Cryptography

Cryptography

Cryptography is the science of using mathematics to encrypt and decrypt data.

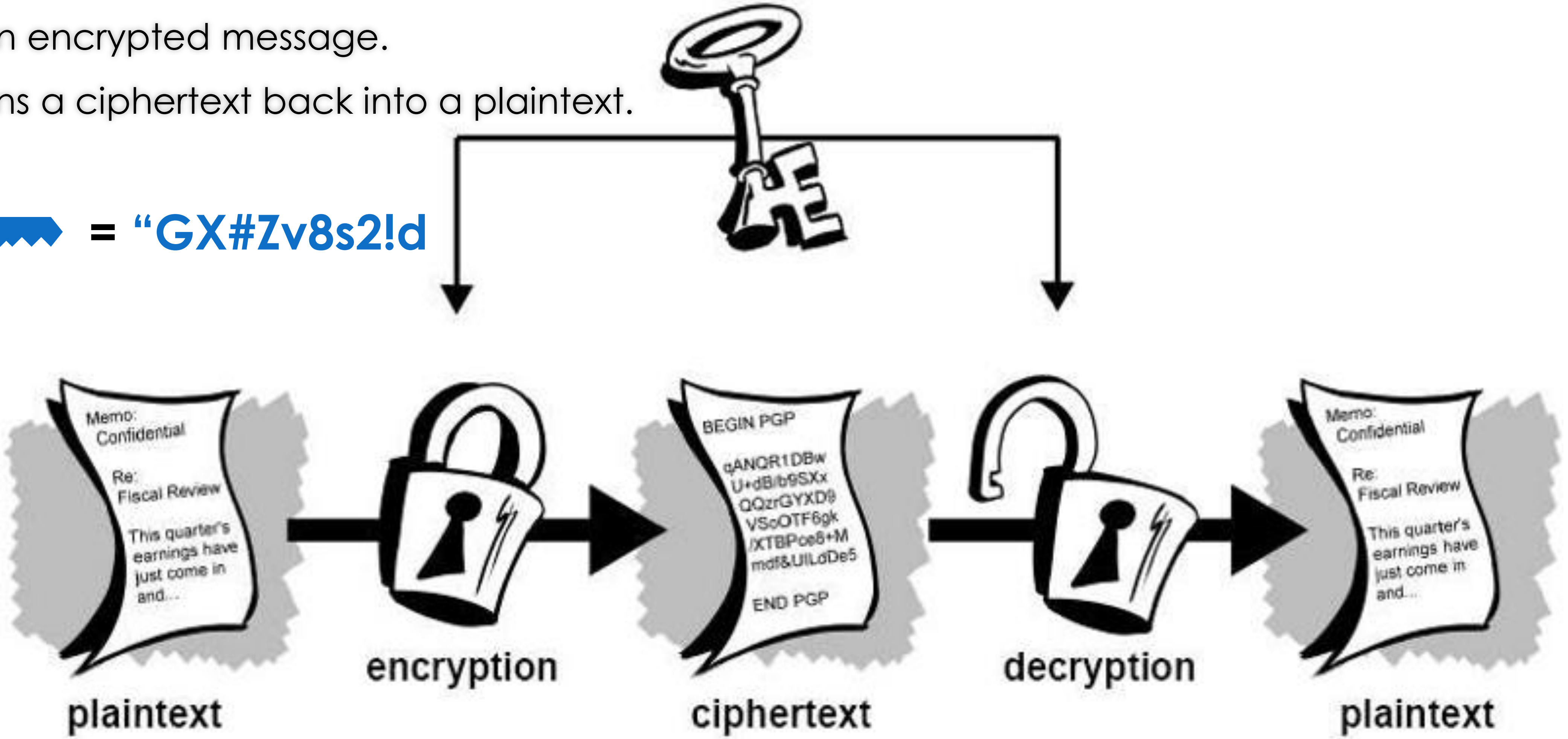
“Hello” + 🔑 = “GX#Zv8s2!d

Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

Definitions

- **Plaintext** (Cleartext) is an unencrypted message.
- **Key** is a sequence of letters, numbers or symbols rather like a password.
- **Encryption** converts the plaintext to a ciphertext.
- **Ciphertext** is an encrypted message.
- **Decryption** turns a ciphertext back into a plaintext.

“Hello” + 🔑 = “GX#Zv8s2!d



Definitions

- **Cryptosystem:**

  Hardware or software implementation of cryptography that contains all the necessary software, protocols, algorithms, and keys.

- **Algorithm (Cipher):**

  Set of mathematical and logic rules used in cryptographic functions.

- **Cryptology:**

  The study of both cryptography and cryptanalysis.

- **“Kerckhoffs” principle:**

  Concept that an algorithm should be known and only the keys should be kept secret.

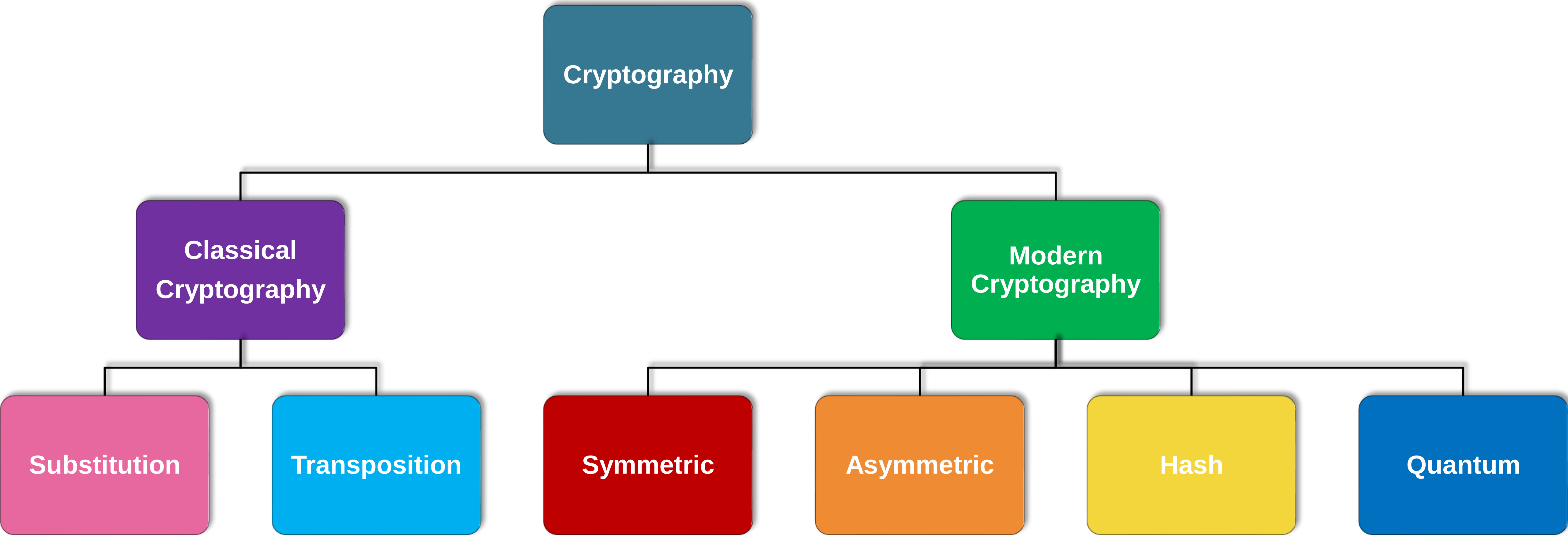
Definitions

○ Cryptanalysis:

is the science of breaking encrypted communication.

- ➢ Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.
- ➢ It uses mathematical analysis of the cryptographic algorithm, as well as side-channel attacks that do not target weaknesses in the cryptographic algorithms themselves, but instead exploit weaknesses in their implementation and the devices that run them. like frequency analysis

Cryptography Classification



Thank you