ENCRYPTION TECHNIQUES FOR SENSITIVE DATA

PRESENTATION

01 WHY ENCRYPTION MATTERS?

- **Protecting Sensitive Information:** Prevents unauthorized access during storage or transmission.
- **Maintaining Data Confidentiality:** Ensures information stays private.
- **Regulatory Compliance:** Adheres to legal standards for data protection.

02 WHY ENCRYPTION MATTERS?

Encryption relies on three key components:

- **Data:** The information to be protected.
- **Encryption Engine:** The algorithm or process that transforms data.
- **Key Manager:** Generates and manages the encryption keys.

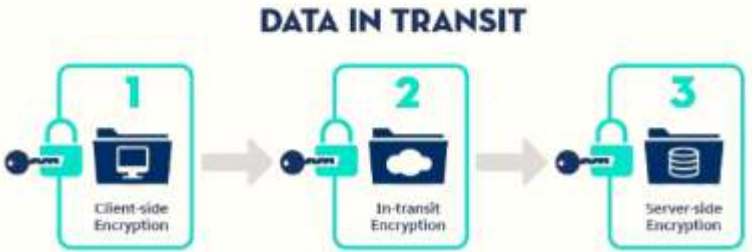
Data exists in two states:

- **Plaintext:** Readable data before encryption (e.g., "Hello, World!").
- **Ciphertext:** Unreadable data after encryption (e.g., "X5gH9kLm3pQw").

Encryption Keys:

- Random strings of bits that secure the encryption process.
- Without the correct key, ciphertext cannot be decrypted.

03 STATES OF DATA ENCRYPTION



Data in Transit:

- Actively moving information, such as emails, messages, or files being transferred over a network.
- Vulnerable to interception during transfer.

Data at Rest:

- Stored information, such as files on a hard drive, databases, or cloud storage.
- Secured through encryption to prevent unauthorized access and breaches.

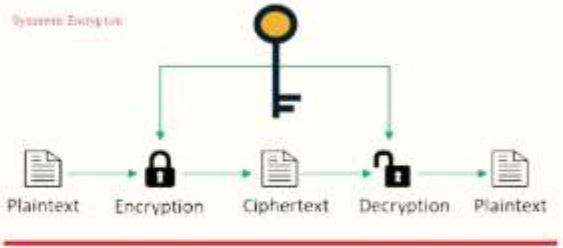
04 TYPES OF ENCRYPTION

Symmetric Encryption:

- Uses a **single key** for both encryption and decryption.
- It is **efficient and fast** but faces challenges in securely managing and distributing the key.
- Examples include **AES (Advanced Encryption Standard)** and **DES (Data Encryption Standard).**

Asymmetric Encryption:

- **Uses a pair of keys**: a public key for encryption and a private key for decryption.
- It is **more secure for key distribution** but is **computationally intensive** and slower than symmetric encryption.
- An example is **RSA (Rivest-Shamir-Adleman).**

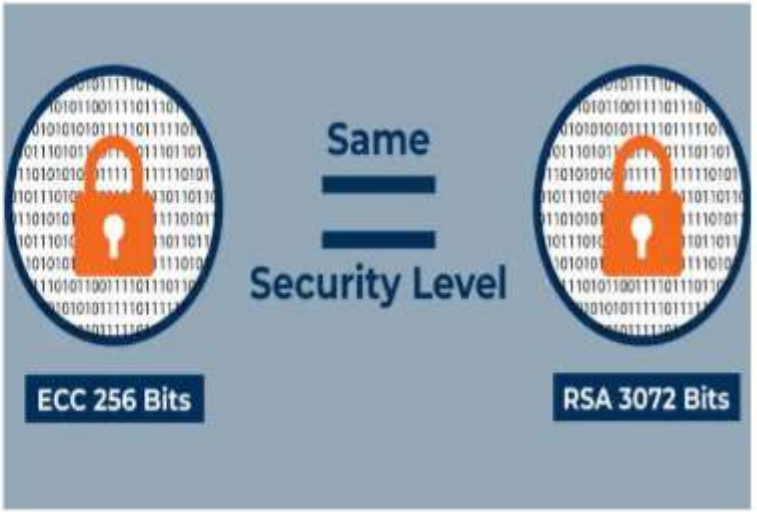


05 POPULAR ENCRYTION METHODS

Encryption algorithms are the mathematical formulas used to secure data by transforming it into unreadable ciphertext. These algorithms ensure that sensitive information remains confidential, whether it's stored on a device or transmitted over a network. Different algorithms are designed for specific use cases, balancing factors like security, speed, and key management.

ECC (ELLIPTIC CURVE CRYPTOGRAPHY)

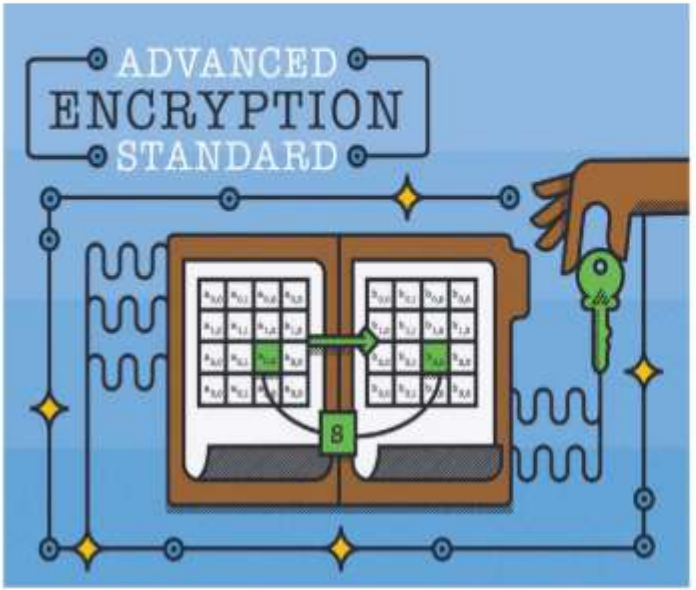
ECC is an **asymmetric encryption algorithm** that provides strong security with shorter key lengths, making it ideal for mobile devices and systems with limited resources.



TWOFISH

Twofish is a **symmetric encryption algorithm** that is **fast**, **efficient**, and **free to use**, making it popular in software applications and file encryption

AES (ADVANCE ENCRYPTION STANDARD)



AES is a **symmetric encryption algorithm** known for its high security and widespread use, supporting key lengths of **128**, **192**, and **256** bits.

3DES (TRIPLE DATA ENCRYPTION STANDARD

3DES is an **enhanced version of DES** that uses **three keys** for added security, though it is slower than AES and primarily used in legacy systems.

RSA (RIVEST-SHAMIR-ADLEMAN)

RSA is an **asymmetric encryption algorithm** that forms the foundation of internet security protocols like **HTTPS**, using a public key for encryption and a private key for decryption.

06 BEST PRACTICES FOR ENCRYPTING DATABASE FIELDS

- **Hash passwords** using secure algorithms like bcrypt to protect user credentials.
- **Encrypt personal identifiers and financial data** (e.g., credit card numbers, Social Security numbers) using strong encryption methods like **AES (Advanced Encryption Standard)**.
- **Implement secure key management practices** to ensure encryption keys are stored and accessed securely.

```
-- Example of encrypting a database field using SQLite
UPDATE users
SET credit_card = AES_ENCRYPT('1234-5678-9012-3456', 'encryption_key');
```

07 COMPLIANCE WITH DATA SECURITY STANDARDS

Key Regulations:

- **Data Privacy Act of 2012 (Philippines):** Protects personal data and ensures privacy rights for individuals.
- **ISO 27001/27701:** International standards for information security and privacy management.

Implementation Steps:

1. Review legal requirements to ensure compliance with relevant regulations.
2. Conduct regular audits to assess and improve data security practices.
3. Document encryption practices to demonstrate compliance during audits or inspections.