End-to-end Encryption

Source: TH

Why in News?

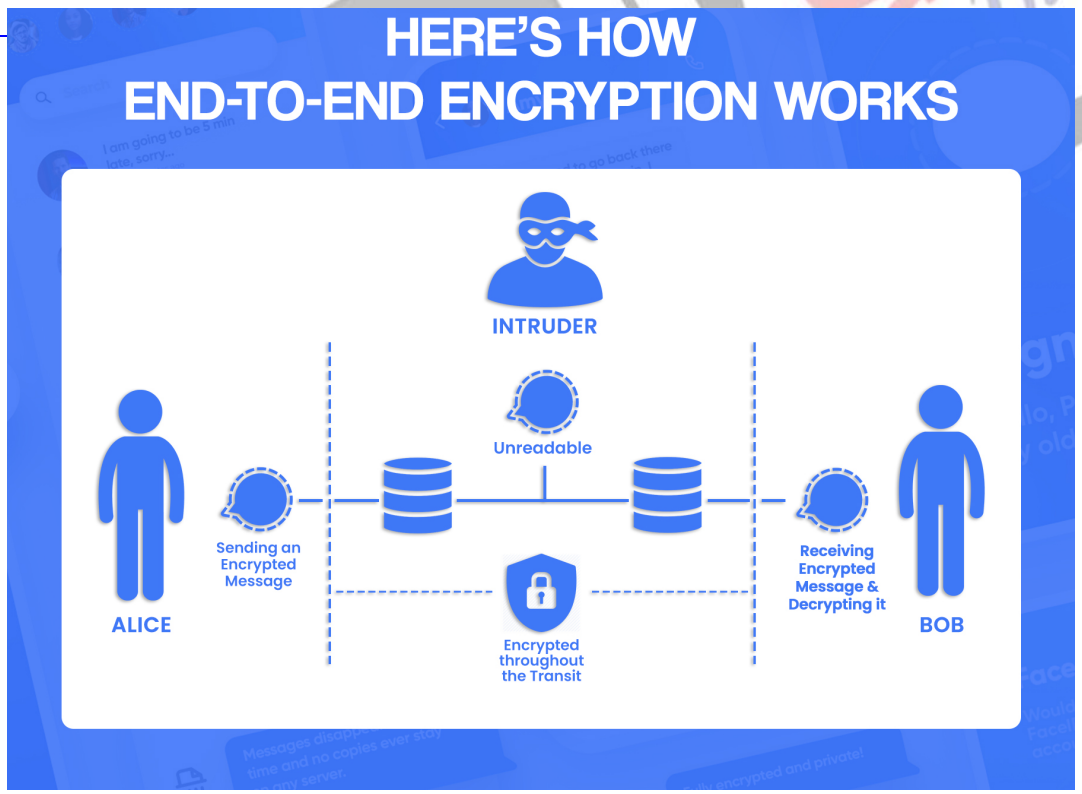
End-to-end encryption is crucial for **cybersecurity**, ensuring secure transmission of sensitive data by **encoding** it exclusively for the sender and recipient.

- It protects against unauthorized access, theft, surveillance, and tampering, especially in the face of rising **cyber threats.**

What is Encryption?

- **About:** Encryption involves **transforming** consumable information into an unconsumable form according to various rules, fundamentally encompassing different rule sets.
    - In this context, the **key** is a set of data that enables a computer to **decrypt** encrypted text by understanding the specific rules used to encrypt it.

//



- **E2E Encryption:** E2E encryption involves securing specific points through which data is transmitted.
    - When communicating with a friend on a messaging app, messages are encrypted during

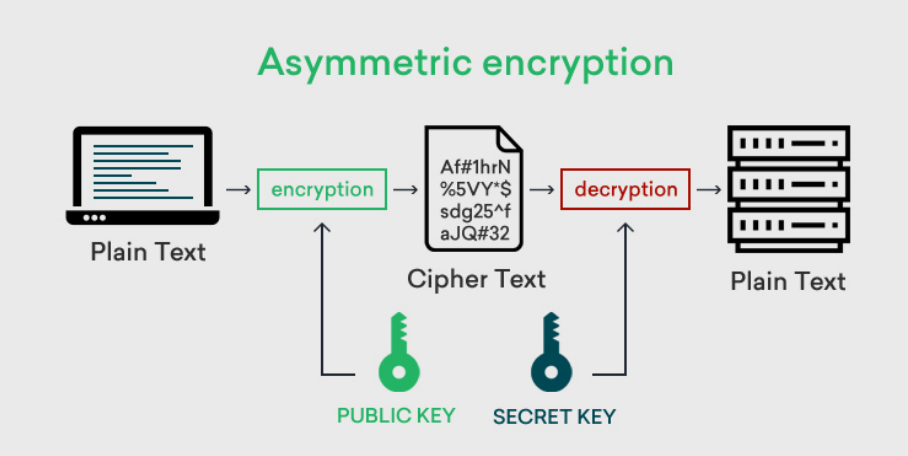
transit to **prevent unauthorized access**, employing both encryption-in-transit, which secures messages during relay between the server and the user, and **end-to-end encryption (E2E)**, which ensures encryption both during transit and while stored on the server until the recipient decrypts it.

Think of it like this:

1. Regular message: Sending a postcard - anyone can read it.

2. End-to-end encryption: Sending a sealed, coded letter - only the recipient with the right code can read it.

- **Process of Encryption**: Various encryption methods can be employed based on the desired level of secrecy and protection for information.
  - **Symmetric encryption** involves **using the same key** for both encrypting and decrypting information, with **Data Encryption Standard (DES)** serving as a well-known example of a **symmetric encryption protocol.**
    - Symmetric encryption, exemplified by the **Advanced Encryption Standard (AES)** used in scenarios like encrypting a computer's hard drive or setting a **WiFi password**, proves beneficial when the sender and recipient are identical entities.
  - **Asymmetric encryption**, also known as **public-key cryptography,** operates on the principle of using a **pair of keys:** a public key and a private key.
    - The **public key** is openly shared and can be used by anyone to encrypt messages, but only the possessor of the corresponding **private/secret key** can decrypt those messages.
    - This asymmetric encryption approach **ensures secure communication** without the need for both parties to share the same key. This way, the encryption process can be public, but decryption remains private, providing a secure means of communication.



- **Vulnerabilities of E2E Encryption:** While E2E encryption is a robust security measure, various factors, including potential vulnerabilities like **Man In the Middle (MITM) attacks**, user complacency, malware threats, company backdoors, and legal requirements, can impact the overall security of encrypted messages.

What is the Role of Hash Function?

- There are different symmetric and asymmetric schemes that encrypt messages in different ways, i.e. using different **hash functions.**
  - The role of a hash function is to encrypt a message while ensuring certain properties:
    - **Message Concealment:** The hash function should take an input message and generate an **encrypted version** known as the **digest.** Importantly, given the digest, it should not reveal information about the original message.
    - **Fixed-Length Output:** The function should accept messages of variable lengths

and produce a digest with a fixed length. This **prevents deducing** the original message length from the digest length.
- **Unique Digests:** The hash function must produce **unique digests** for unique messages, ensuring that different messages do not result in the same hash.

UPSC Civil Services Examination, Previous Year Question (PYQ)

Prelims:

Q.The terms 'WannaCry, Petya and EternalBlue' sometimes mentioned in the news recently are related to (2018)

(a) Exoplanets
(b) Cryptocurrency
(c) Cyber attacks
(d) Mini satellites

Ans: C

Mains:

Q. Keeping in view of India's internal security, analyse the impact of cross-border cyber-attacks. Also, discuss defensive measures against these sophisticated attacks. **(2021)**