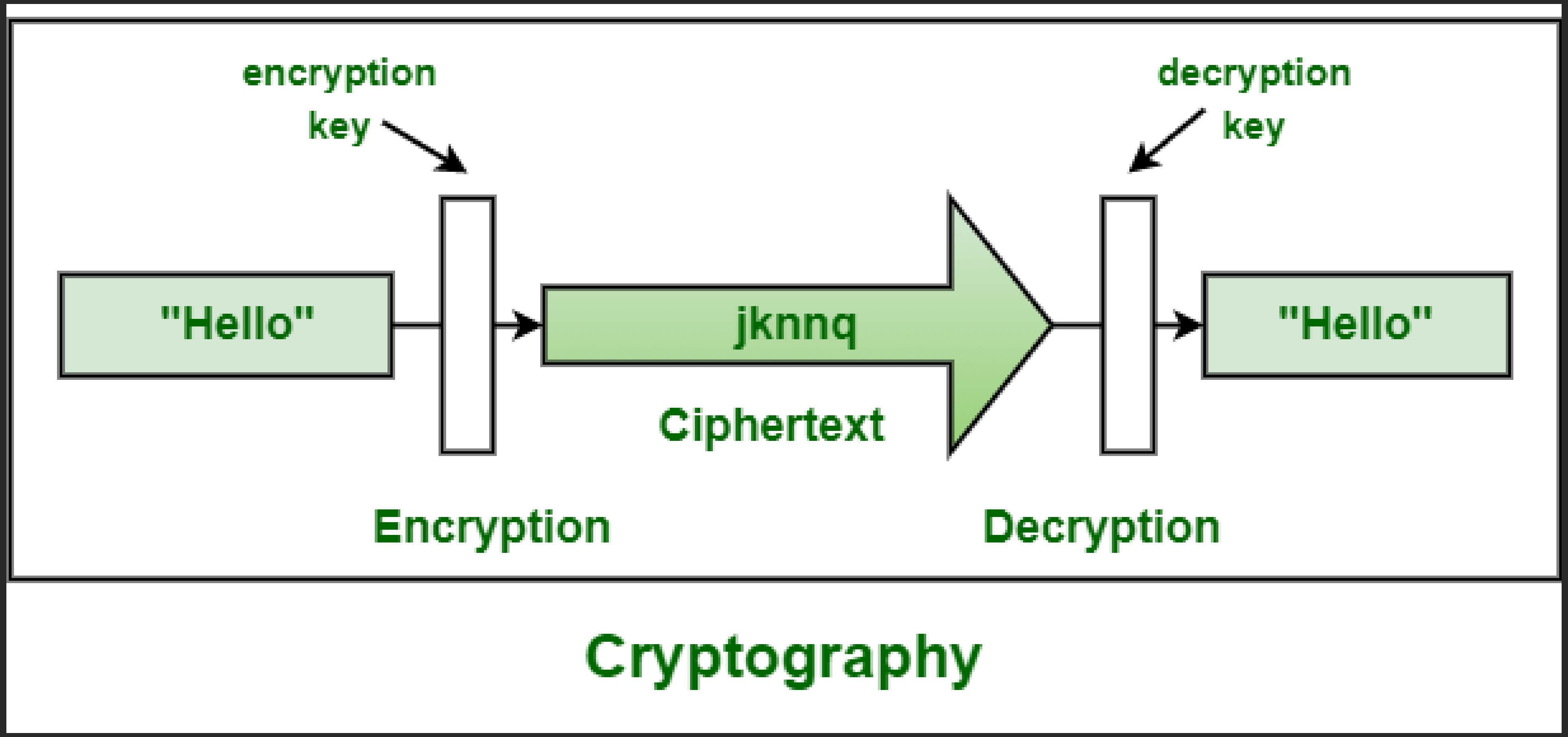
CRYPTOGRAPHY

Nguyễn Đăng Khoa
Nguyễn Minh Tùng
Phạm Thiên Nhật
Nguyễn Trần Nhật Bảo

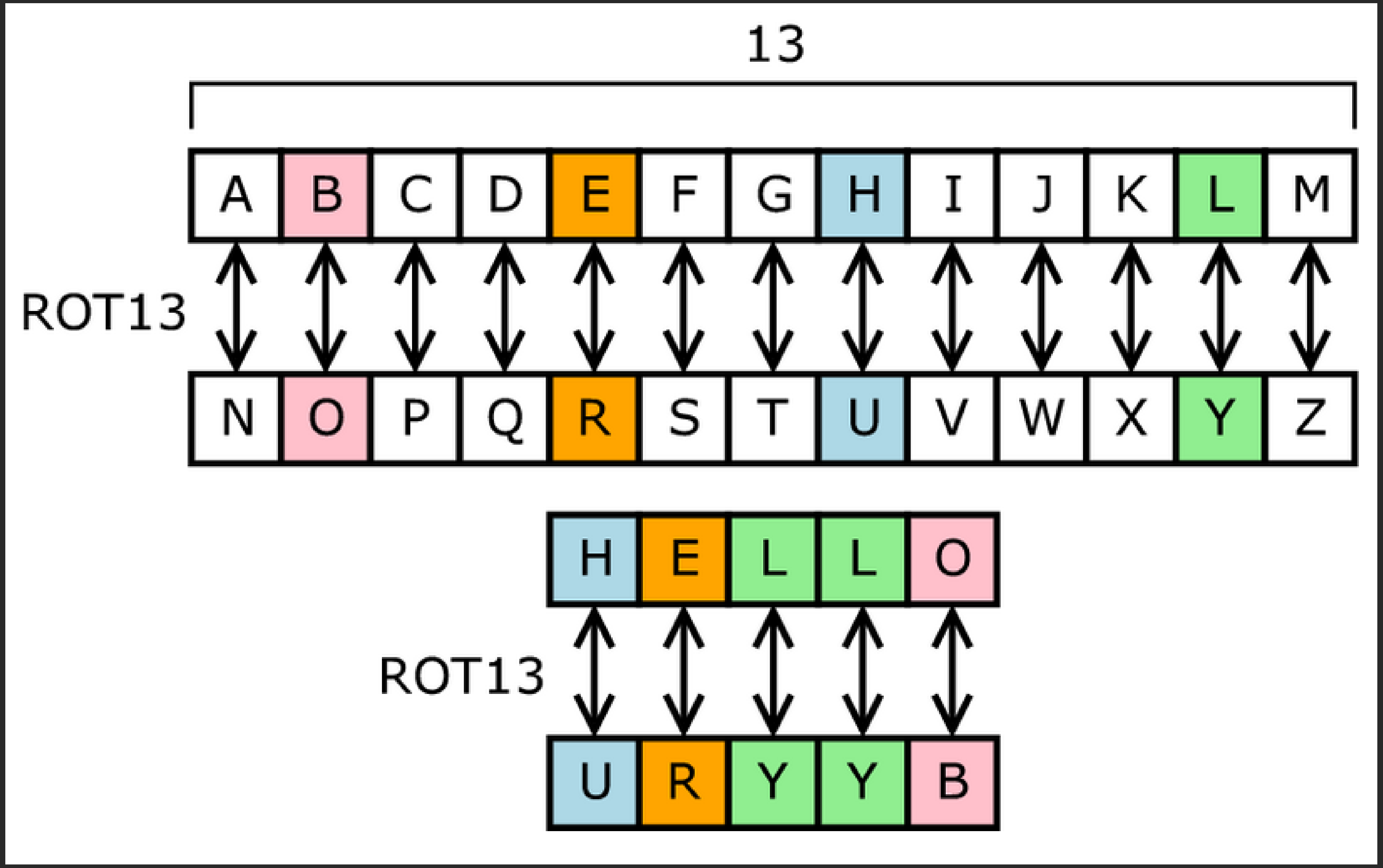
WHAT IS CRYPTOGRAPHY

Cryptography is the practice and study of techniques for secure communication
Cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages

Alice and Bob – are shouting their messages in a room full of people. The goal is to protect this communication so that only Alice and Bob can understand the content of the messages.



WHAT IS CRYPTOGRAPHY



MODERN CRYPTOGRAPHY

Modern cryptography is heavily based on mathematical theory and computer science practice

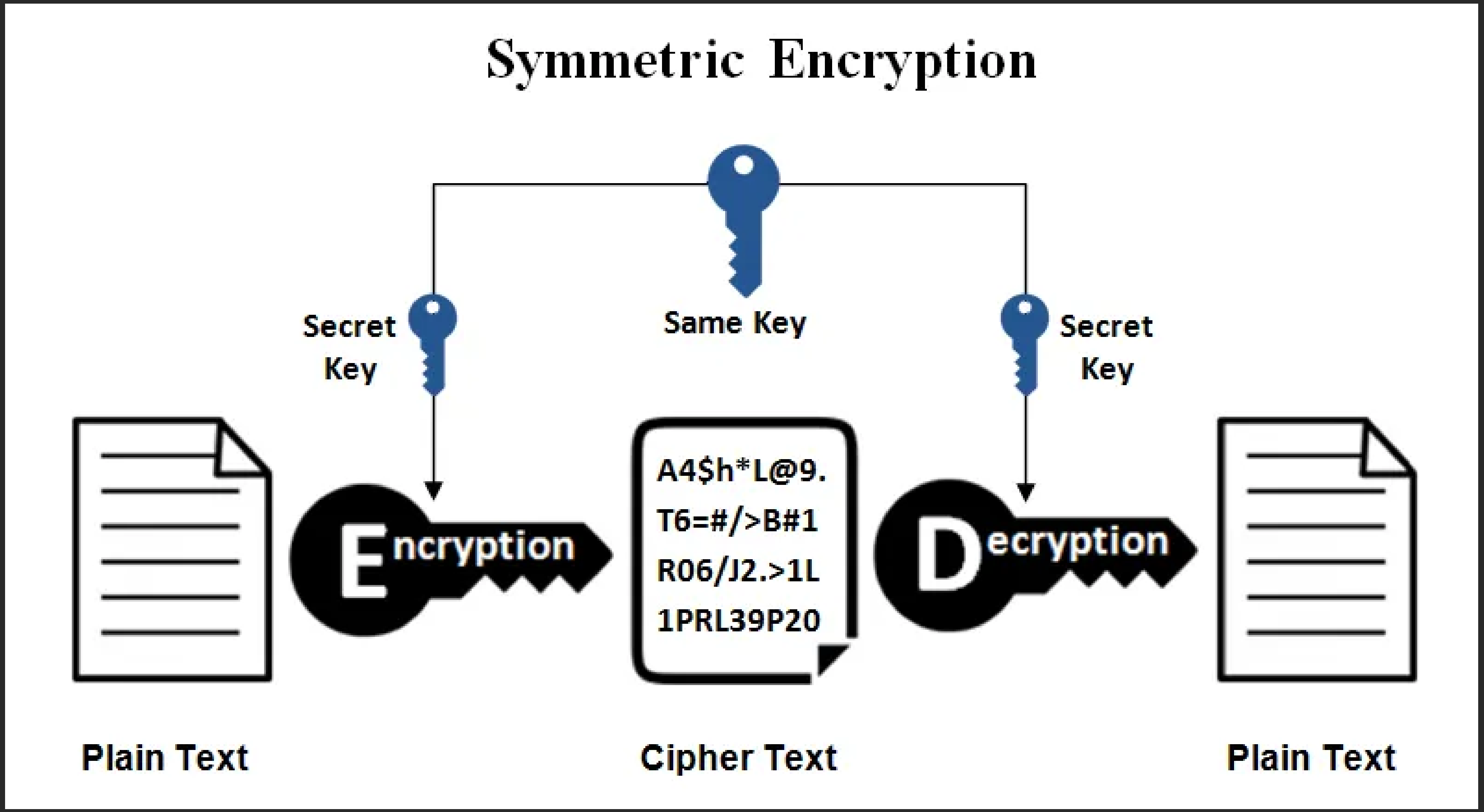
Modern cryptography has many purposes:

- Confidentiality
- Authentication
- Integrity checking
- Non-repudiation

TYPES OF CRYPTOGRAPHY

One major drawback that the two parties must somehow exchange the key in a secure way as there is only one single key for encryption as well as decryption process.

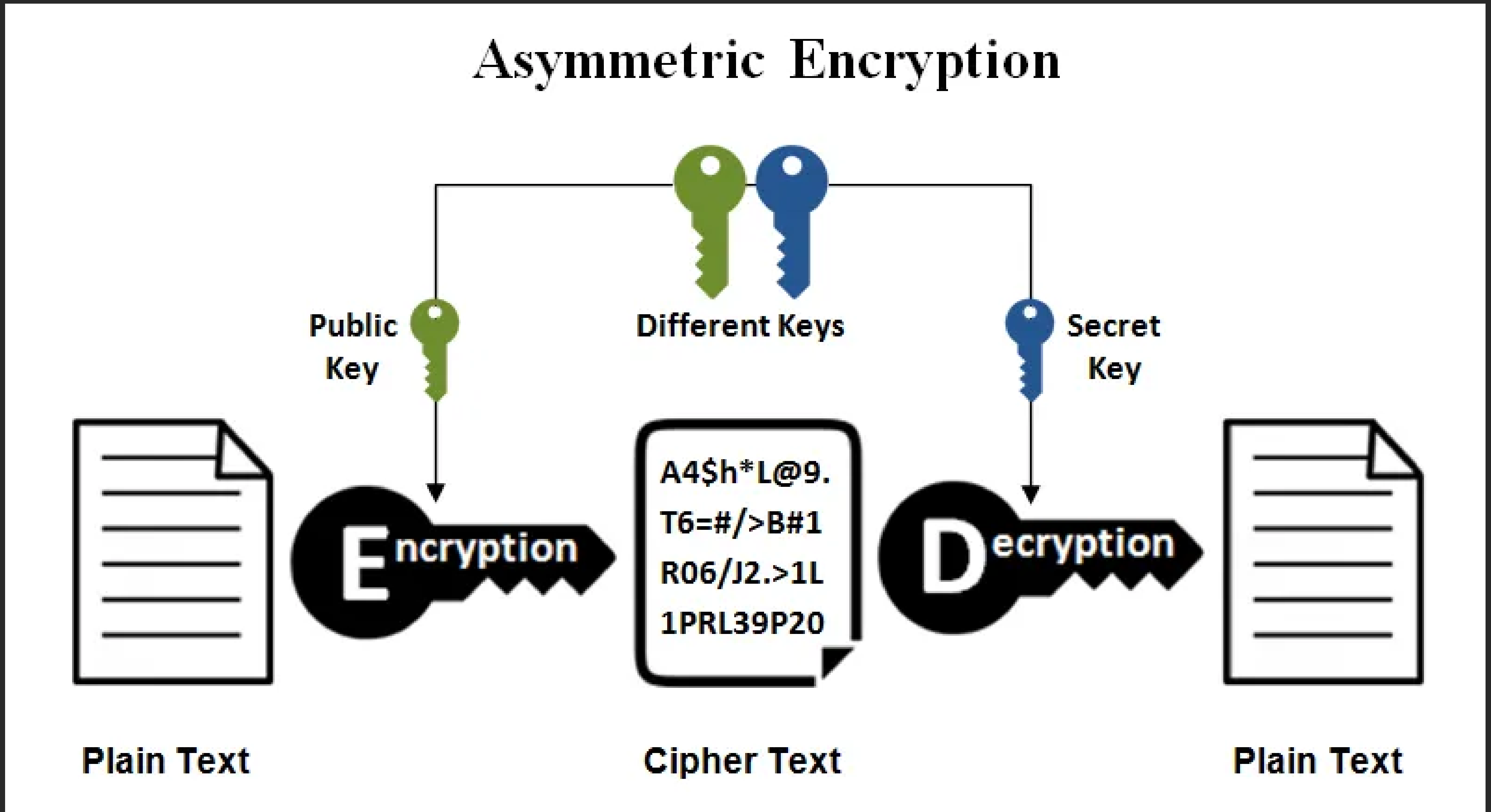
Example: AES (Advanced Encryption Standard), DES



TYPES OF CRYPTOGRAPHY

Every user uses two keys (private key and public key).
Either of the key can be used to encrypt the message and the one left is used for decryption purpose.

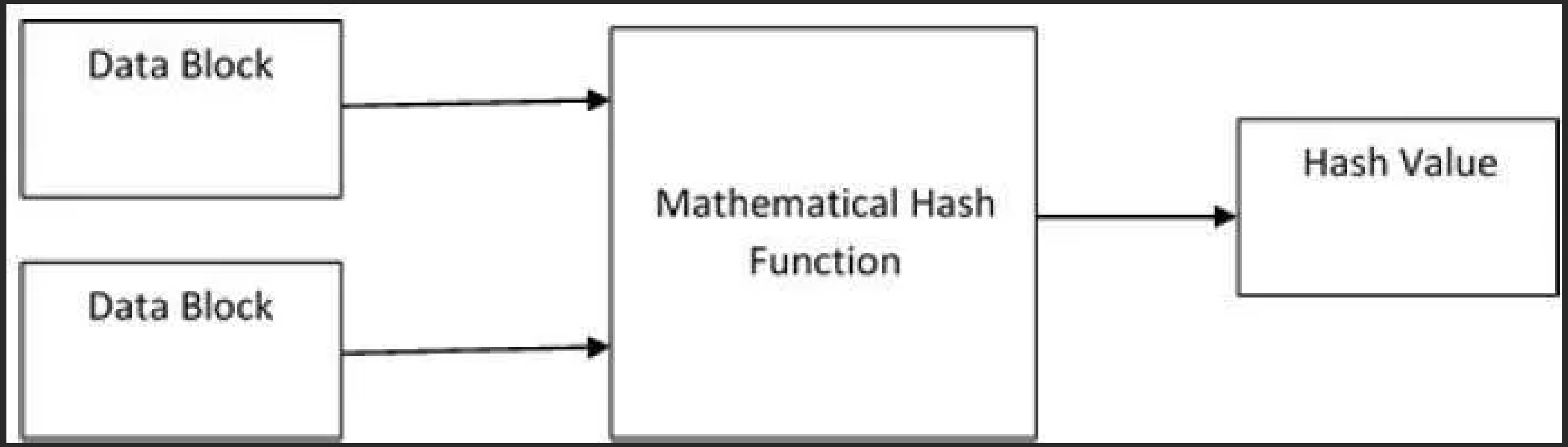
Example: RSA, DSA, ...



TYPES OF CRYPTOGRAPHY

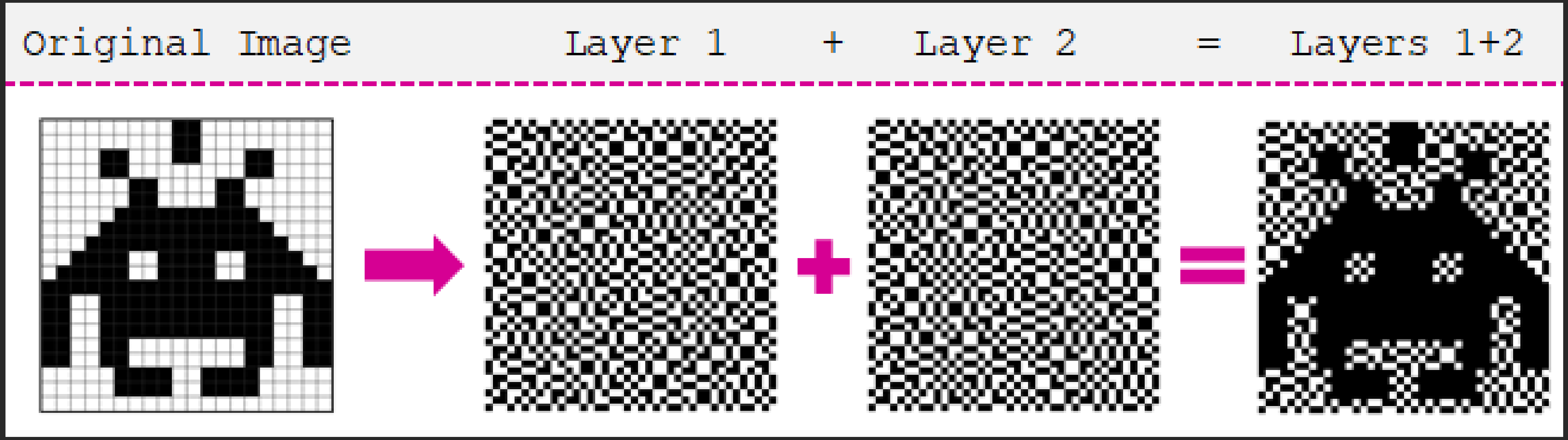
A Hash function is a cryptography algorithm that takes input of arbitrary length and gives the output in fixed length.
This system operates in one-way manner and does not require any key.

Example: MD5, SHA



VISUAL CRYPTOGRAPHY

A cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decrypted information appears as a visual image


Original Image
Layer 1
+
Layer 2
=
Layers 1+2