CRYPTOGRAPHY: ENCRYPTION & WHATSAPP!

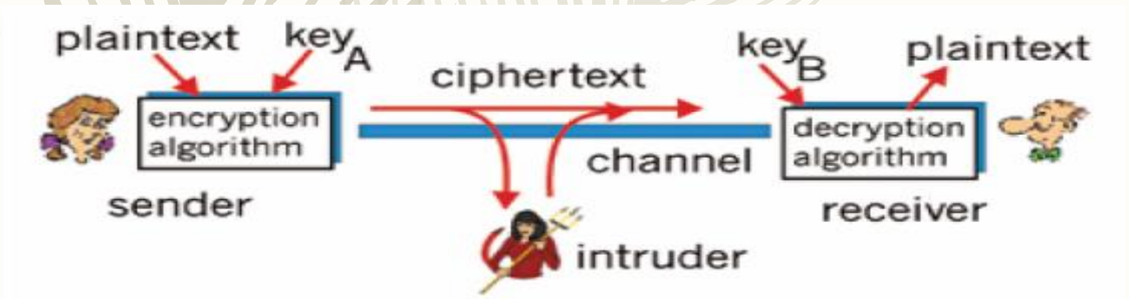
– What is Cryptography?

Converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without anyone decoding it back into a readable format.

– Why should we care?

Authentication, Data Confidentiality, Data Integrity and Non-Repudiation

– Principles of Cryptography



What is Encryption?

The process of converting the information from ‘plain text’ to ‘cipher text’ is known as ‘encryption.’

Symmetric encryption: separate instance of the same “key”; DES, 3DES

Asymmetric encryption : use different “keys” ; RSA,AES

– What does end-to-end encryption mean?

- Only the data is encrypted
- Headers, trailers, and routing information are not encrypted
- Implemented using asymmetric cryptography or public key systems

– Encryption in Whatsapp !!

- The conversations and calls are “end-to-end” encrypted
- “Once a session has been established, clients exchange messages that are protected with a Message Key using AES256 in CBC mode for encryption and HMAC-SHA256 for authentication”

How to verify?

– Open the chat.

– Tap on the name of the contact to open the contact info screen.

– Tap Encryption to view the QR code and 60-digit number.