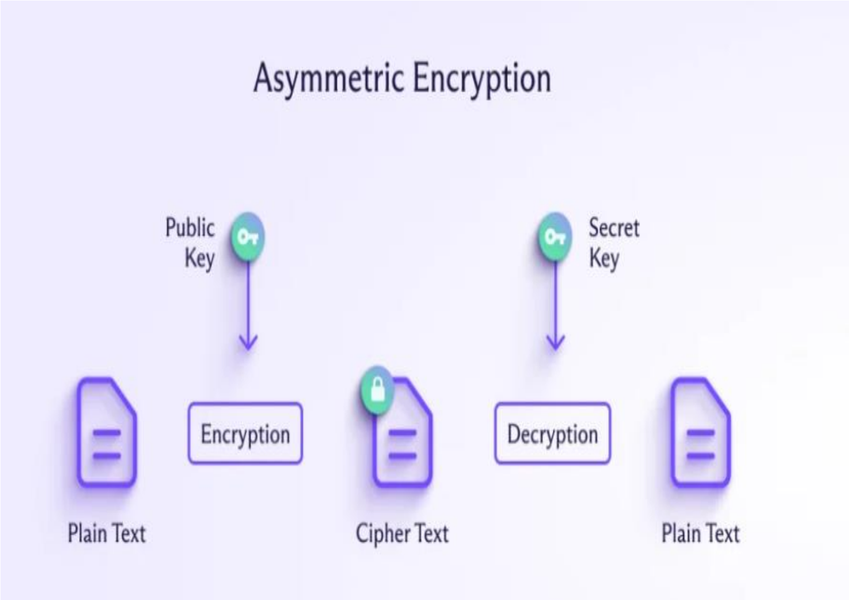
Encryption is the process of encoding data (plain-text) into random data (cipher-text) using a key



- https://www.pandasecurity.com/en/mediacenter/what-is-encryption/

Encryption Keys





–Symmetric key (secret key)

- Smaller key sizes
- Faster
- Key management is hard
- Typically used for data encryption

–Asymmetric key (public key)

- Larger key sizes
- Slower
- Key management is easier
- Typically used for digital signatures etc.

https://proton.me/blog/what-is-encryption

Encryption

- Data At Rest Encryption
  - Volume Level Encryption
    - Handled by the User/CSP
    - Only applicable for data on volume storage
    - **Instance-managed encryption:** The encryption engine runs within the instance, and the key is stored in the volume but protected by a passphrase or keypair.
    - **Externally managed encryption:** The encryption engine runs in the instance, but the keys are managed externally and issued to the instance on request.

Encryption

- Data At Rest Encryption
  - Object Level Encryption
    - **Cloud handles encryption:** Data is encrypted by the cloud after being transferred in. The cloud provider has access to the key and runs the encryption engine.
    - **Application handles encryption:**
      - The application (or client) encrypts the data before sending it to the cloud.
      - The cloud only stores the already-encrypted object.

Encryption

- Data In Motion Encryption
  - Most cloud providers’ APIs to interact with data natively support DIM encryption through
    - IPsec
    - VPN
    - etc.
  - Cloud Users and applications need to use DIM encryption when data goes from the cloud to the user and vice versa.
  - In hybrid architectures DIM encryption should be used when data moves from in house storage to the cloud and vice versa

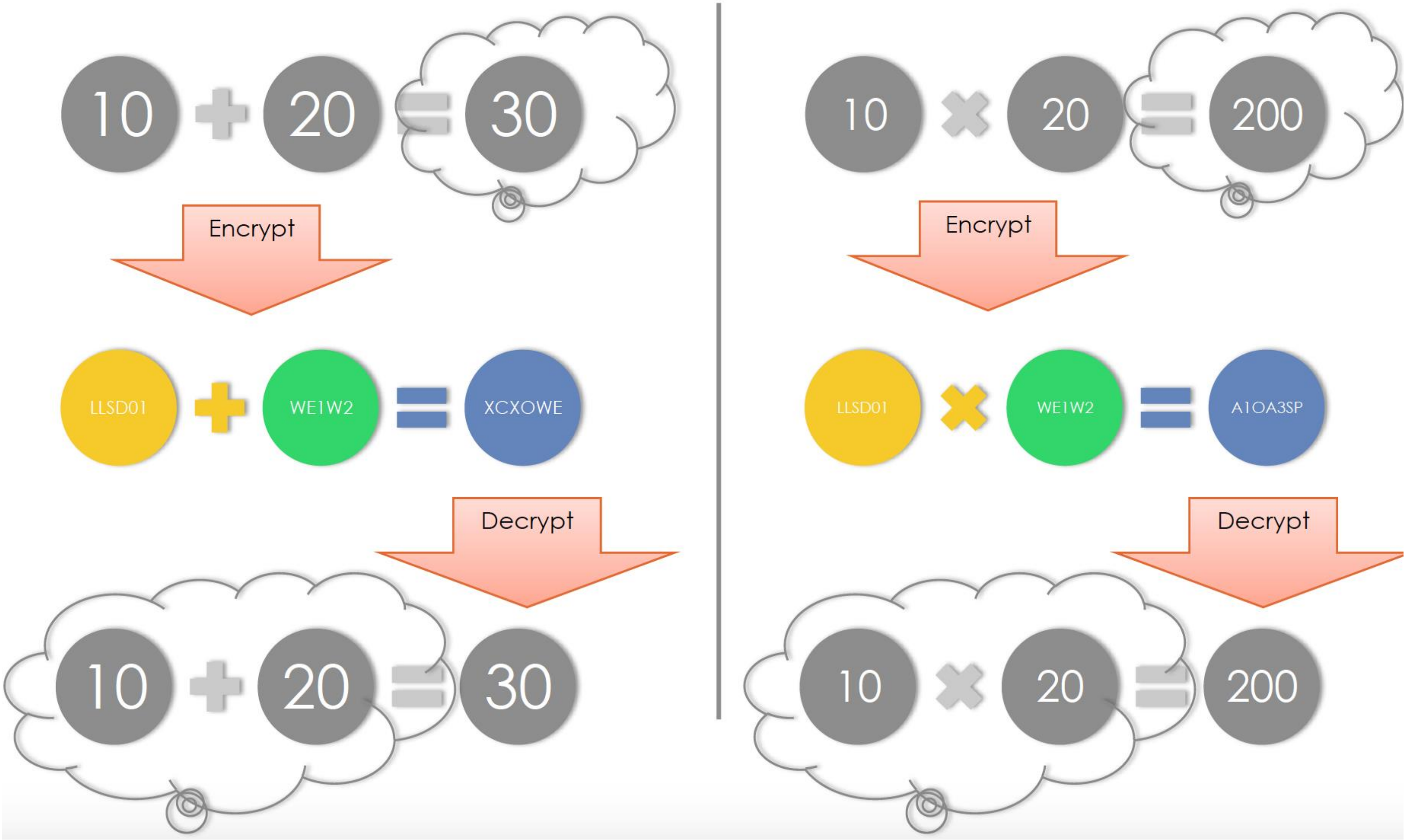
Encryption

- Data in Used (DIU) Encryption
  - Before data can be operated upon or is viewed by the user, it has to be decrypted and stored in the RAM as plain text
  - Enclaves
    - Create areas (enclaves) within RAM, where process data will be stored encrypted
    - Data is only decrypted in CPU registers or cache.

Encryption

- What if we never had to decrypt data?
  - Homomorphic Encryption
    - Allows a limited set of operations on encrypted data (typically addition or/and multiplication, comparison or search)
    - Partially homomorphic encryption
      - If only one operation is allowed
    - Fully homomorphic encryption
      - If both multiplication and addition are allowed

Partially homomorphic encryption



Examples: RSA, Elgamal etc.

Key Management

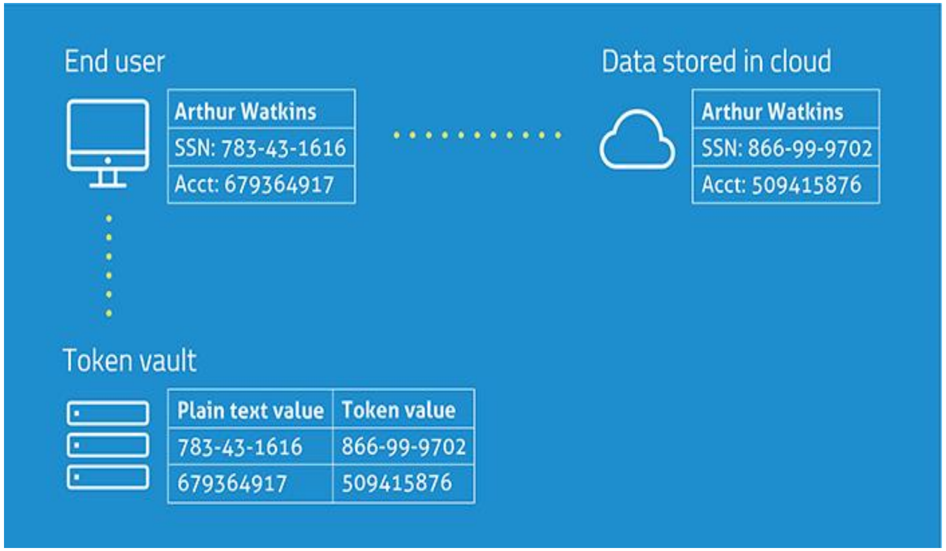
- Key Management refers to an efficient solution to generate, manage and store encryption keys.
- CSPs provide Key Management Systems to do this (e.g. AWS KMS).
- Ensure that your KMS solution is protected through IAM policies, least privilege and separation of duties principles.

Key Management

- There are four potential options for handling key management:
  - HSM/appliance: Use a traditional hardware security module (HSM) or appliance-based key manager, which will typically need to be on-premises, and deliver the keys to the cloud over a dedicated connection.
  - Virtual appliance/software: Deploy a virtual appliance or software-based key manager in the cloud.
  - Cloud provider service: This is a key management service offered by the cloud provider. Before selecting this option, make sure you understand the security model and SLAs to understand if your key could be exposed.
  - Hybrid: You can also use a combination, such as using a HSM as the root of trust for keys but then delivering application-specific keys to a virtual appliance that's located in the cloud and only manages keys for its particular context.

Tokenization

- Tokenization is the process of turning a meaningful piece of data, such as an account number, into a random string of characters called a token that has no meaningful value if breached.
- Tokens serve as reference to the original data, but cannot be used to guess those values.



End user

Arthur Watkins
SSN: 783-43-1616
Acct: 679364917

Data stored in cloud

Arthur Watkins
SSN: 866-99-9702
Acct: 509415876

Token vault

Plain text value	Token value
783-43-1616	866-99-9702
679364917	509415876