INTRODUCTION TO CRYTOGRAPHY

```
~ $ alias aryanploxxx = “Aryan Gupta” _
```

What is Cryptography?

- Art of protecting information by transforming it into unreadable format
- It is about constructing and analysing protocols that prevent third parties or public from reading private messages

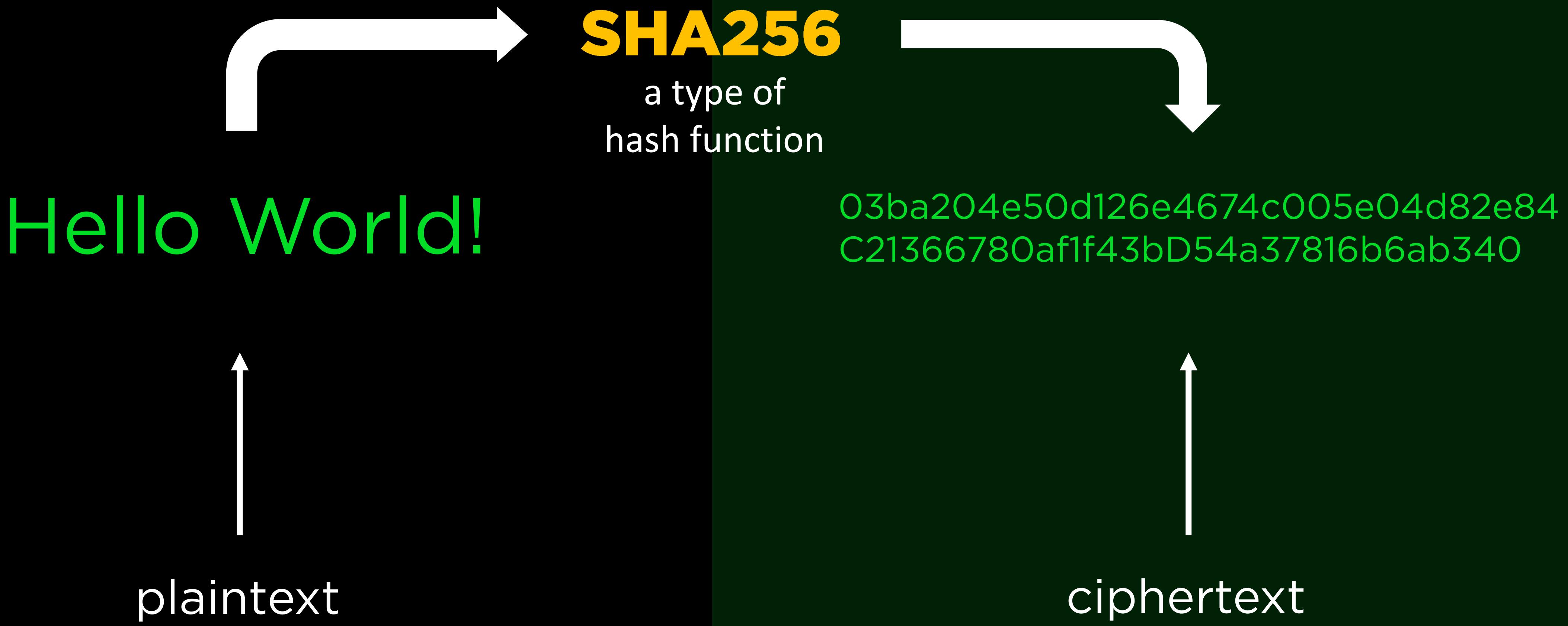
Current Applications of Cryptography

- Secure communications
- End-to-end Encryption
- Storing Data
- Authentication of Identity
- Blockchain/Cryptocurrency

Encryption/Decryption

plaintext $\xrightarrow{\text{encryption}}$ ciphertext $\xrightarrow{\text{decryption}}$ plaintext

1. Plaintext: a message in its original form
2. Ciphertext: a message in the transformed, unrecognized form
3. Encryption: the process for producing ciphertext from plaintext
4. Decryption: the reverse of encryption
5. Key: a secret value used to control encryption/decryption



SHA256

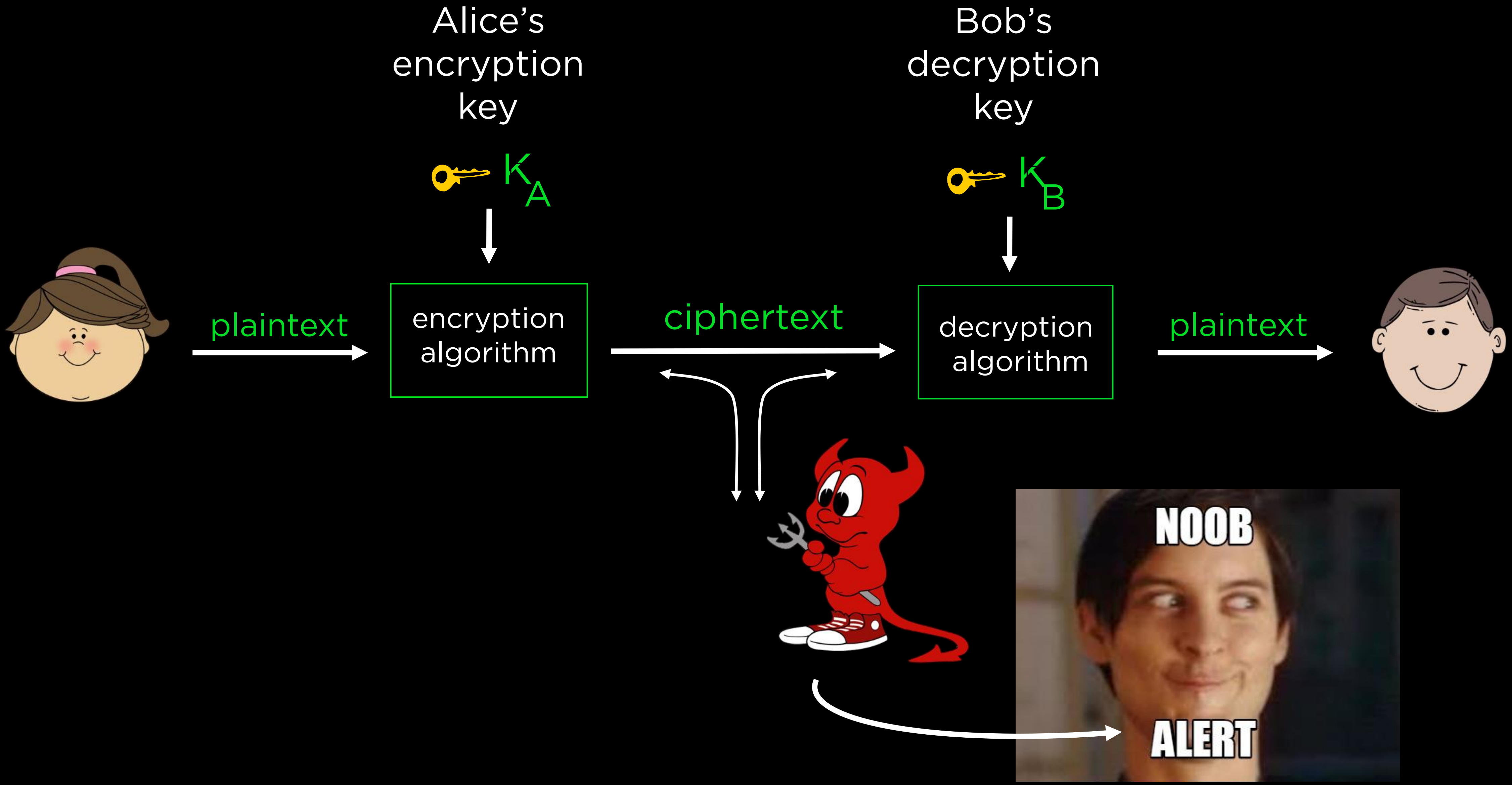
a type of
hash function

Hello World!

03ba204e50d126e4674c005e04d82e84
C21366780af1f43bD54a37816b6ab340

plaintext

ciphertext



Alice’s encryption key

K_A

Bob’s decryption key

K_B

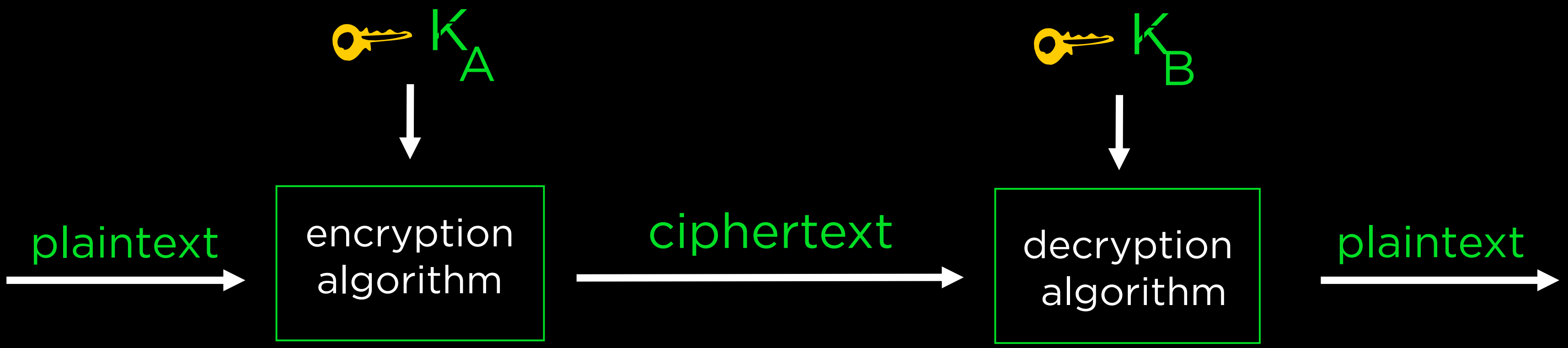
plaintext

encryption algorithm

ciphertext

decryption algorithm

plaintext



If K_A and K_B are same, then these type of ciphers are **Symmetric Ciphers**.

If K_A and K_B are different, then these type of ciphers are called **Asymmetric Ciphers**.

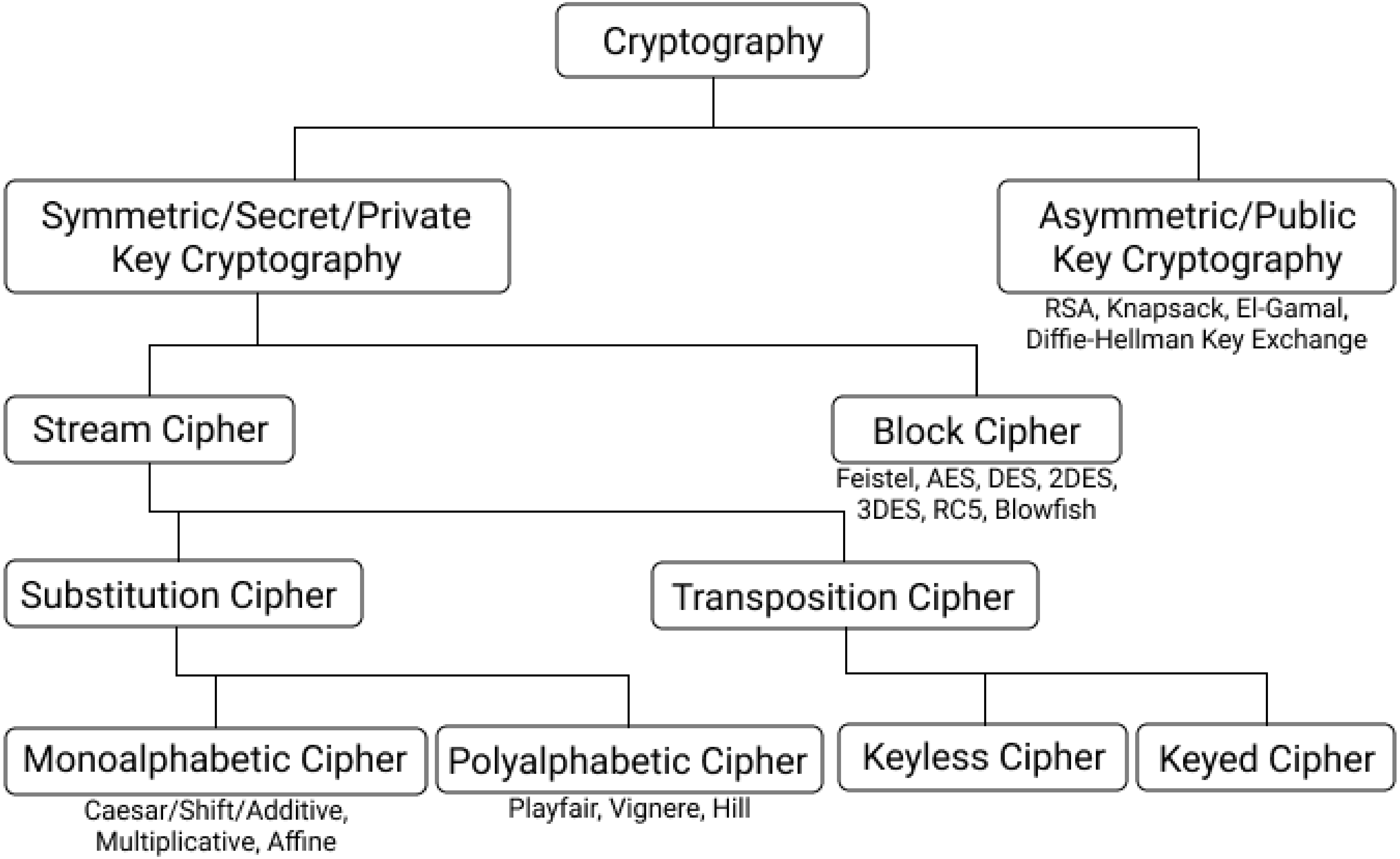
Third type of ciphers are **Hash Functions**, which will be discussed later.

Symmetric Cryptography

- Also called Secret Key Cryptography / Private Key Cryptography
- Used for transfer of bulk data, since it’s faster.
- Most popular example – DES
- Other examples – AES, RCY, 2DES etc.

Asymmetric Cryptography

- Also called Public Key Cryptography.
- Uses a pair of keys – *{ public , private}*
- Popular Examples – RSA, DSA, Diffie-Hellman, Elliptic Curves etc.



Cryptography

Symmetric/Secret/Private Key Cryptography

Asymmetric/Public Key Cryptography

RSA, Knapsack, El-Gamal, Diffie-Hellman Key Exchange

Stream Cipher

Block Cipher

Feistel, AES, DES, 2DES, 3DES, RC5, Blowfish

Substitution Cipher

Transposition Cipher

Monoalphabetic Cipher

Caesar/Shift/Additive, Multiplicative, Affine

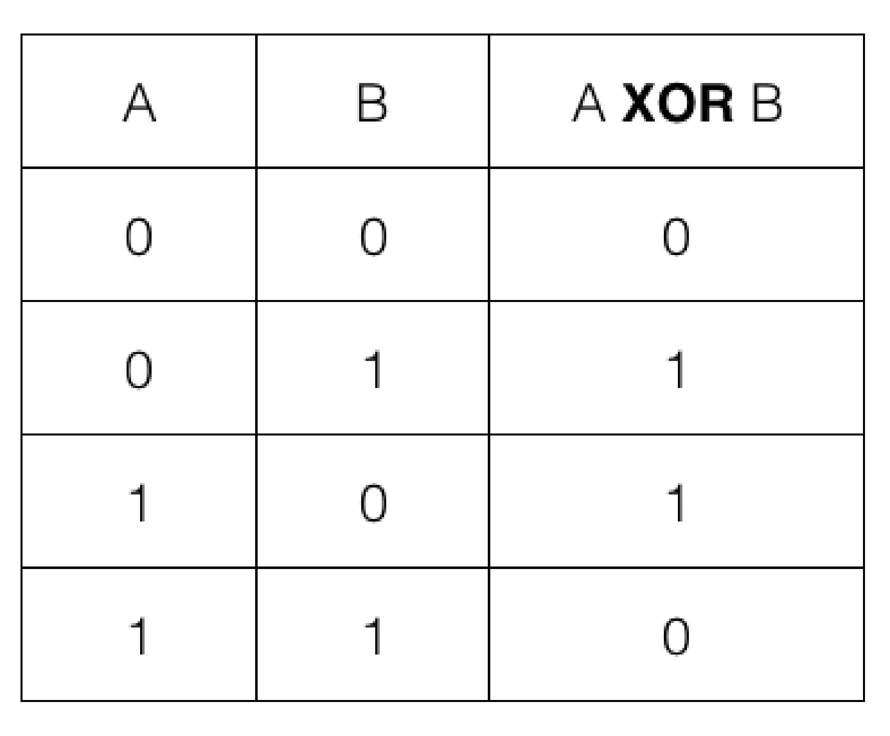
Polyalphabetic Cipher

Playfair, Vignere, Hill

Keyless Cipher

Keyed Cipher

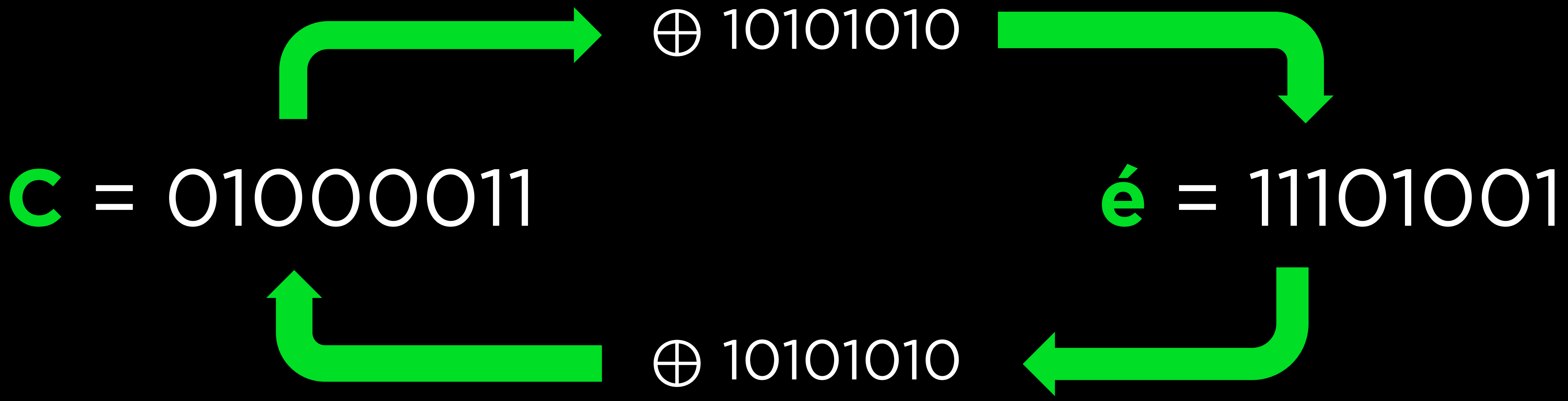
BITWISE XOR Operator



A	B	A **XOR** B
0	0	0
0	1	1
1	0	1
1	1	0

$$
\begin{array}{rcccccc l}
 & 1 & 1 & 0 & 1 & 1 & 0 & \text{plain text} \\
\oplus & 1 & 0 & 0 & 1 & 0 & 1 & \text{key} \\
\hline
 & 0 & 1 & 0 & 0 & 1 & 1 & \text{cipher text} \\
\oplus & 1 & 0 & 0 & 1 & 0 & 1 & \text{key} \\
\hline
 & 1 & 1 & 0 & 1 & 1 & 0 & \text{plain text}
\end{array}
$$

BITWISE XOR Operator



⊕ 10101010

C = 01000011

é = 11101001

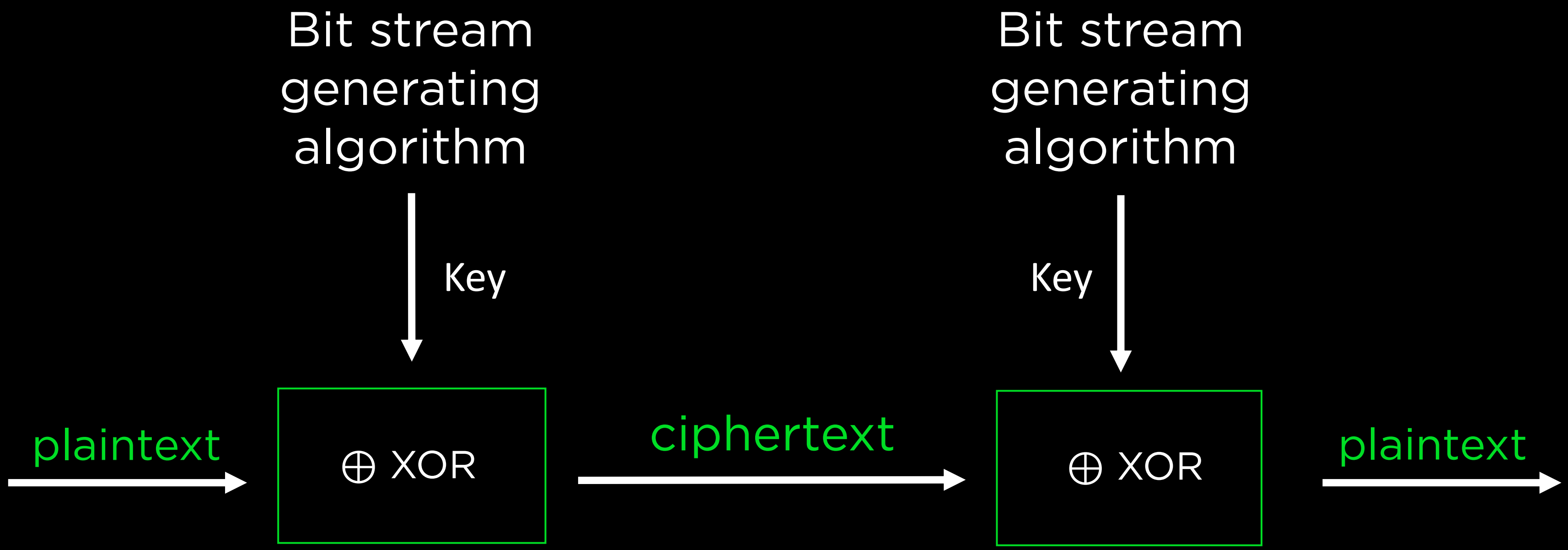
⊕ 10101010

Stream Cipher

- Type of Symmetric Key Cipher.
- Encrypts digital data bit by bit.
- Note that 1 byte (typically space occupied by 1 character) = 8 bits.

Ex. hello = 0110100001100101011011000110110001101111

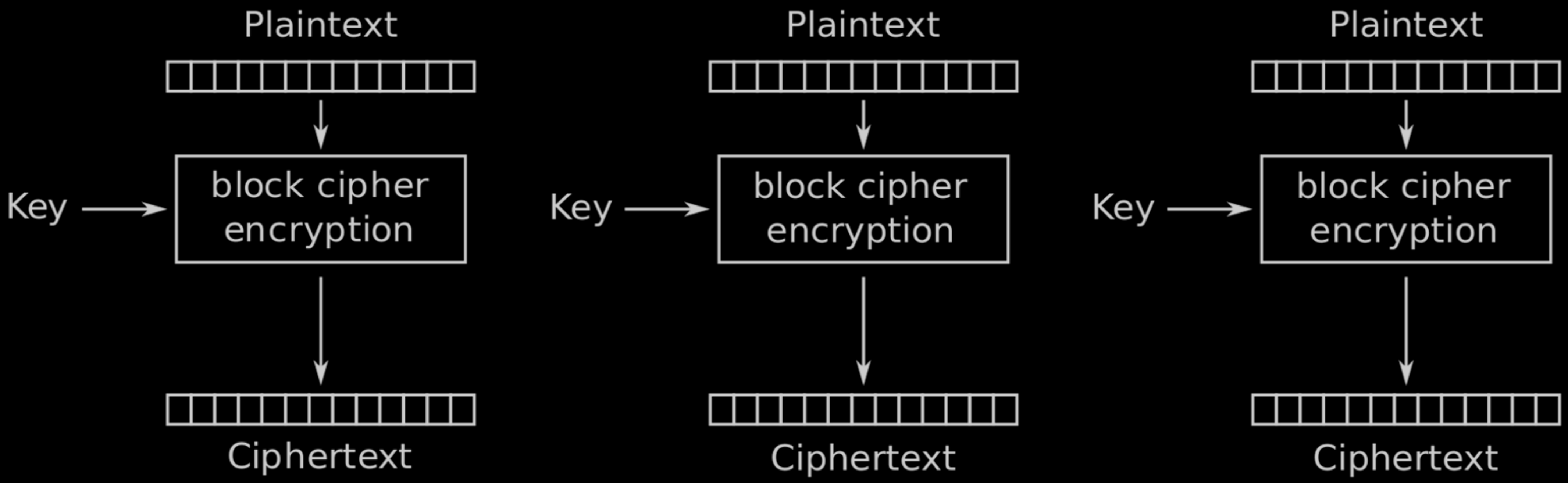
Stream Cipher


Bit stream generating algorithm
Key
Bit stream generating algorithm
Key
plaintext
⊕ XOR
ciphertext
⊕ XOR
plaintext

Block cipher

- Plain text in blocks (usually of 64 and 128 bits) and XOR operation is performed on individual blocks.
- Ex. DES (Data Encryption Standard)

Block Cipher



Substitution Cipher

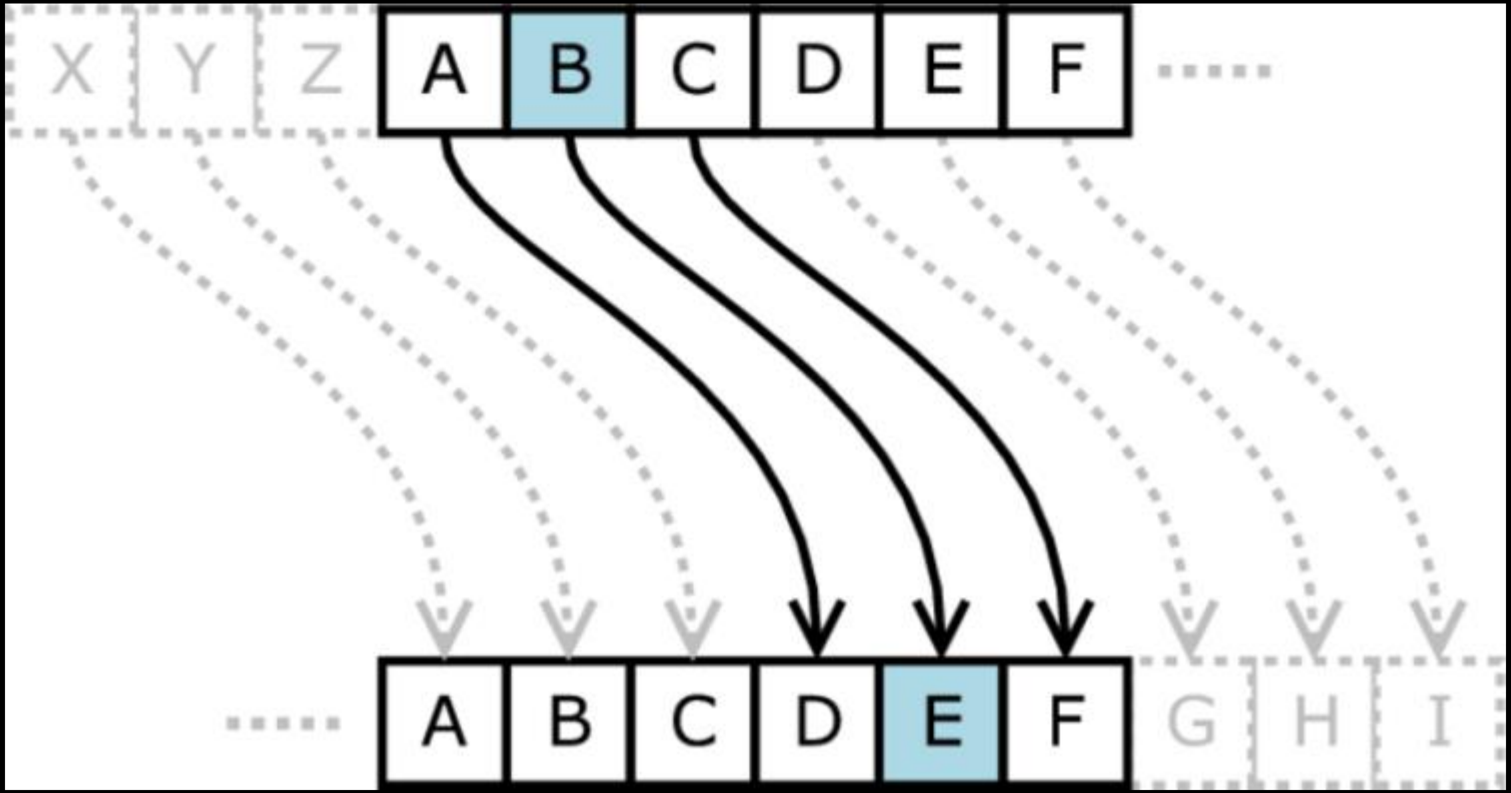
Here every letter/character is substituted by a corresponding letter/character either predetermined by the owner or varies according to the key.

Transposition Cipher

Here the plain text is just permuted according to some pre-defined rules or the key to produce the cipher text.
Ex. HELLO → LLOHE

Caesar Cipher

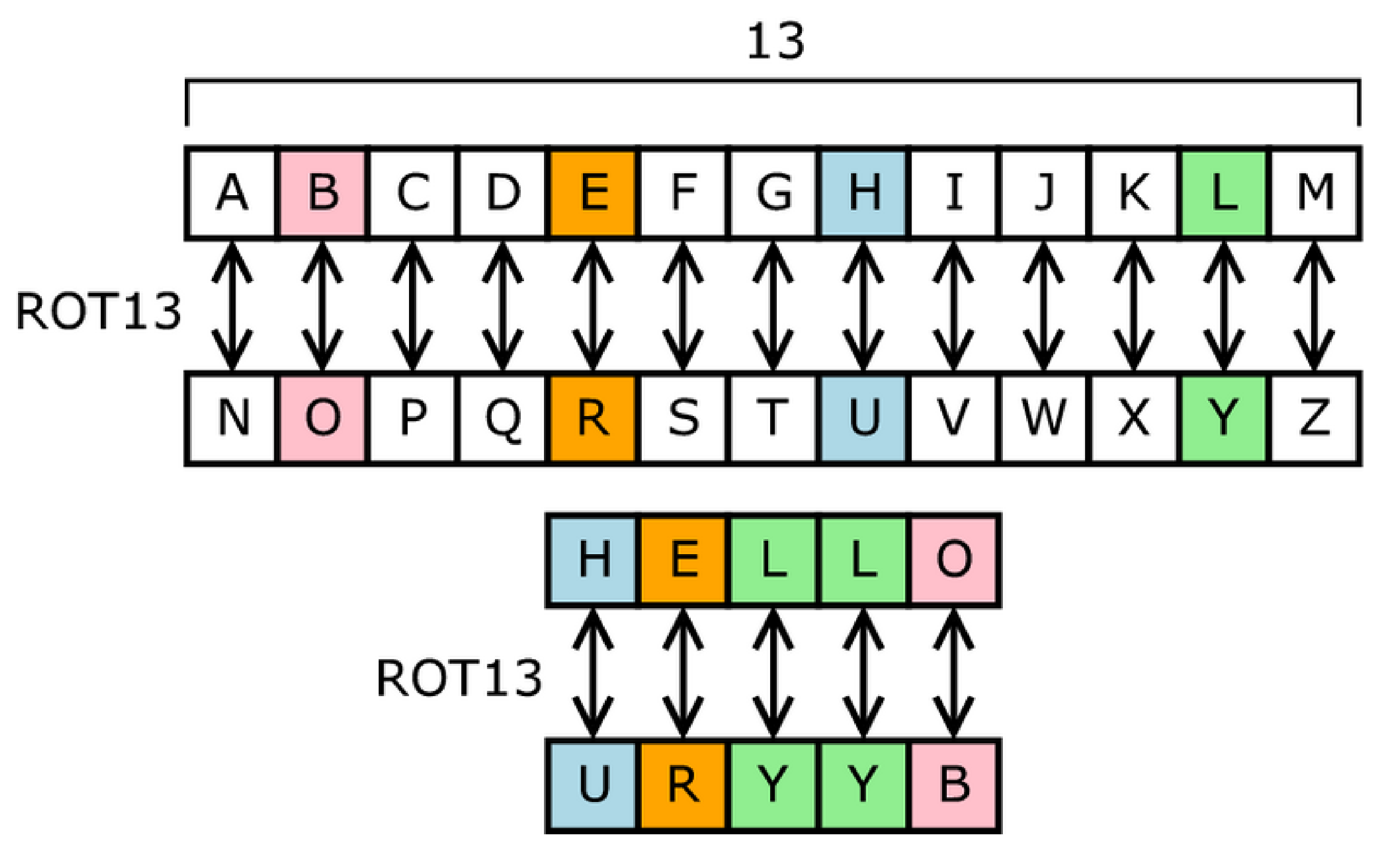
(Example of substitution cipher)



Shift = Key =3

ROT13

(Example of substitution cipher)



A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

H	E	L	L	O
U	R	Y	Y	B

Shift = 13

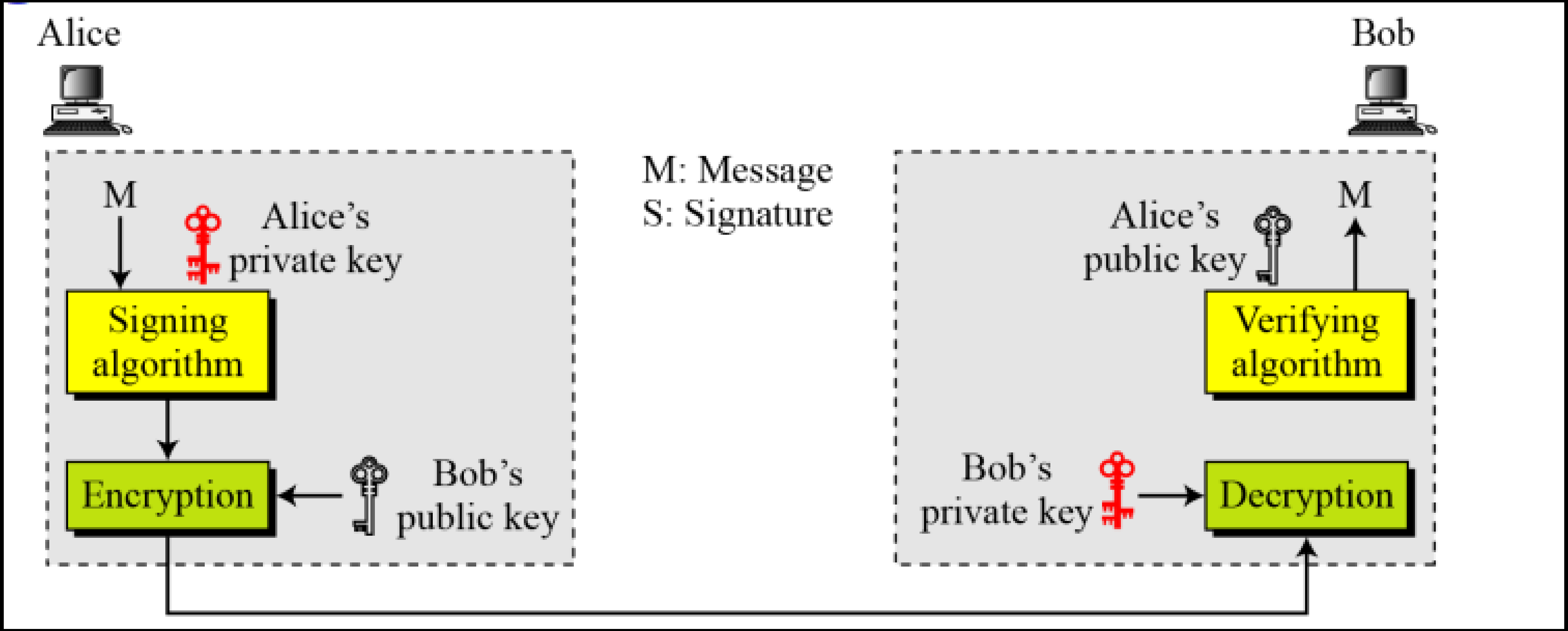
Hash Functions

- Takes in a variable size message and produce a fixed length output.
- Output is called Hash Code / Message Digest.
- Designed in such a way that a single change in input changes the entire output (the hash code).
- Hash Functions are designed to prevent Hash Collisions.
- Popular examples are MD5, SHA1, SHA128, SHA256.

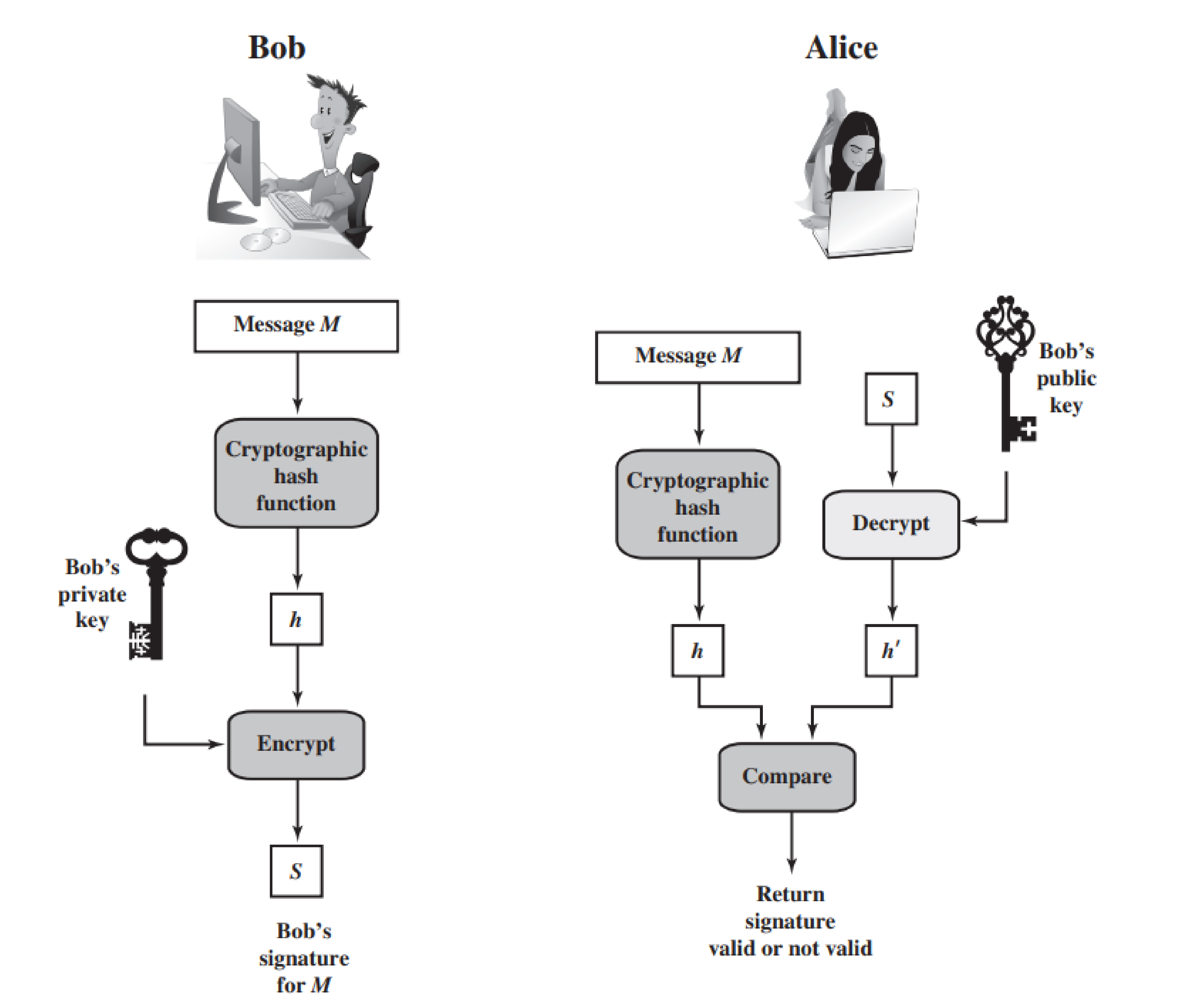
Digital Signature

- Cryptographic technique analogous to hand-written signatures.
- Sender digitally signs document, establishing that he is document owner/creator.
- It is verifiable and non-forgeable – The receiver can prove to someone that a particular sender has sent the file, and no one must have signed document
- Based on asymmetric key cryptography.
- Plays a vital role in E-Commerce, Online Transactions, etc.
- Used for authentication purposes only! Not for encryption.

How Digital Signatures work?



Verification Method



TEST YOUR LUCK LMAO ...

One of them has your code!

aHR0cHM6Ly9iaXQubHkvM1JUSU9lRQ==

QmV0dGVyIGx1Y2sgbmV4dCB0aW1lIQ==

aHR0cHM6Ly9iaXQubHkvM3pvZjVUWg==

QmV0dGVyIGx1Y2sgbmV4dCB0aW1lISAoMSk=

aHR0cHM6Ly9iaXQubHkvM3Y1dzNVRg==

QmV0dGVyIGx1Y2sgbmV4dCB0aW1lISAoMik=

SGV5eSB0aGVyZSEgY29kZSBpc24ndCBoZXJlIQ==