# Apply Cryptographic Algorithms

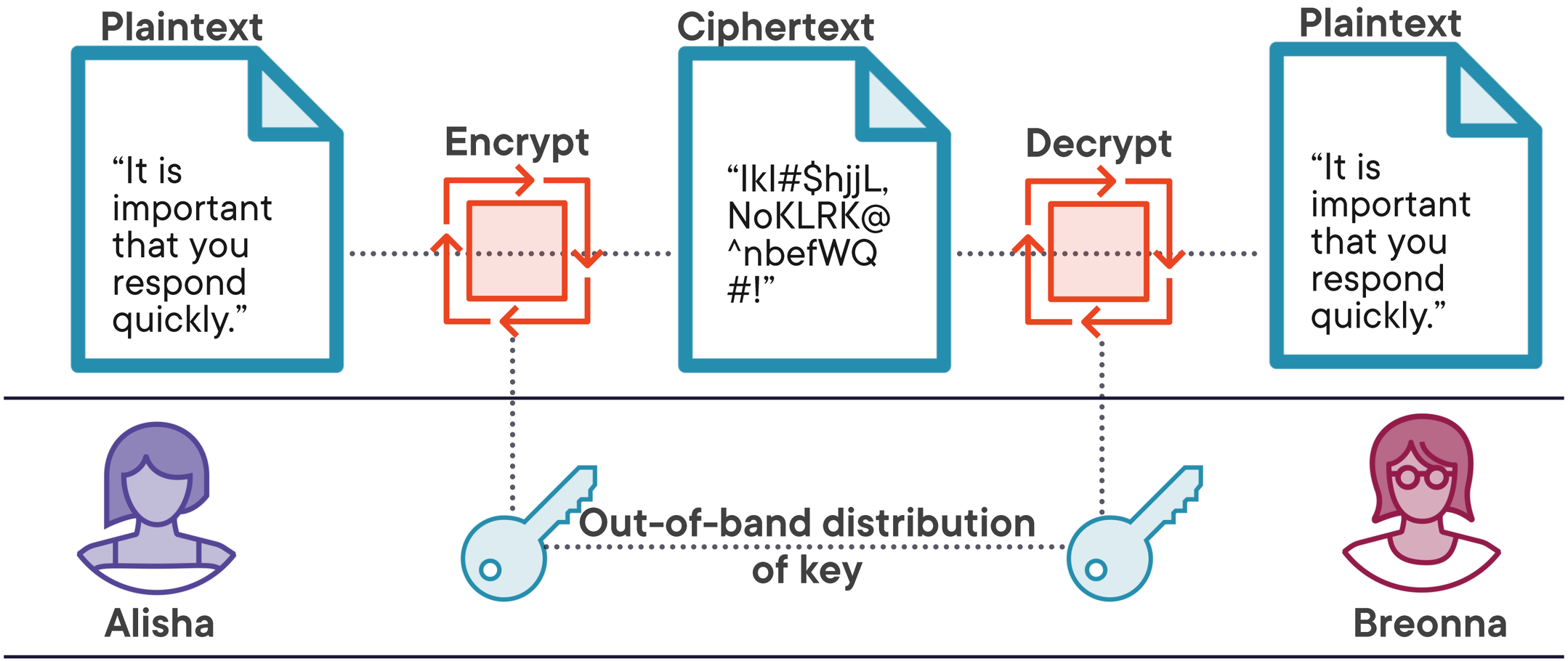
**Dr. Lyron H. Andrews**

Cryptography for SSCP®

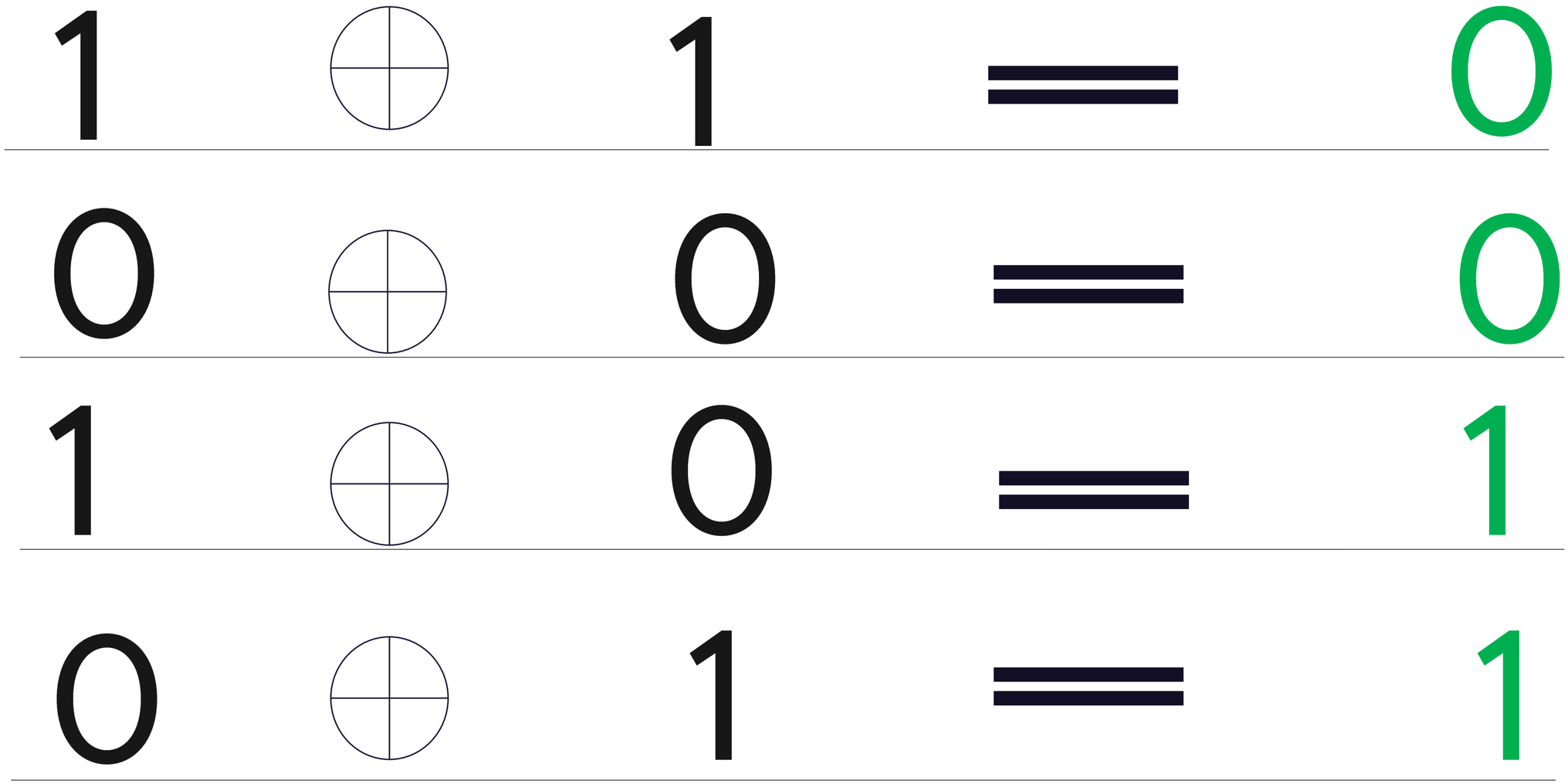
@drlyronandrews | www.profabula.com

# Symmetric Algorithms Overview

# Symmetric Key Process Flow



# Foundational Math for Symmetric Ciphers



# Symmetric Algorithms Issues

## Advantages

Excellent for confidentiality

Encryption and decryption are relatively fast

Generally patent free use without cost

Provides some level of integrity (HMAC, Keyed-hash)

## Disadvantages

Key distribution challenges

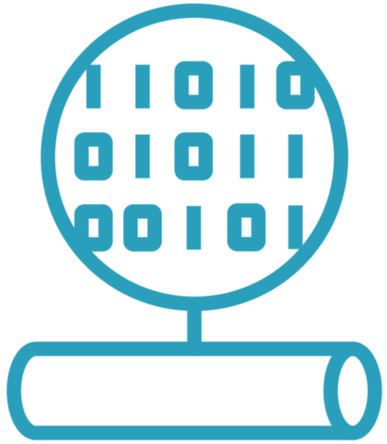
Poor authentication and no non-repudiation

# The problem with symmetric keys: n(n-1)/2

# 5,000 users = 12,497,500 keys



# Symmetric Cipher Types



**Stream-based**

Encryption operations is on a constant stream of 0s and 1s.


**Block-based**

Encryption operation is on fixed blocks of plaintext.

# Symmetric Stream-based Algorithm Types and Characteristics

# Symmetric Stream-based Algorithms Applicability and Identification

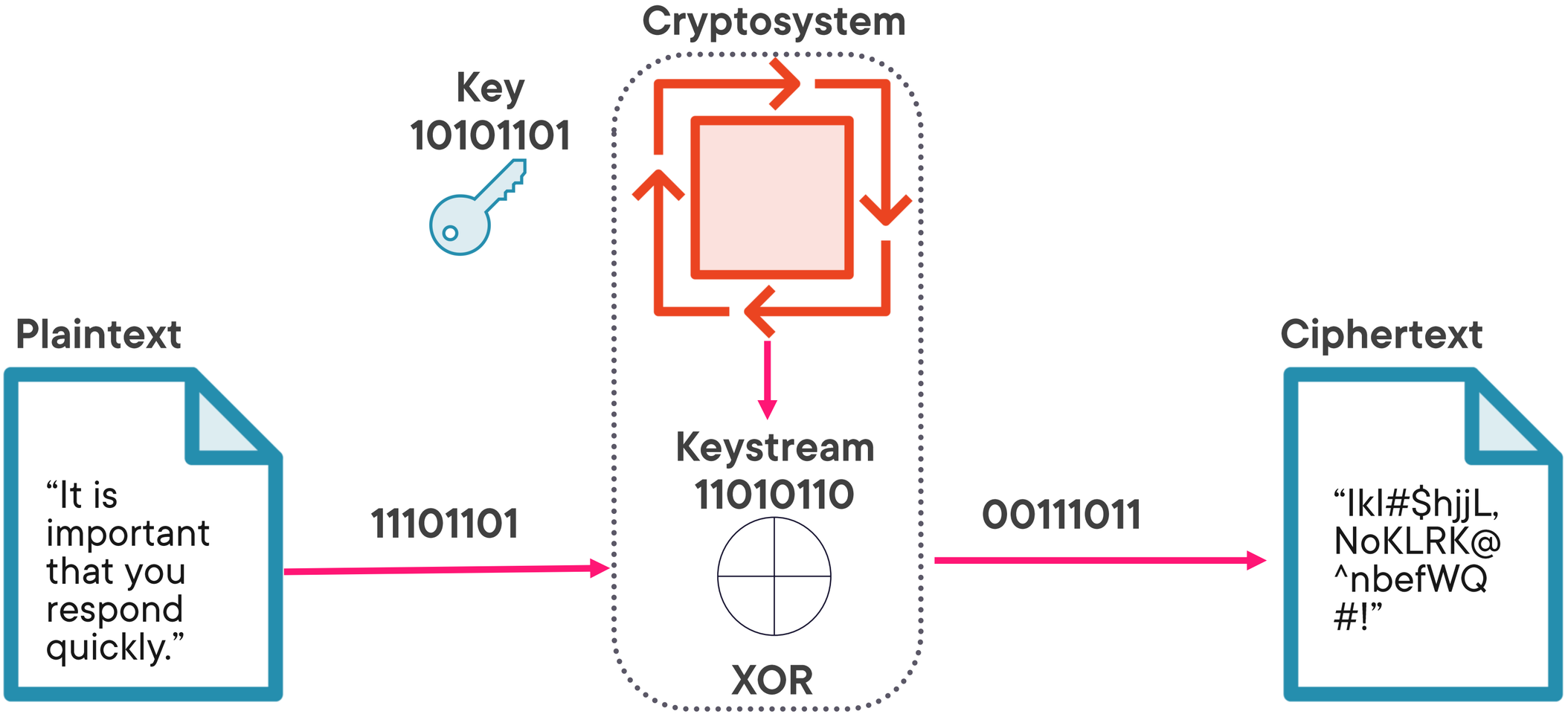
Data in transit

High-speed with minimal latency

Often embedded in hardware

Each bit or byte is encrypted

# Symmetric Stream-based Basics



RC4

SEAL

WAKE

A5

# Symmetric Stream-based Algorithms

# RC4 Characteristics

Published in 1987

Variable key length 1-256 bytes

Key initializes a state vector which generates keystream to XOR plaintext

Considered to be deprecated by NIST

# The Initial Block-based Symmetric Algorithm

# Symmetric Block-based Algorithms Applicability and Identification

Encrypts fixed plaintext data blocks of 64, 128, 192, 256 bits

Viewed as more robust than stream ciphers

May have modes that behave as stream

Horst Feistel headed up research at IBM in the 1960's that eventual led to the release of Data Encryption Standard (DES) in 1977

# Data Encryption Standard (DES)

64-bit blocks

Two 32-bit halves

56-bit key

48-bit subkeys

16 rounds of encryption

# Five Modes of DES

**Electronic Code Book (ECB)**

Block mode

**Cipher Block Chaining (CBC)**

Block mode / IV

**Cipher Feedback (CFB)**

Stream mode

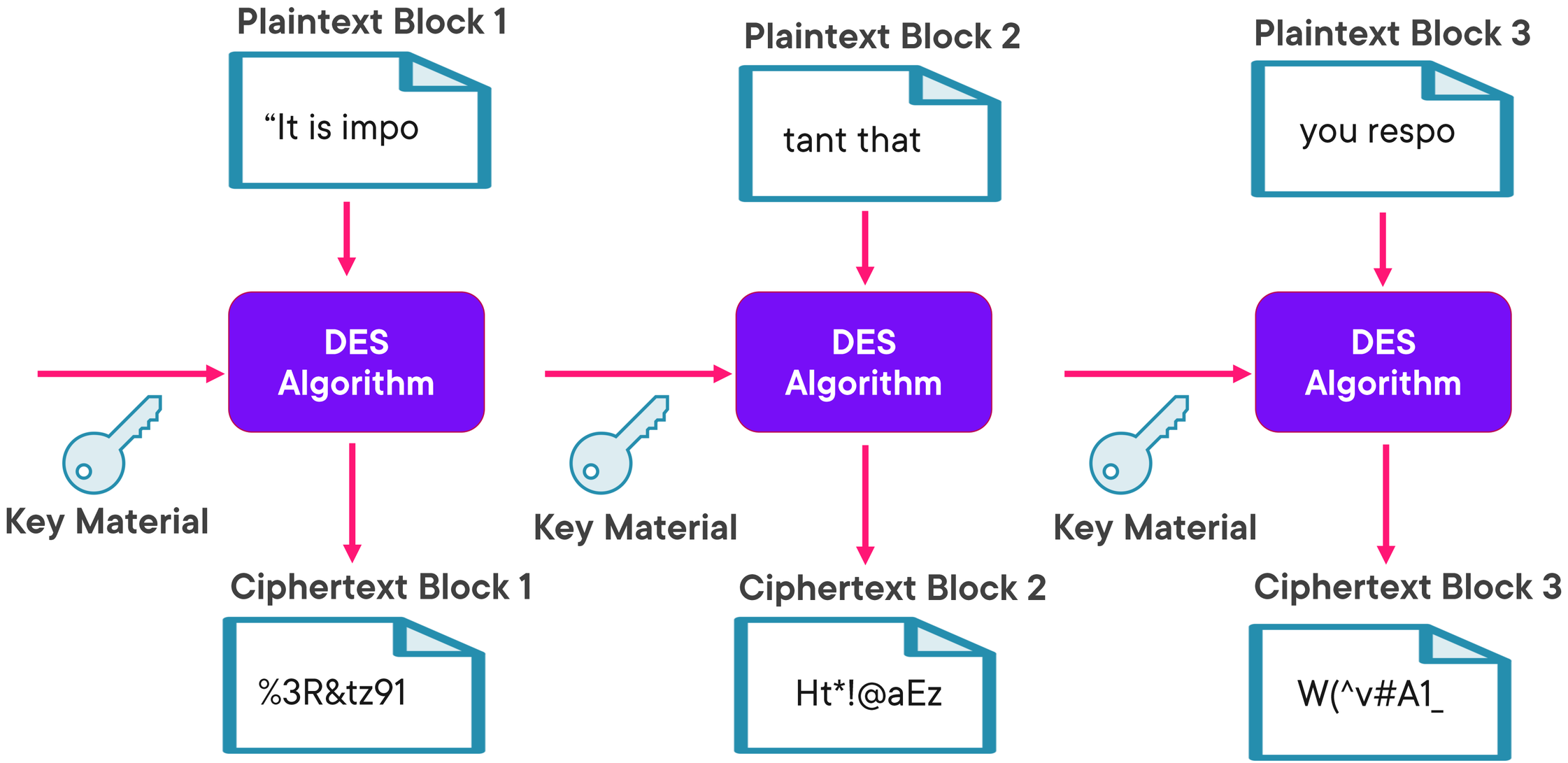
**Output Feedback (OFB)**

Stream mode

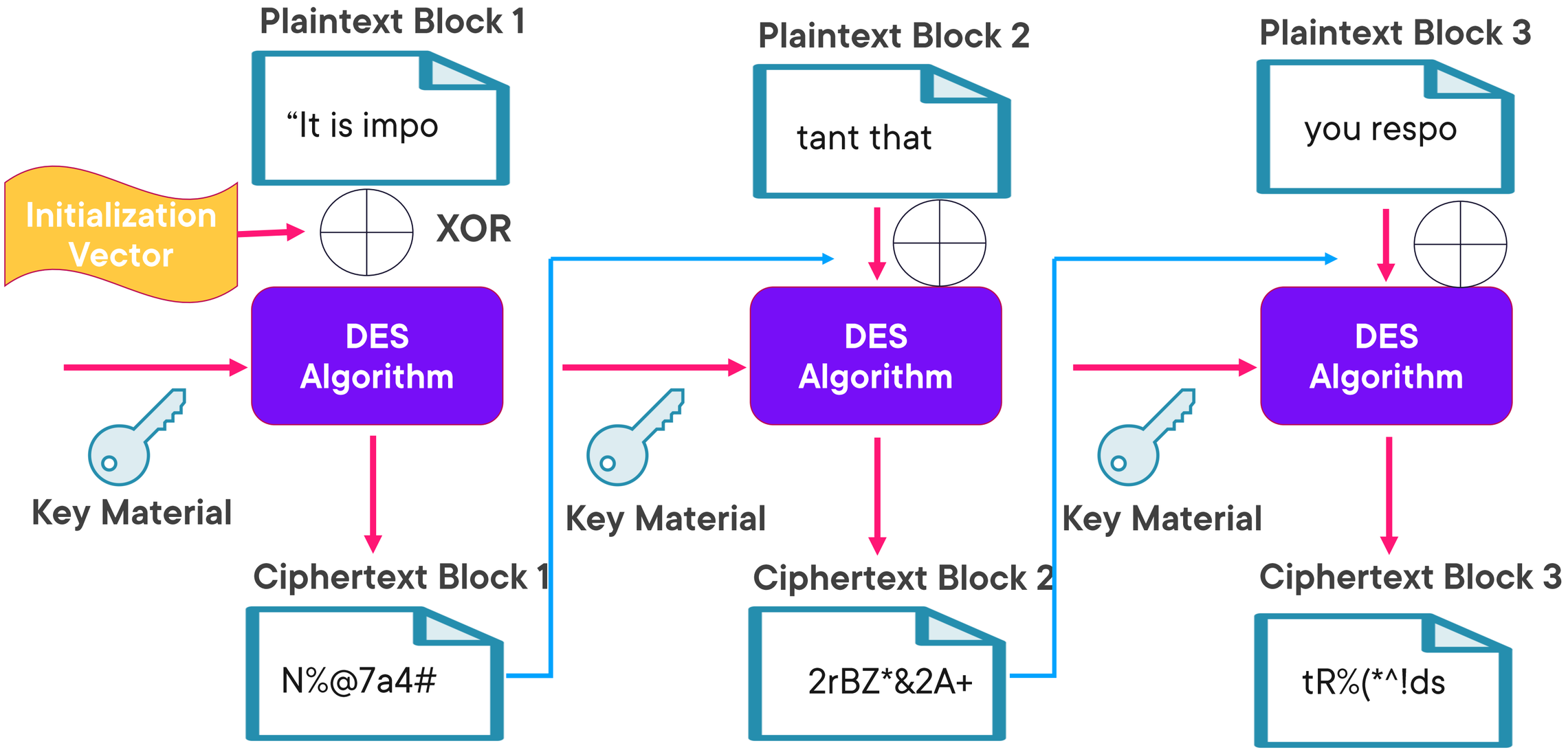
**Counter Mode (CTR)**

Stream mode

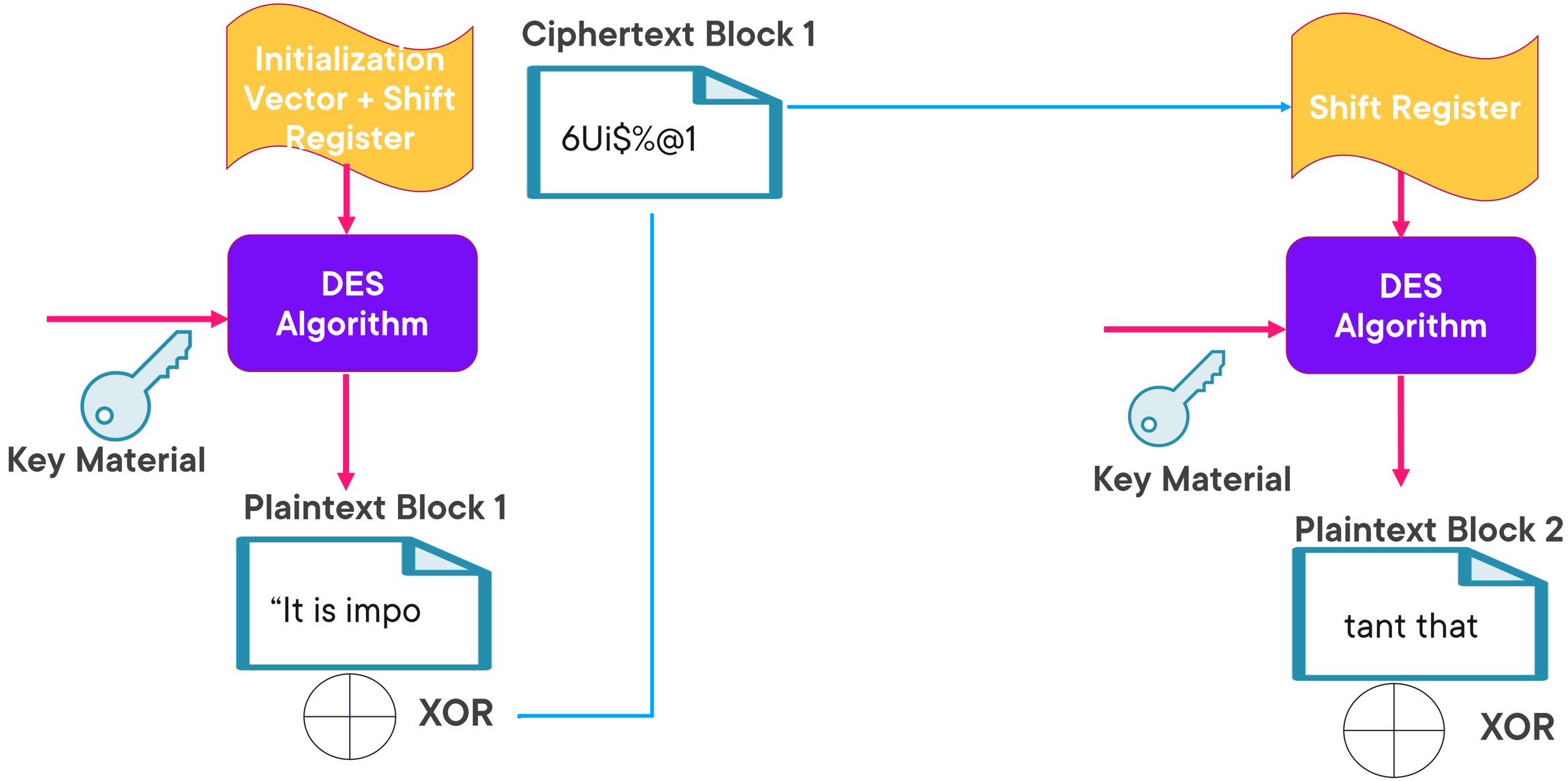
# DES Block Mode Electronic Code Book (ECB )



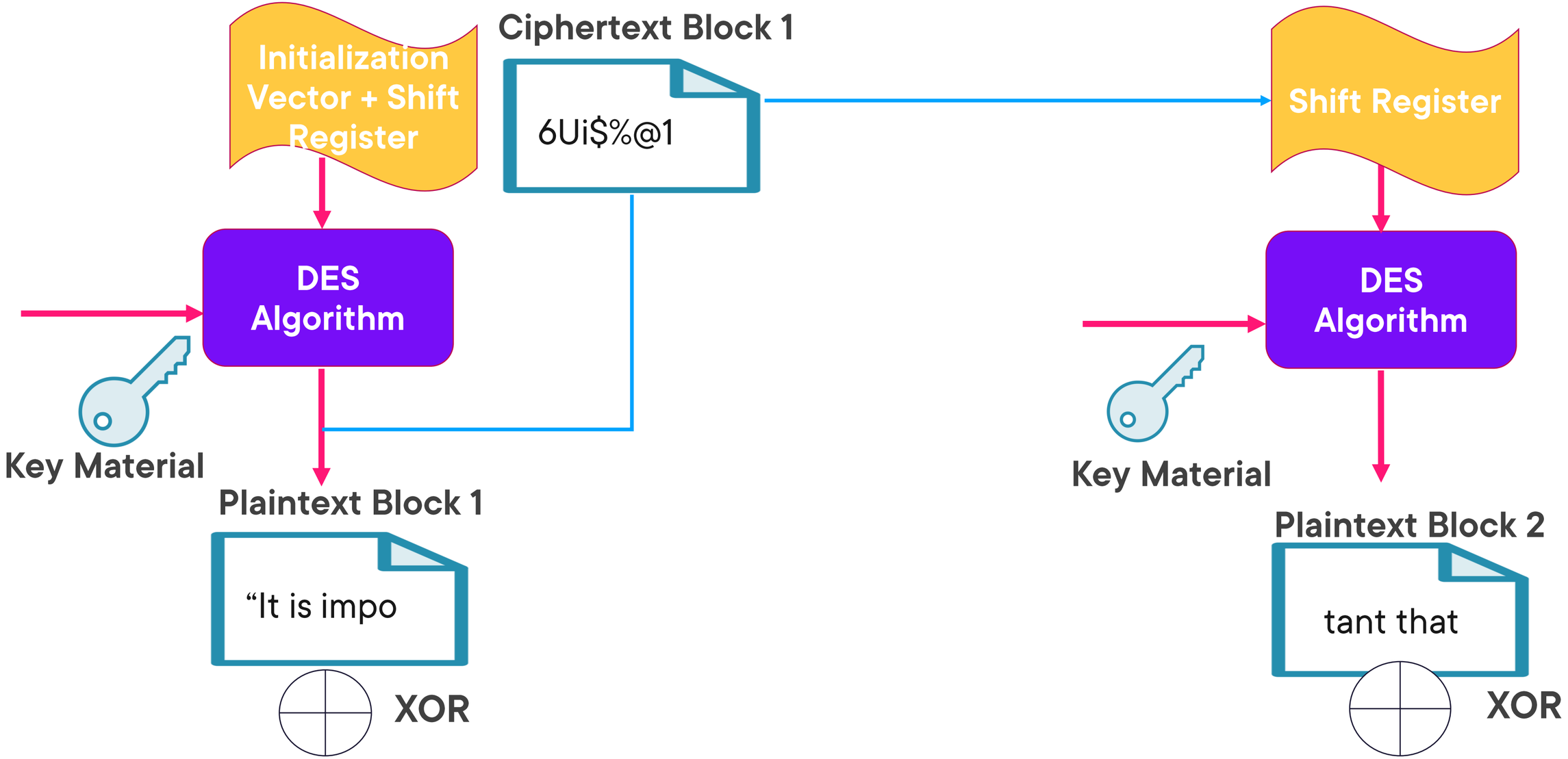
# DES Block Mode Cipher Block Chaining (CBC)



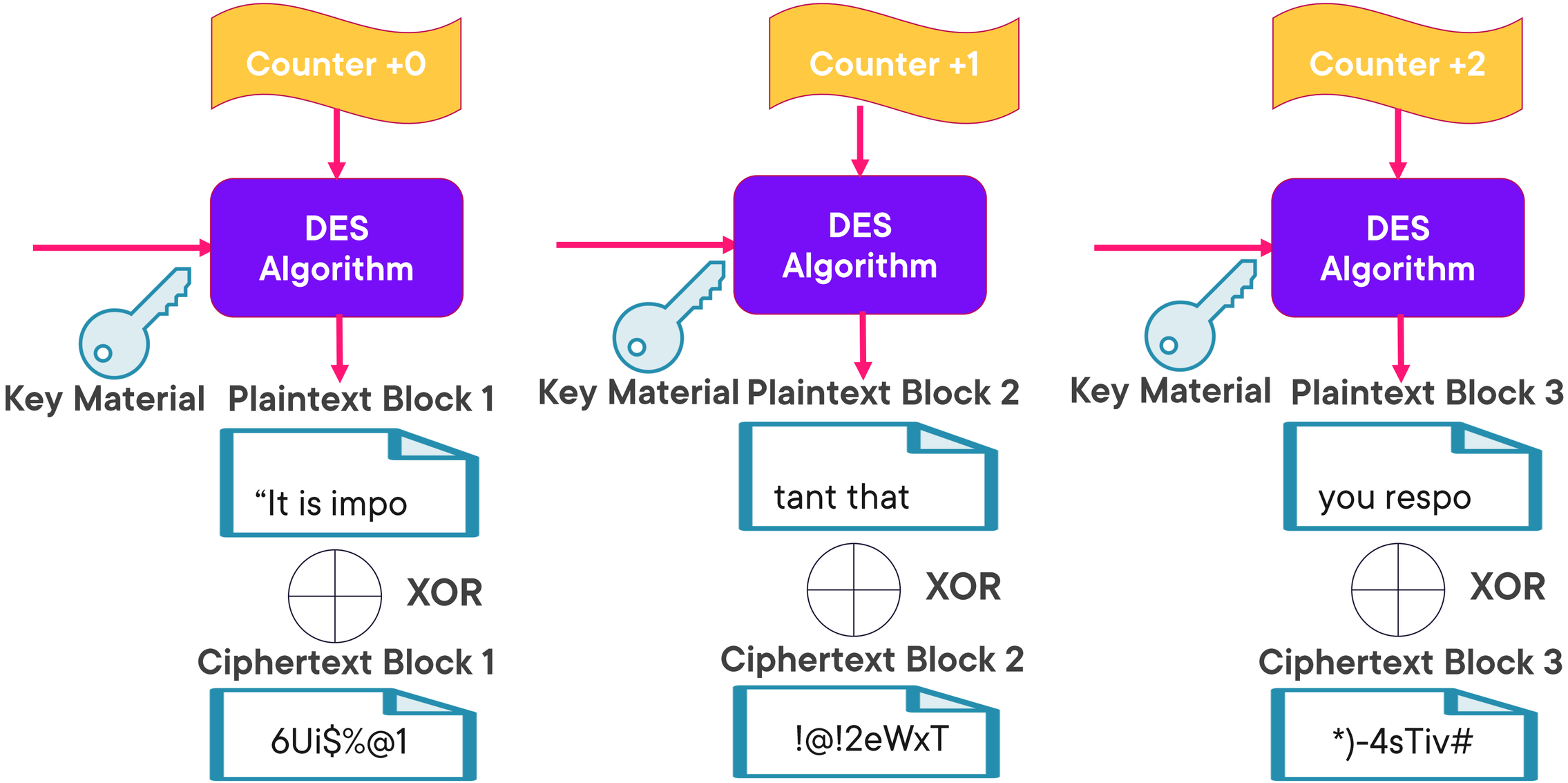
# DES Stream Mode Cipher Feedback (CFB)



# DES Stream Mode Output Feedback (OFB)



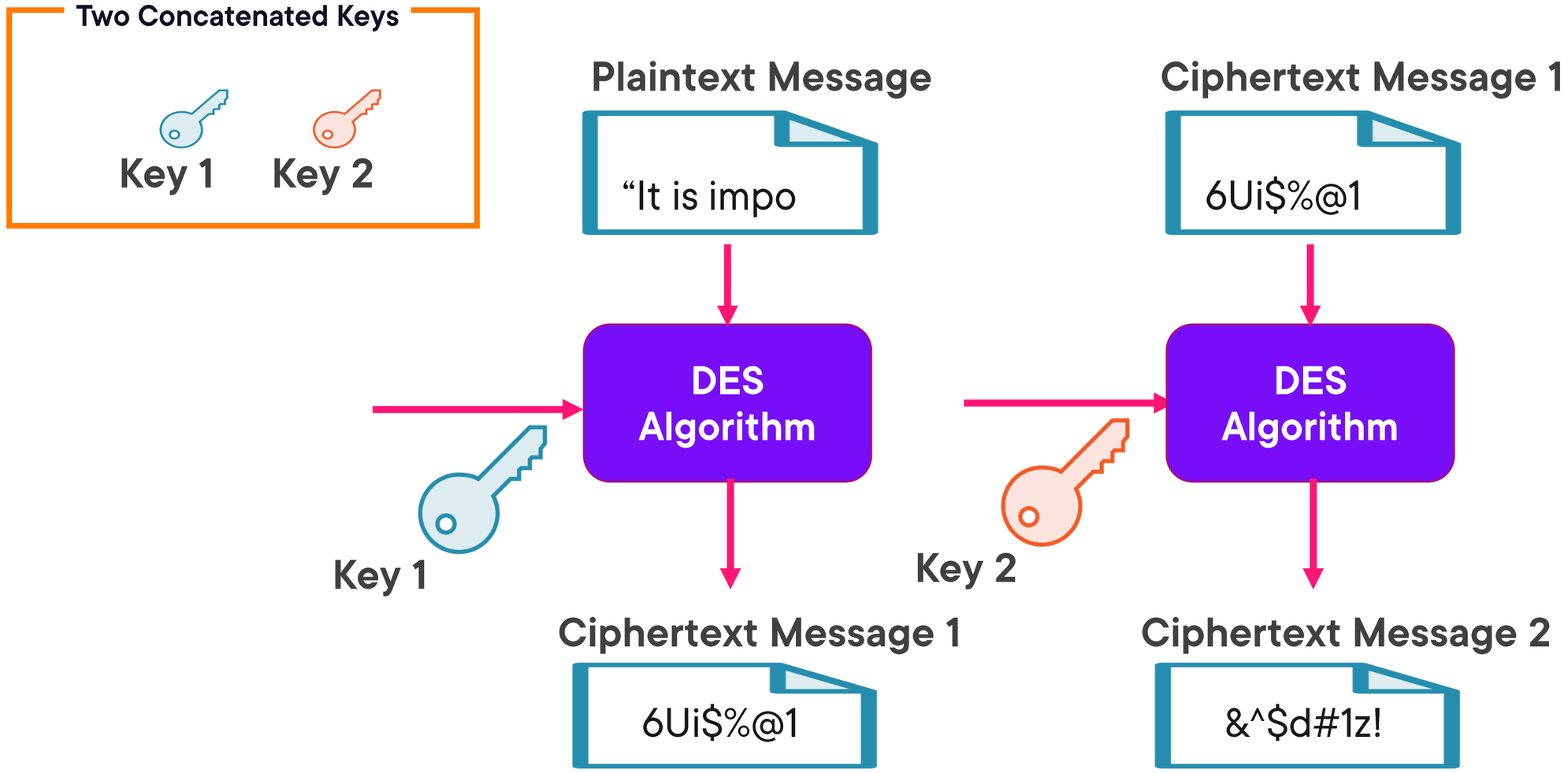
# DES Stream Mode Counter (CTR)



# Double (2DES) and Triple DES (3DES)

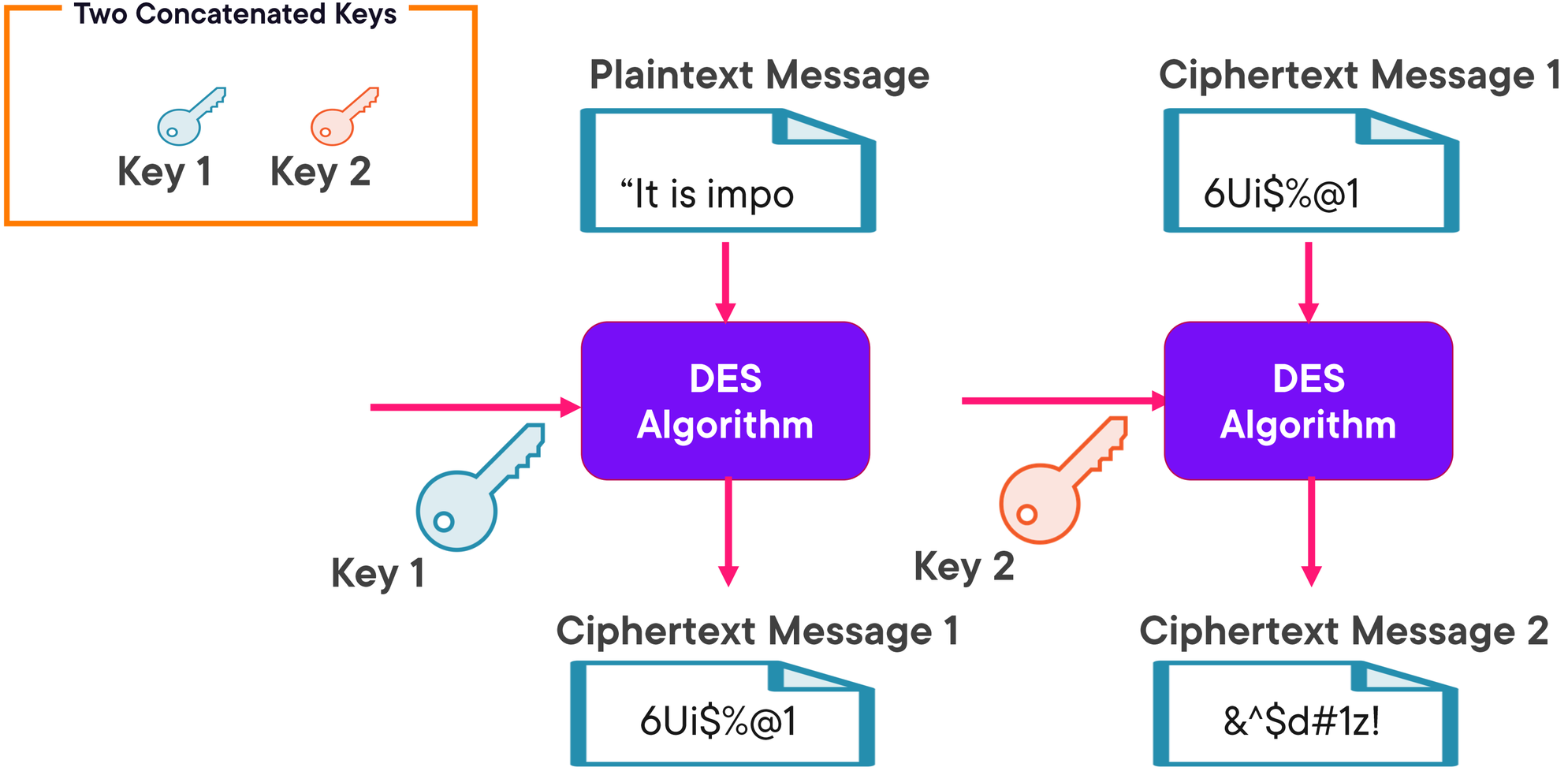
For its time DES served the purpose of confidentiality, but Moore’s Law and cryptanalytic advances exposed weaknesses.

# Double DES (2DES)

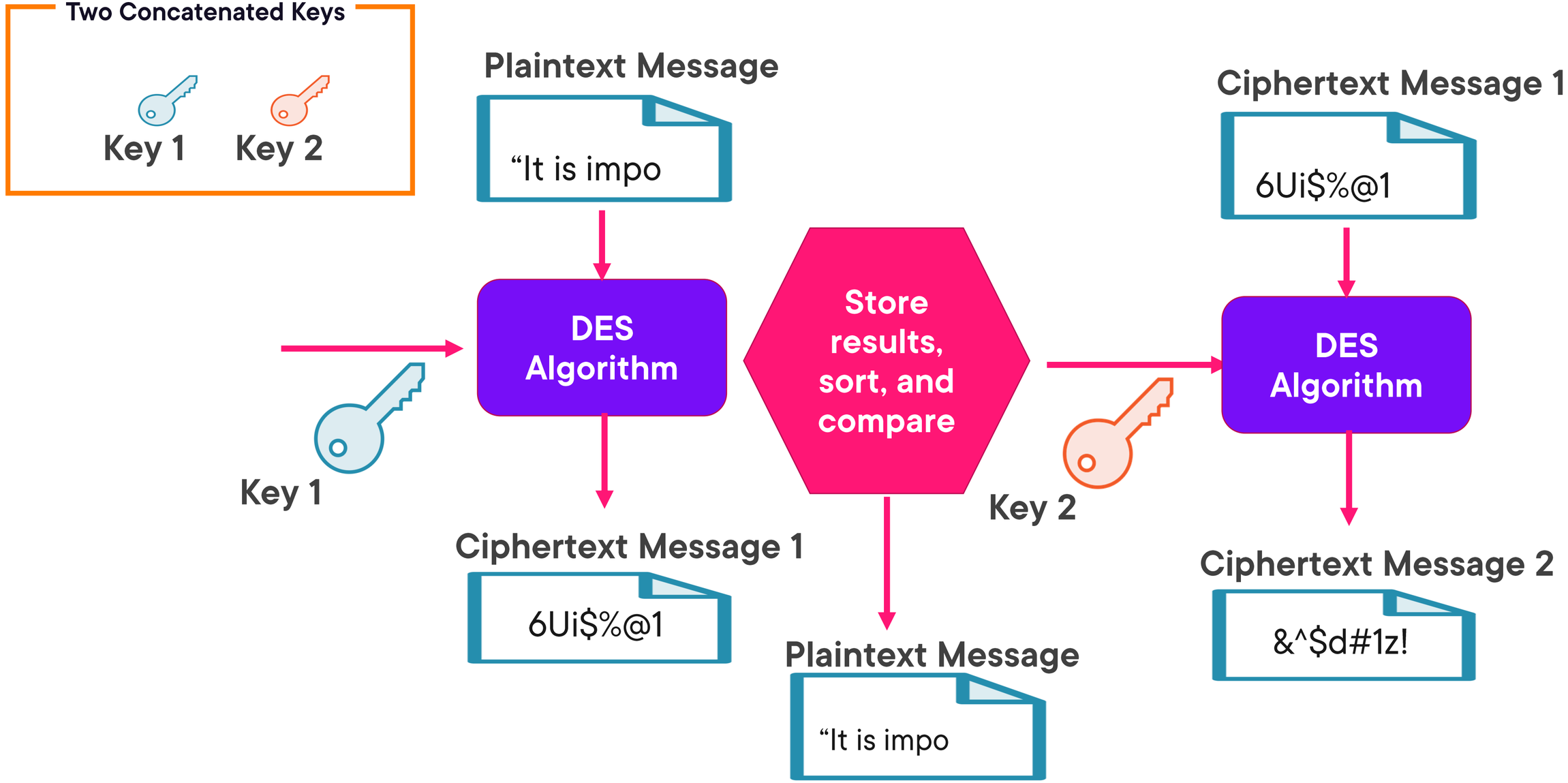


# Double DES calculates C = EK2(EK1(P))

# Meet-in-the-Middle Attack

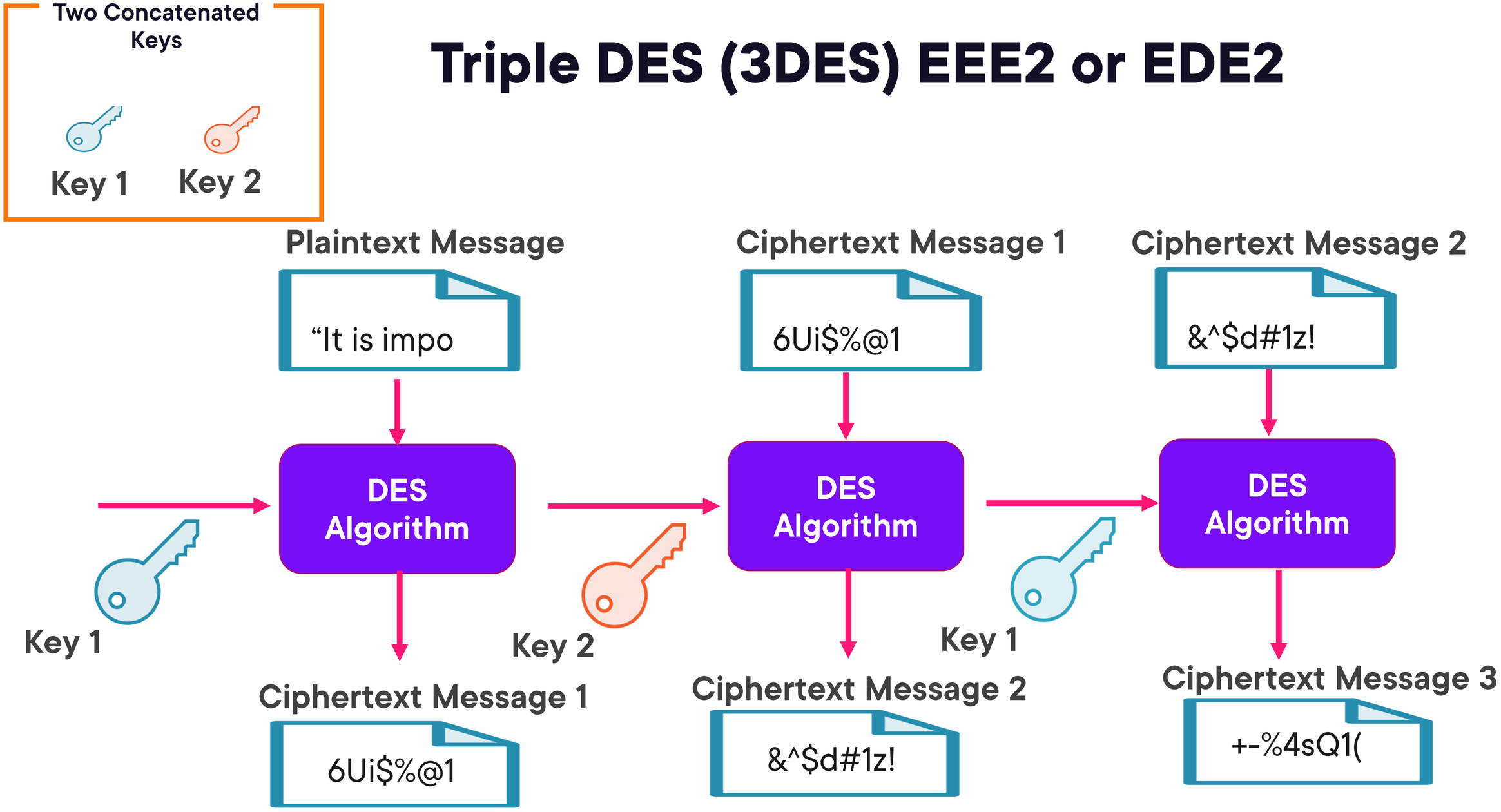


# Meet-in-the-Middle Attack

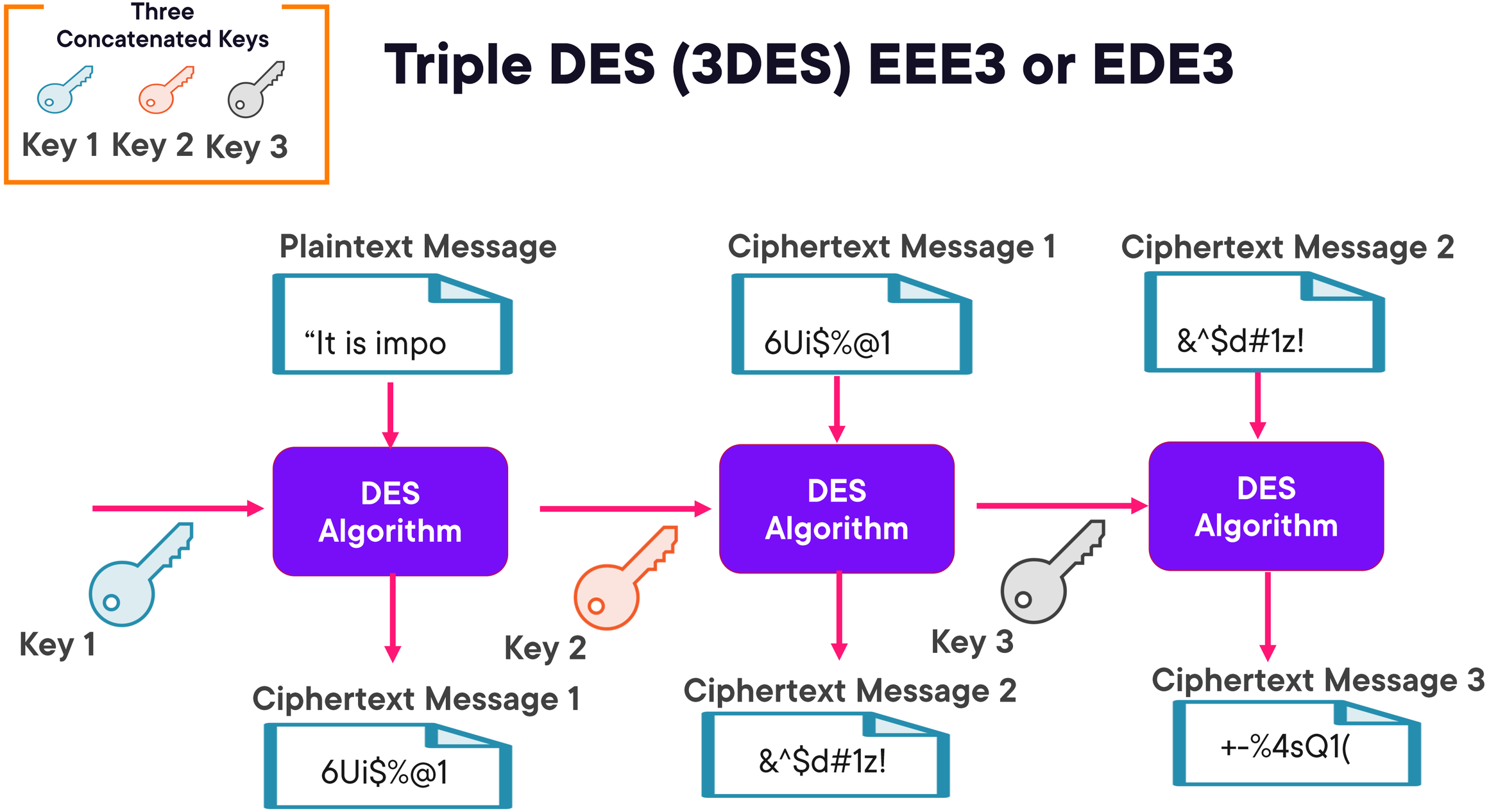


# Because of Meet-in-the-Middle Double DES $2^{112}$ only provides $2^{57}$ relative strength.

# Triple DES (3DES) EEE2 or EDE2



# Triple DES (3DES) EEE3 or EDE3



Triple DES calculates

C = EK1(EK2(EK1(P))) for the EEE2 mode

C = EK1(DK2(EK1(P))) for the EDE2 mode

C = EK3(EK2(EK1(P))) for the EEE3 mode

C = EK3(DK2(EK1(P))) for the EDE3 mode

Because of Meet-in-the-Middle Triple DES $2^{168}$ only provides $2^{112}$ relative strength.

# Symmetric Block-based Algorithm Types and Characteristics

**“Beginning in 1997, NIST worked with industry and the cryptographic community to develop an Advanced Encryption Standard (AES). The overall goal was to develop a Federal Information Processing Standard (FIPS) specifying an encryption algorithm capable of protecting sensitive government information well into the 21st century. The algorithm was expected to be used by the U.S. Government and, on a voluntary basis, by the private sector.”**

Cryptographic Standards and Guidelines – January 2021 - NIST

MARS

Serpent

RC6

Twofish

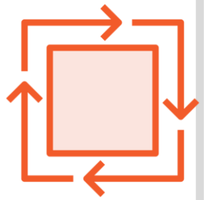
Rijndael

# Advanced Encryption Standard Contest Finalists

# MARS


Block size – 128 bits plain text

Key size – 128 to 448 bits



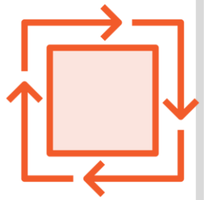
Rounds - 32

Differentiation -  MARS is not well suited for restricted-space environments due to its ROM requirement, which tends to be the highest among the finalists

# Serpent


Block size – 128 bits

Key size – 256 bits



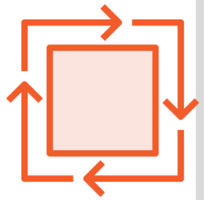
Rounds - 32

Differentiation – of finalist slowest in software fastest in hardware processing

# RC6


Block size – 128 bits

Key size – 256 bits



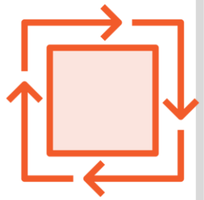
Rounds - 20

Differentiation -  block, key, and round sizes are parameterized, it therefore supports key sizes much higher than 256 bits.

# Twofish


Block size – 128 bits

Key size – 128, 192, 256 bits



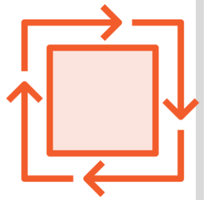
Rounds - 16

Differentiation - throughput is somewhat reduced for the larger key sizes.

# Rijndael


Block size – 128, 192, 256 bits

Key size - 128, 192, 256 bits



Rounds – 10, 12, 14

Differentiation -the key setup performance for Rijndael is consistently the fastest of all the finalists

**“NIST selected Rijndael as the proposed AES algorithm at the end of a very long and complex evaluation process. During the evaluation, NIST analyzed all public comments, papers, verbal comments at conferences, and NIST studies and reports. NIST judged Rijndael to be the best overall algorithm for the AES.”**

Report on the Development of the Advanced Encryption Standard (AES)–
May-June 2001 - NIST

# Demo

**Let’s look at a symmetric key and cryptosystem’s actions on plaintext**

- This will help to understand the application of cryptography on plaintext
- We will use CyrpTool to demonstrate confidentiality and access control

# Asymmetric Algorithms Overview

# Five Rules of Asymmetric Encryption

## Process Order

When one half of key-pair encrypts the other decrypts

## Public Key

Encryption objective is confidentiality and access control

## Private Key

Encryption objective is integrity, authenticity, and non-repudiation

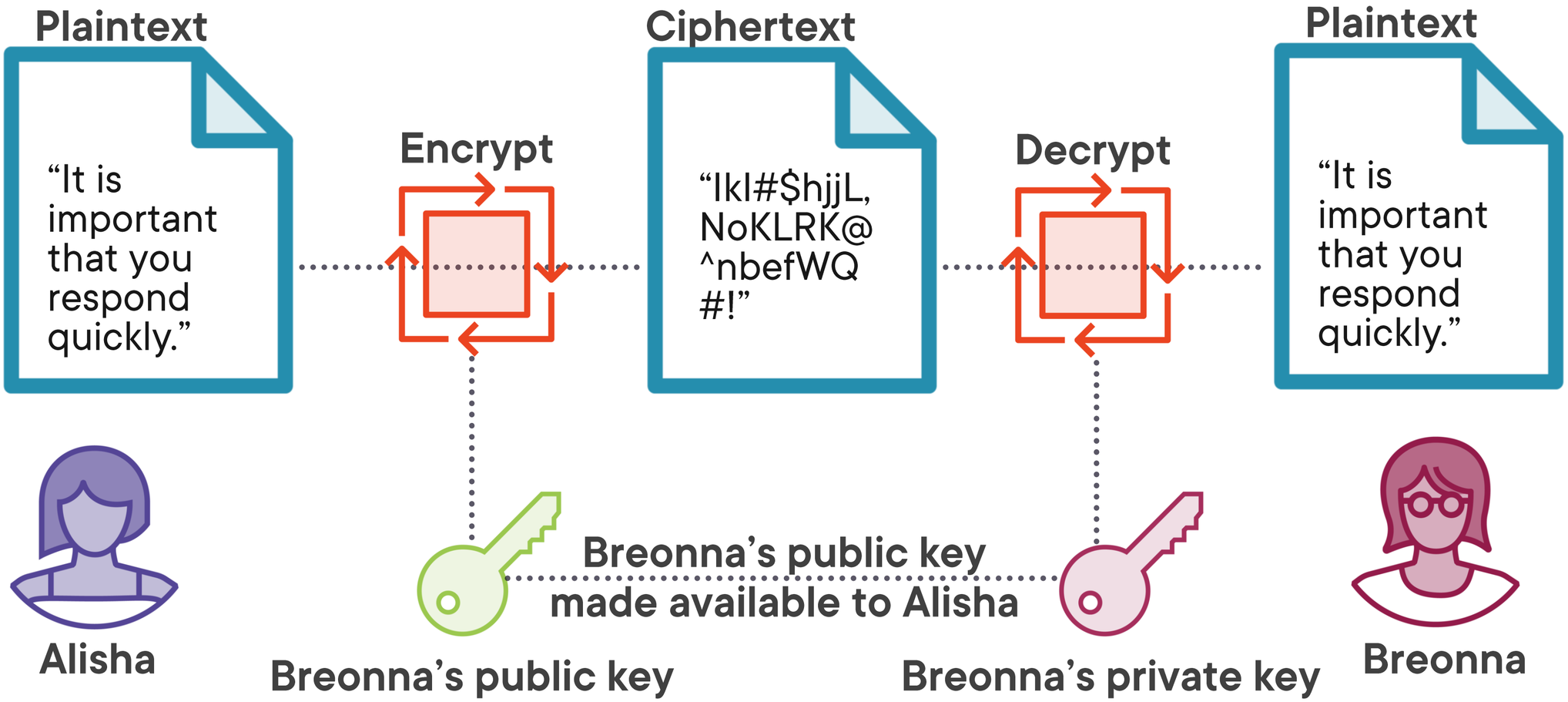
## Digital Signature

Private key (encrypting) signing a digest

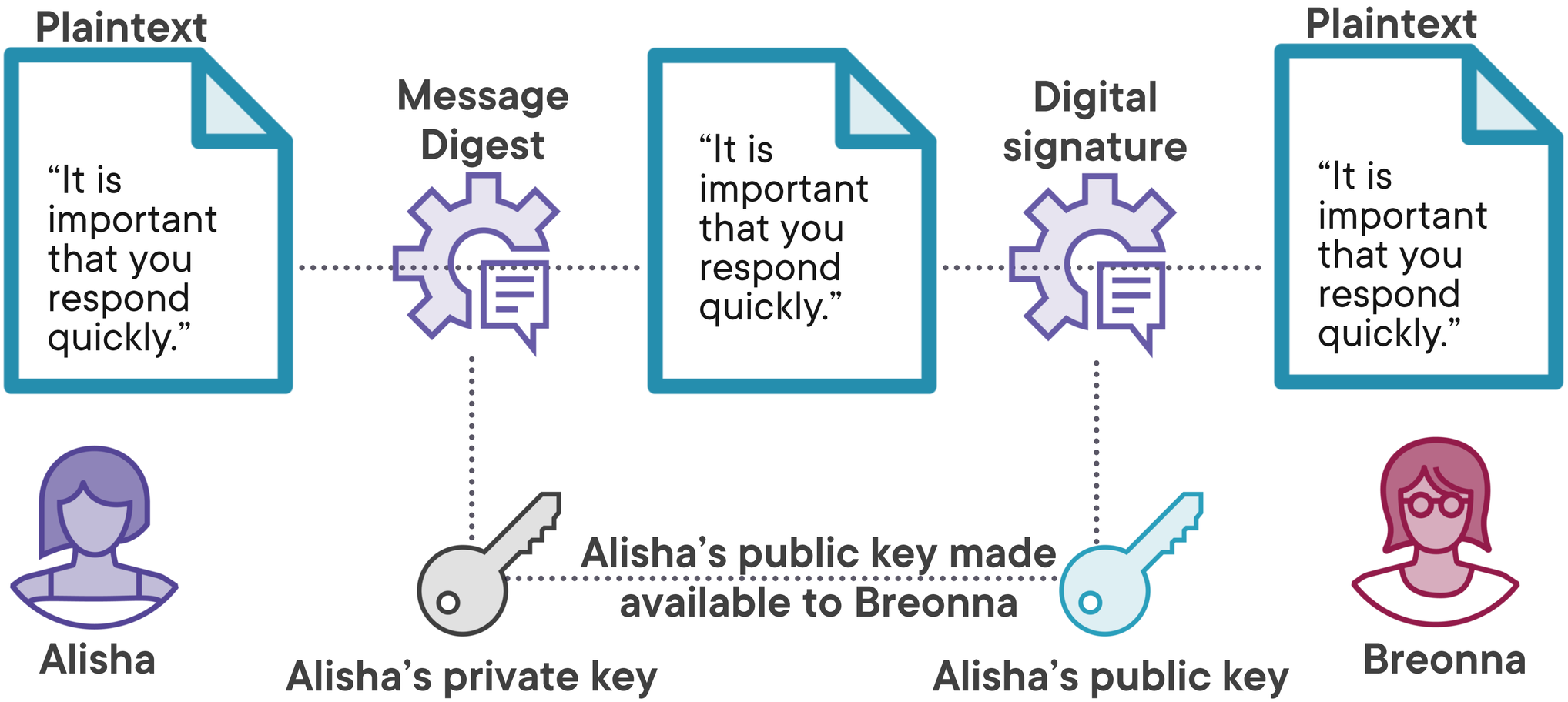
## Digital Certificate

Digital document containing DS of CA and public key of owner

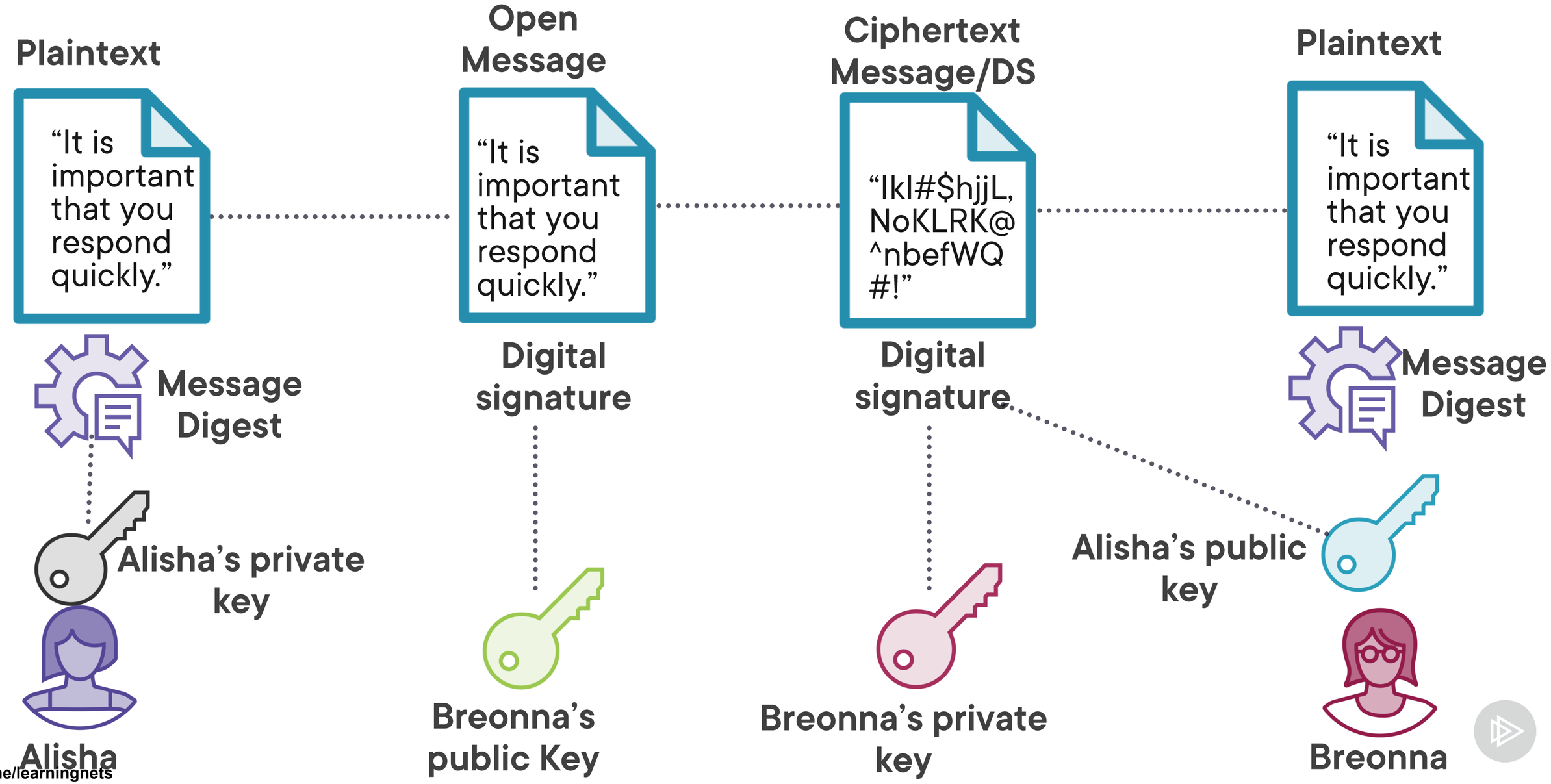
# Asymmetric Key Process Flow for Confidentiality



# Asymmetric Key Process Flow for Non-repudiation



# Asymmetric Key Process Flow for Non-repudiation and Confidentiality



# The Initial Asymmetric Algorithm

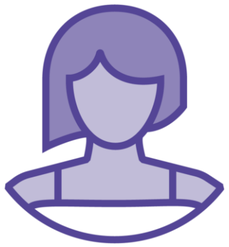
**“Public key distribution systems offer a different approach to eliminating the need for a secure key distribution channel. In such a system, two users who wish to exchange a key communicate back and forth until they arrive at a key in common. A third-party eavesdropping on this exchange must find it computationally infeasible to compute the key from the information overheard.”**

New Directions in Cryptography – November 1976 – IEEE vol IT 22
Whitfield Diffie and Martin E. Hellman

# Diffie-Hellman-Merkle Modulus Math Problem

Publicly Accessible Numbers

G=11 P=17



Alisha

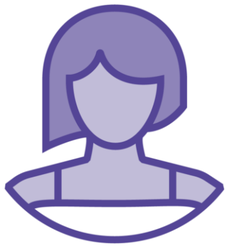
Breonna

# Diffie-Hellman-Merkle Modulus Math Problem

Publicly Accessible Numbers

G=11 P=17

G=11 P=17



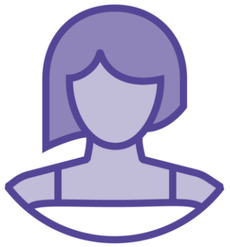
Alisha

Breonna

# Diffie-Hellman-Merkle Modulus Math Problem

Publicly Accessible Numbers

G=11 P=17



Alisha

G=11 P=17

Breonna

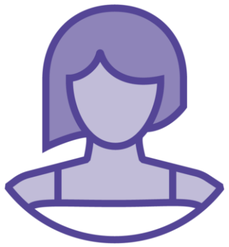
# Diffie-Hellman-Merkle Modulus Math Problem

Privately retained numbers
independently selected by each



G=11 P=17

G=11 P=17



Alisha

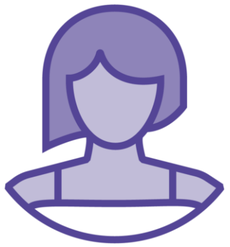
Breonna

# Diffie-Hellman-Merkle Modulus Math Problem

$11^5 \bmod 17 = 10$

5 remains a secret

G=11 P=17



Alisha

9

G=11 P=17

Breonna

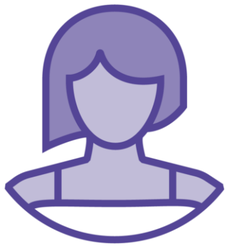
10

# Diffie-Hellman-Merkle Modulus Math Problem

$11^5 \bmod 17 = 10$

5 remains a secret

G=11 P=17



Alisha

6

$11^9 \bmod 17 = 6$

9 remains a secret

G=11 P=17

10

Breonna

# Diffie-Hellman-Merkle Modulus Math Problem

$6^5$ mod 17=7

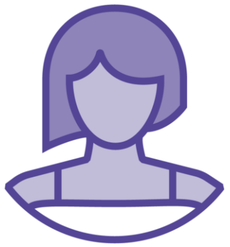
$11^5$ mod 17=

$11^9$ mod 17=

9 remains a secret

G=11 P=17

G=11 P=17



Alisha

10

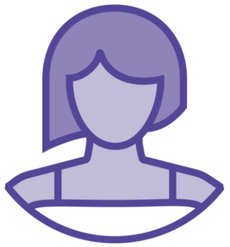
Breonna

# Diffie-Hellman-Merkle Modulus Math Problem

$6^5 \bmod 17 = 7$

$11^5 \bmod 17 =$

G=11 P=17



Alisha

$10^9 \bmod 17 = 7$

$11^9 \bmod 17 =$

G=11 P=17

Breonna

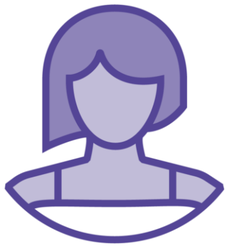
# Diffie-Hellman-Merkle Modulus Math Problem

$6^5 \bmod 17 = 7$ → Shared-secret is 7 ← $10^9 \bmod 17 = 7$

$11^5 \bmod 17 =$

$11^9 \bmod 17 =$

G=11 P=17



Alisha

G=11 P=17

Breonna

# Asymmetric Algorithm Types and Characteristics

# Diffie-Hellman-Merkle

Primary function – negotiation “exchange” of symmetric keys

Primary mathematics – discrete logarithms over finite fields

Distinguishing characteristic – first commercially viable asymmetric algorithm

# RSA

Primary function – session keys, digital signatures, and message confidentiality

Primary mathematics – factoring the product of two large prime numbers

Distinguishing characteristic – most widely used asymmetric algorithm in history

# ElGamal

Primary function –session keys, digital signatures, and message confidentiality

Primary mathematics – discrete logarithms over finite fields

Distinguishing characteristic – used concepts of Diffie-Hellman-Merkle for key distribution while introducing digital signature scheme

# Elliptic Curve Cryptography (ECC)

Primary function –session keys, digital signatures, and message confidentiality


Primary mathematics – algebraic structure of elliptic curves over finite fields

Distinguishing characteristic – shorter key lengths uses less computational power

# ECC vs. RSA

| ECC Key length (bits) | RSA Key length (bits) |
|---|---|
| 160 | 1024 |
| 224 | 2048 |
| 256 | 3072 |
| 384 | 7680 |
| 512 | 15360 |

# Asymmetric cryptography is too slow.



# Demo

**Let’s generate a private/public key pair**

- This will allow confidential protection of host device connecting remotely and non-repudiation
- We will use CLI feature of SSH from a command prompt

# Hashing Algorithms Overview

# System Integrity Codes

Parity bits

Checksums

Cyclic Redundancy Checks (CRC)

Message authentication codes (MAC and HMAC)

Hashing

# Hashing Primitives

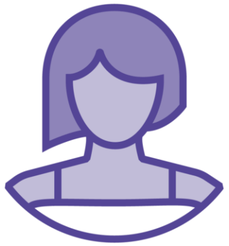
Easy to compute the hash value for a message

Infeasible to generate a message given hash

Infeasible to modify a message without changing hash

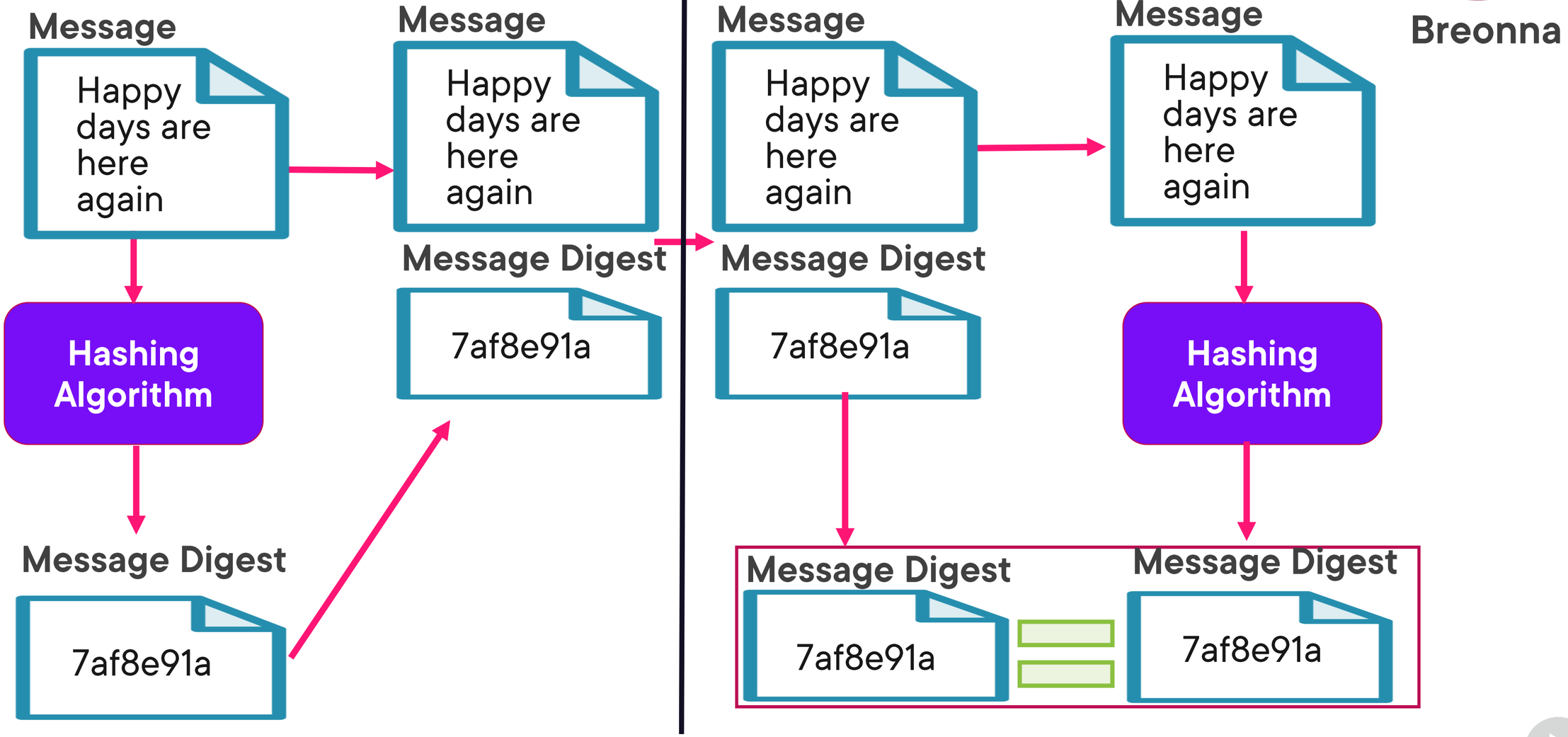
Difficult to find two different messages with the same hash

# Hash Operation

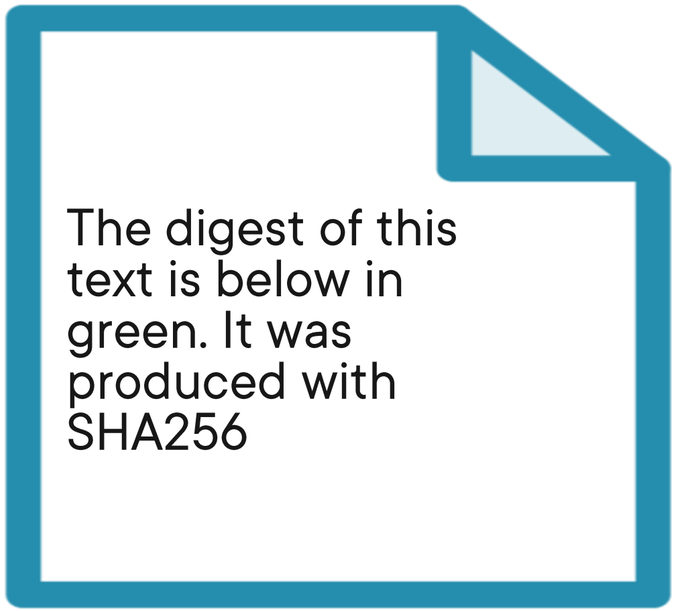


Alisha

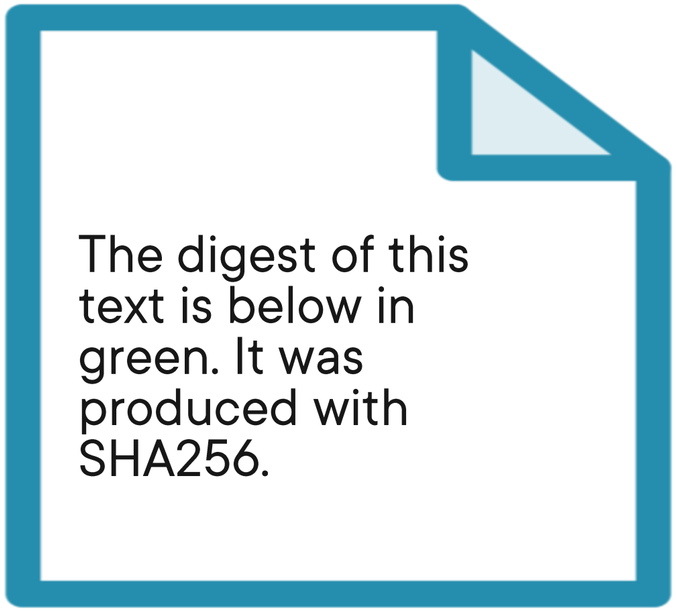
Breonna



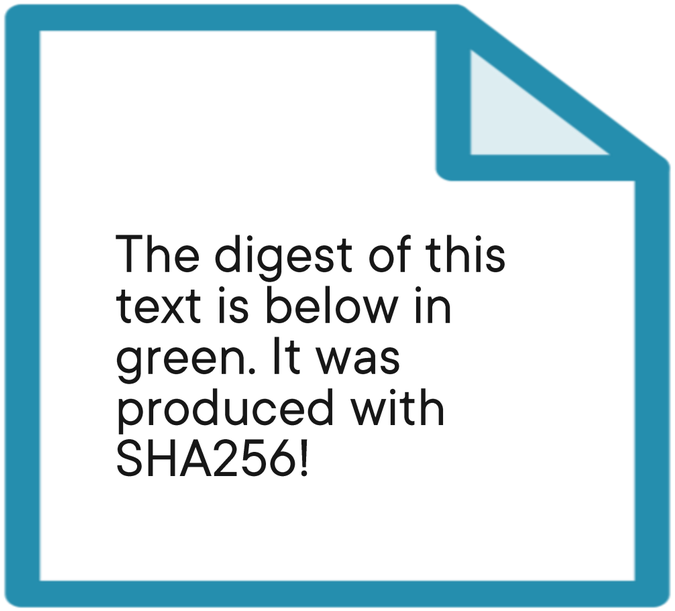
# Digest Sensitivity to Change




a8cd0052dc0da24
9082747c83bf5ac2
9d7246f648b1981c2
c91e0e7a0d0eba77




a686c6b46079323e
41e7e18555b0a3d4
d47b6d26016d11df2
097c83915312e69




d623ae37719173936
cc788dc325863774
adb5d1822be8d4ab
4cdd354971bb0b0

# Hashing Algorithm Types and Characteristics

MD2

MD4

MD5

# Message Digest (MD)

SHA-0

SHA-1

SHA-2

SHA-3

# Secure Hash Algorithm (SHA)

# Additional Hash Algorithms

## HAVAL

128-bit block, variable-bit digest

## RIPEMD-160

512-bit block, 160-bit digest

Up Next:

# Up Next:
# Secure Protocols and Cryptographic Lifecycles