Encryption Terminology and Mandated Requirements

Dr. Lyron H. Andrews
ISO/IEC AIMS Lead Implementor
CISSP/CCSP/SSCP/CRISC/CISM/CCSK/CCZT
@drlyronandrews | www.profabula.com

Overview

Overview

- Define the basic terms of cryptology
- Understand cryptography within historical contexts
- Use the correct cryptographic key for a specific business requirement

SSCP Certification Examination

Domains	Weights
Security Concepts and Practices	16%
Access Controls	15%
Risk Identification, Monitoring, and Analysis	15%
Incident Response and Recovery	14%
Cryptography	9%
Network and Communication Security	16%
Systems and Application Security	15%

SSCP Certification Examination

Domains	Weights
Security Concepts and Practices	16%
Access Controls	15%
Risk Identification, Monitoring, and Analysis	15%
Incident Response and Recovery	14%
Cryptography	9%
Network and Communication Security	16%
Systems and Application Security	15%

Defining Terms Related to Cryptology

Cryptology

The study of codes, or the art of writing and solving them.

Citation: Oxford Languages

Cryptology Subsets

Cryptography

Secret writing

Cryptanalysis

Activities to defeat secret writing

Basic Cryptography Terms

Encrypt/Encipher

Message converted to ciphertext/cryptogram

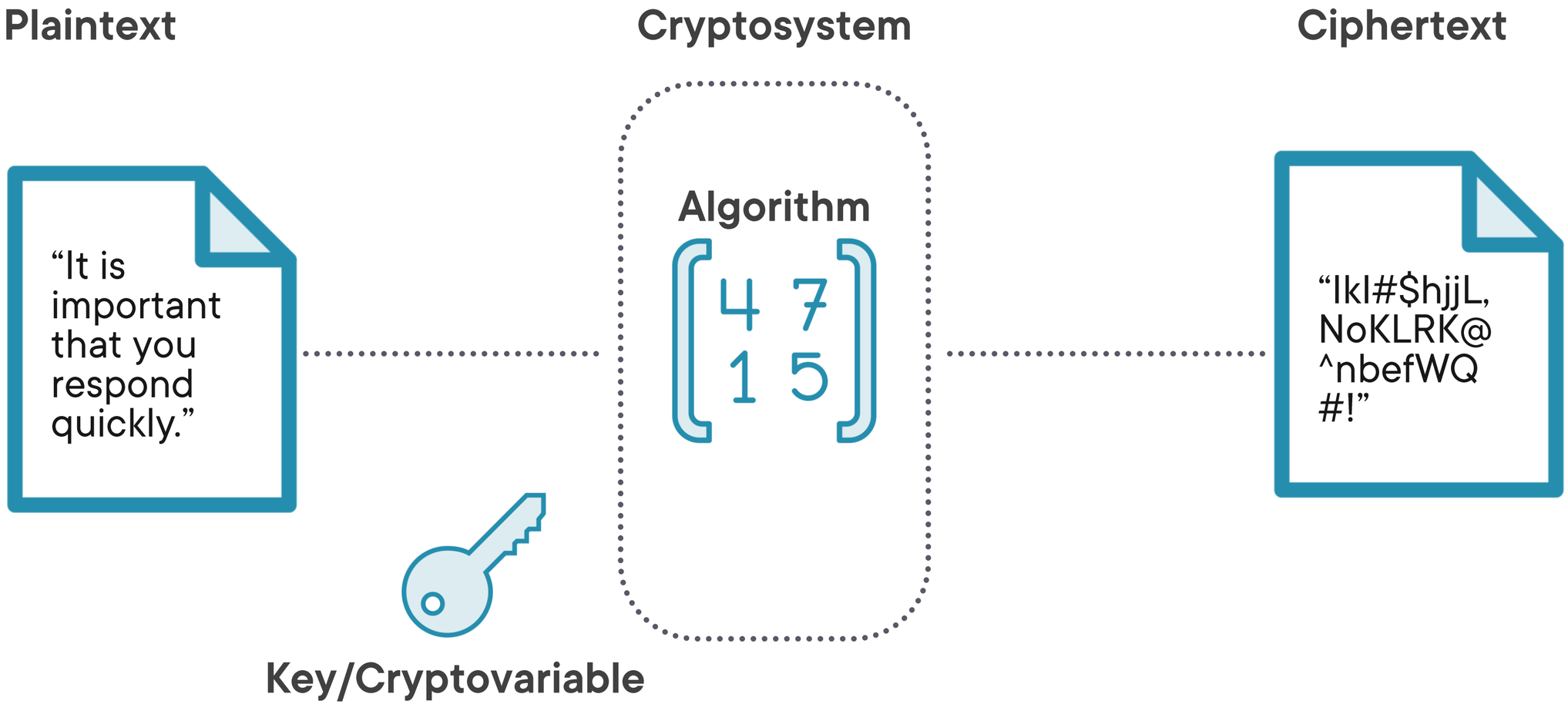
Decrypt/Decipher

Reverting ciphertext to plaintext

Plaintext/Cleartext

The message in original readable form

Basic Cryptography Action



Work Factor Implications

Key space

Length of cryptovariable

Avalanche effect

Minor change causes major effect

Initialization Vector

Plaintext additive before encrypting

Confusion

Substitution of values

Diffusion

Transposition of values

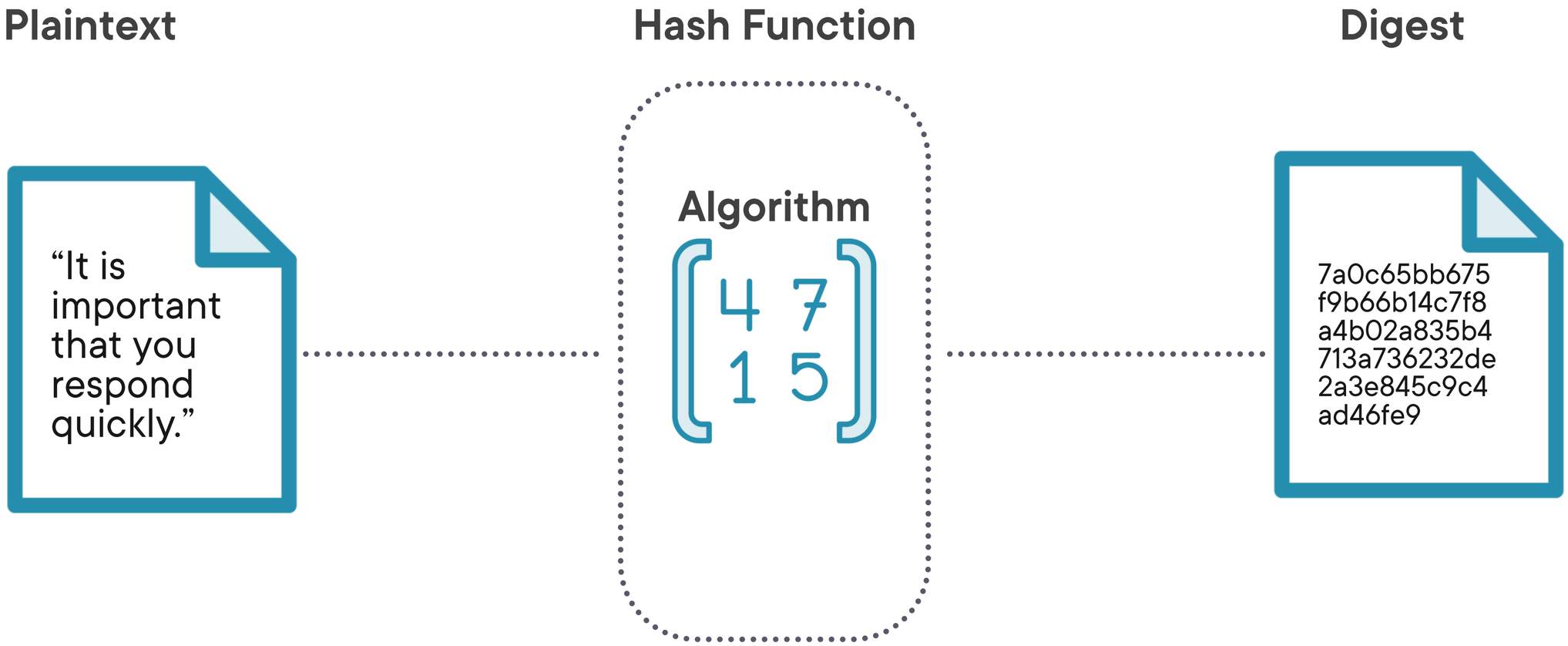
Sample Cryptographic Flaws

Cryptanalysis is aided by inherent defects and proactive actions

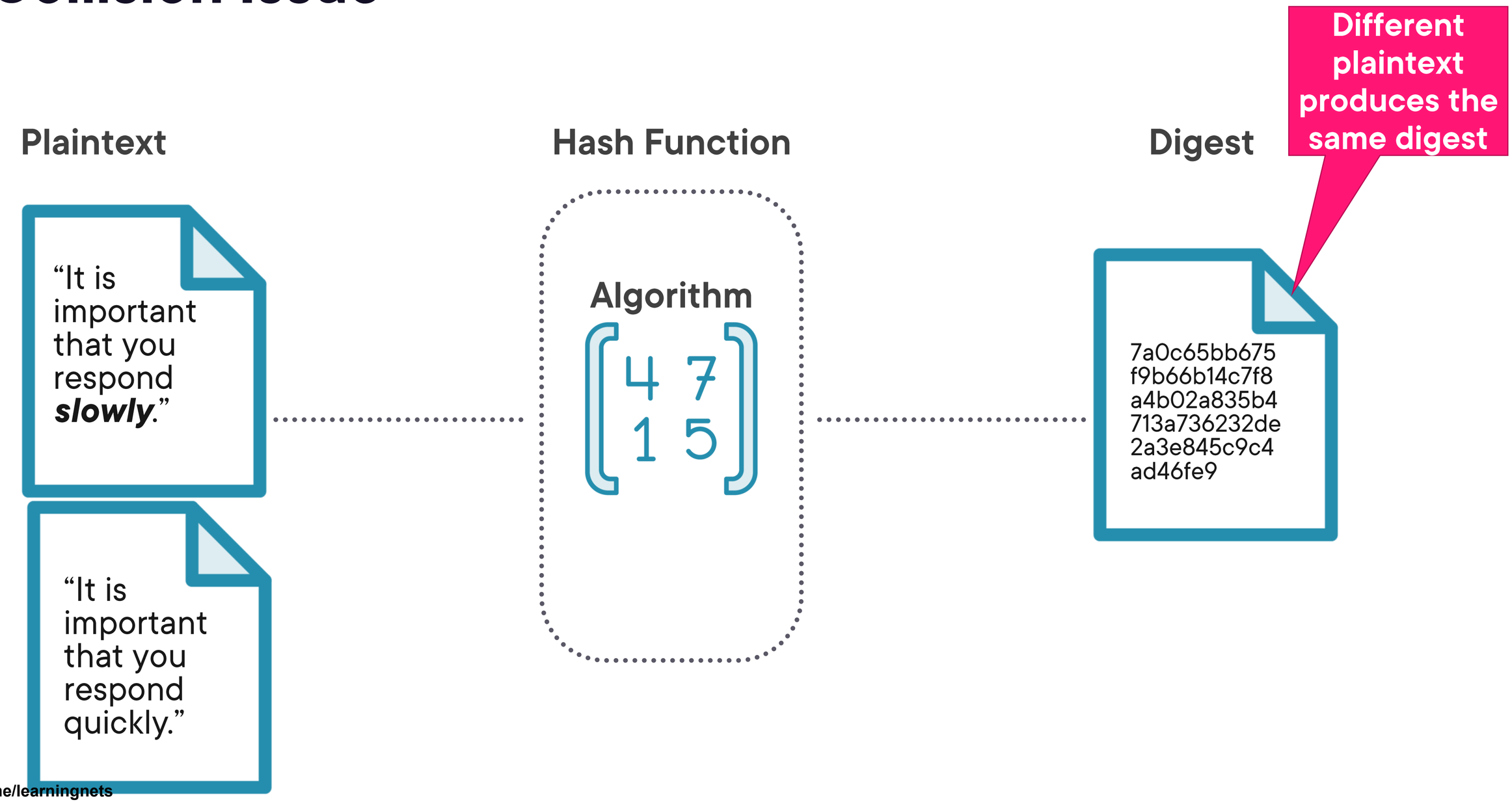
Collision

Hash functions produce same digest for different text.

Collision Issue



Collision Issue



Sample Cryptographic Flaws

Cryptanalysis is aided by inherent defects and proactive actions

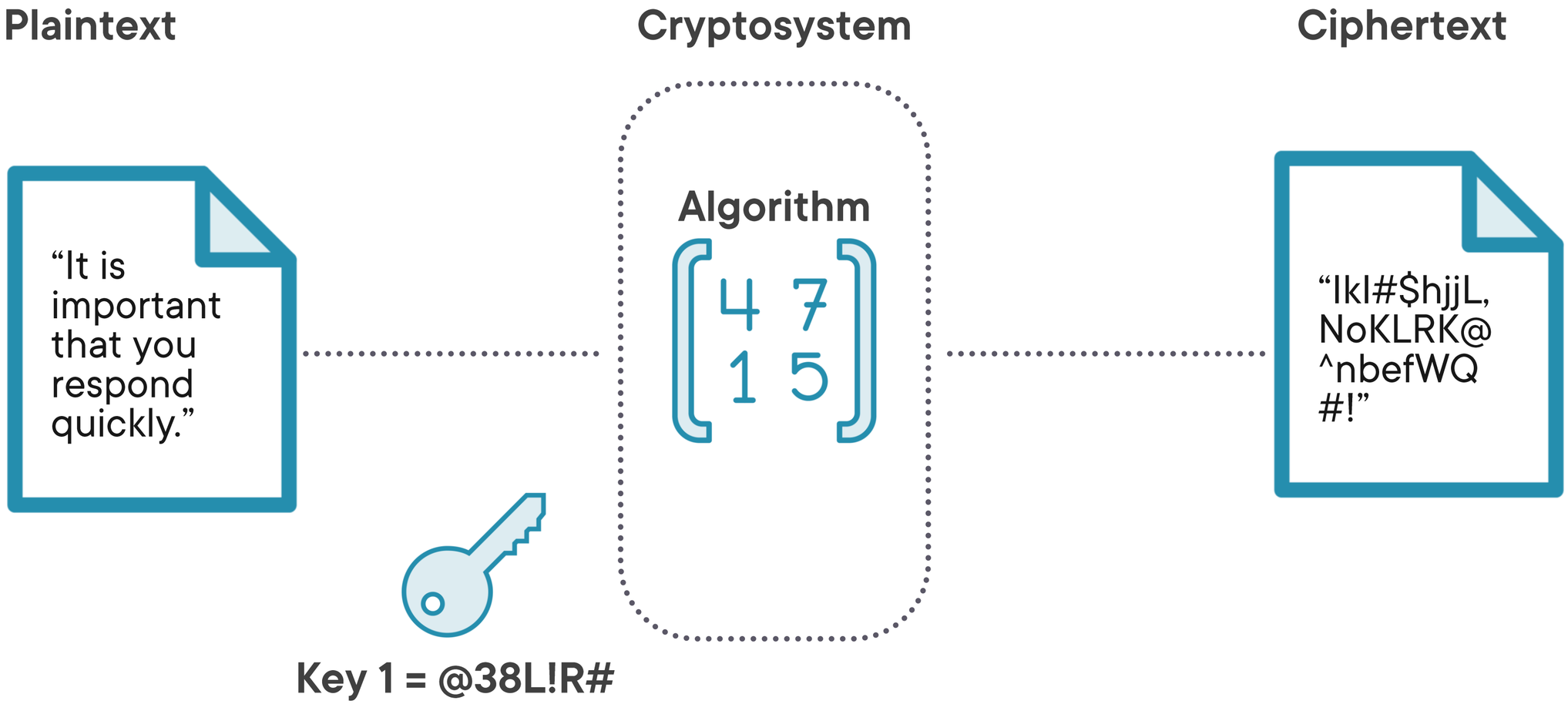
Collision

Hash functions produce same digest for different text.

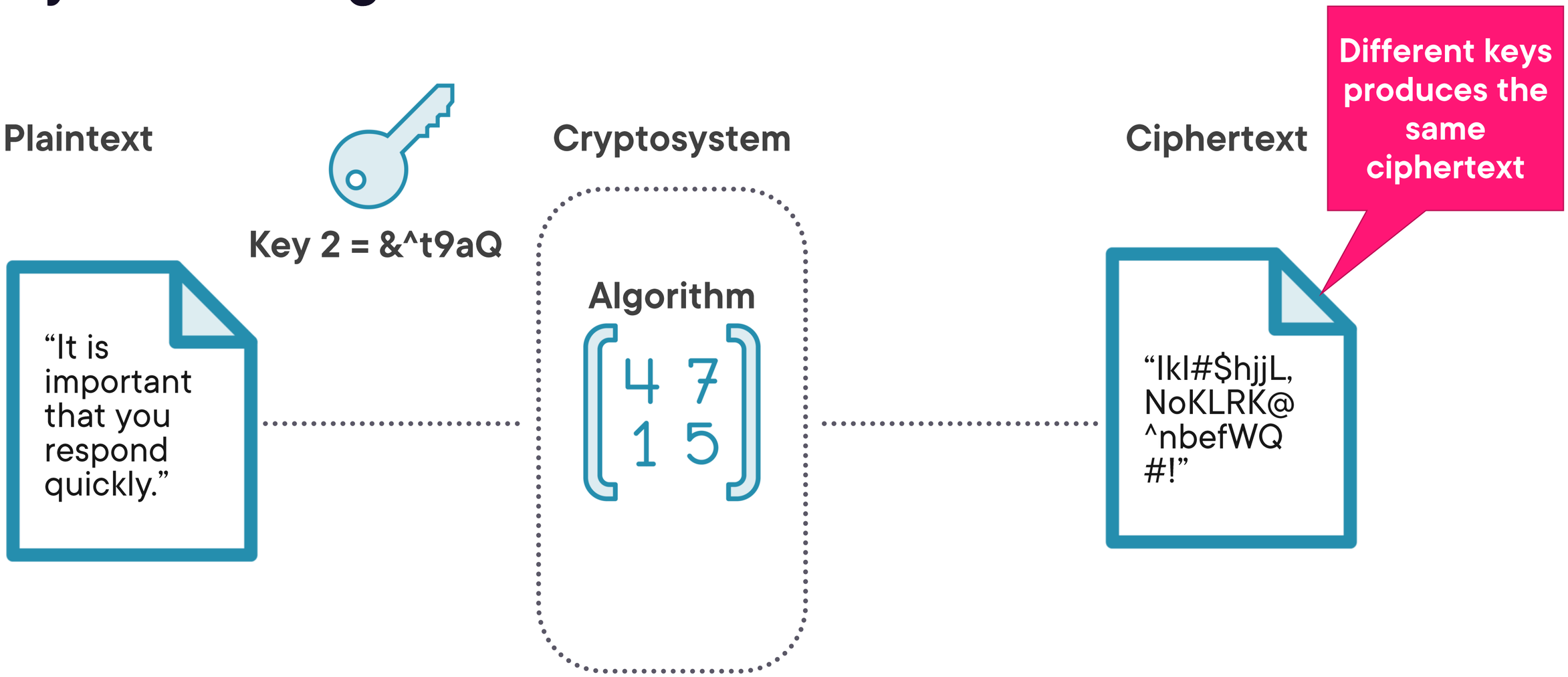
Key Clustering

Two separate keys produce same cipher text.

Key Clustering



Key Clustering



Sample Cryptographic Flaws

Cryptanalysis is aided by inherent defects and proactive actions

Collision

Hash functions produce same digest for different text.

Key Clustering

Two separate keys produce same cipher text.

Man-in-the-Middle

Monitoring and intercepting communications.

A Brief History of Cryptography

Evolution of Cryptography

Manual – Written

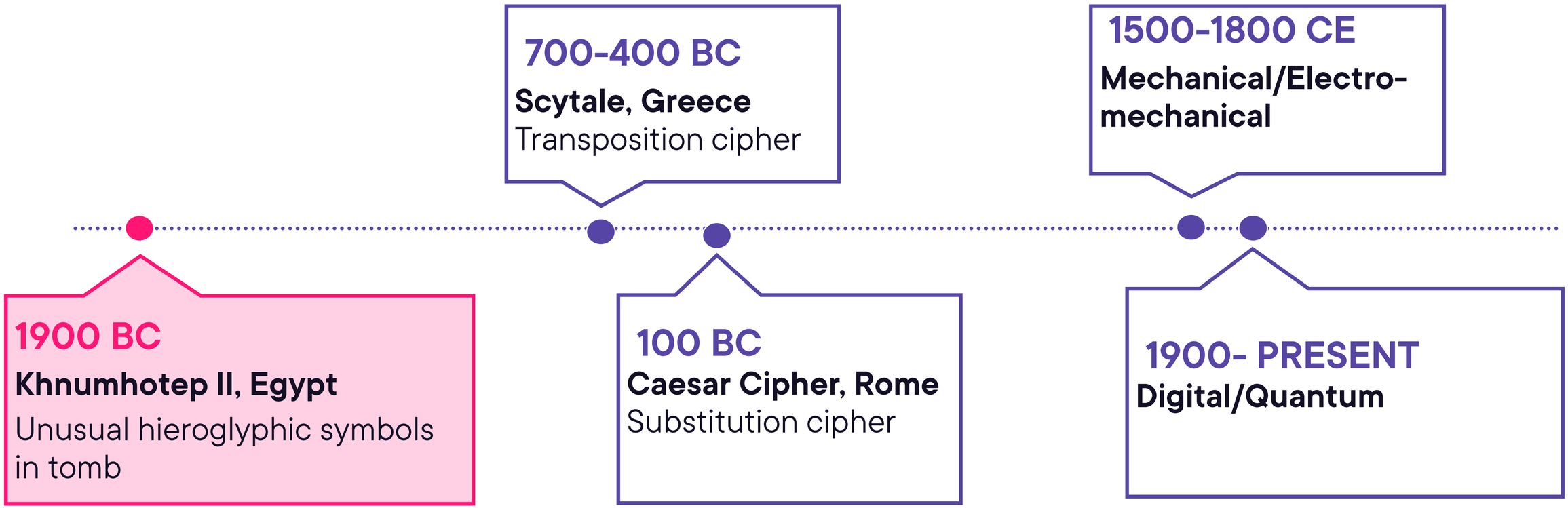
Mechanical – Rotating gears and cipher wheels

Electro-Mechanical – Basic circuit logic and gears

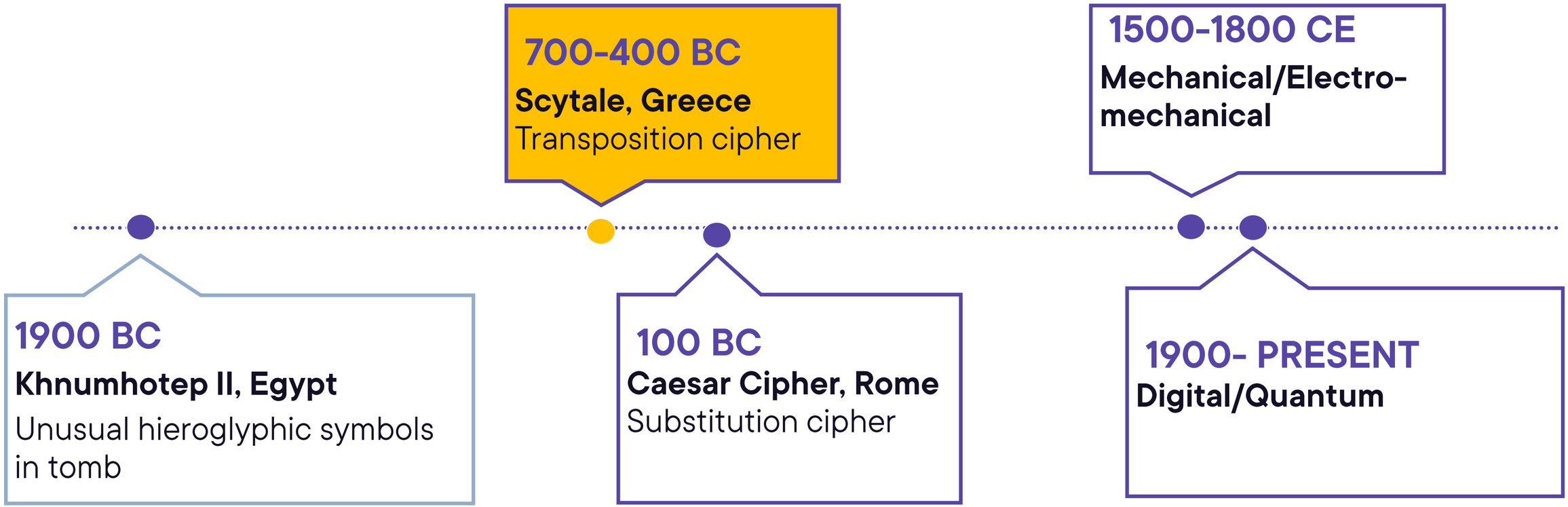
Digital – Binary logic

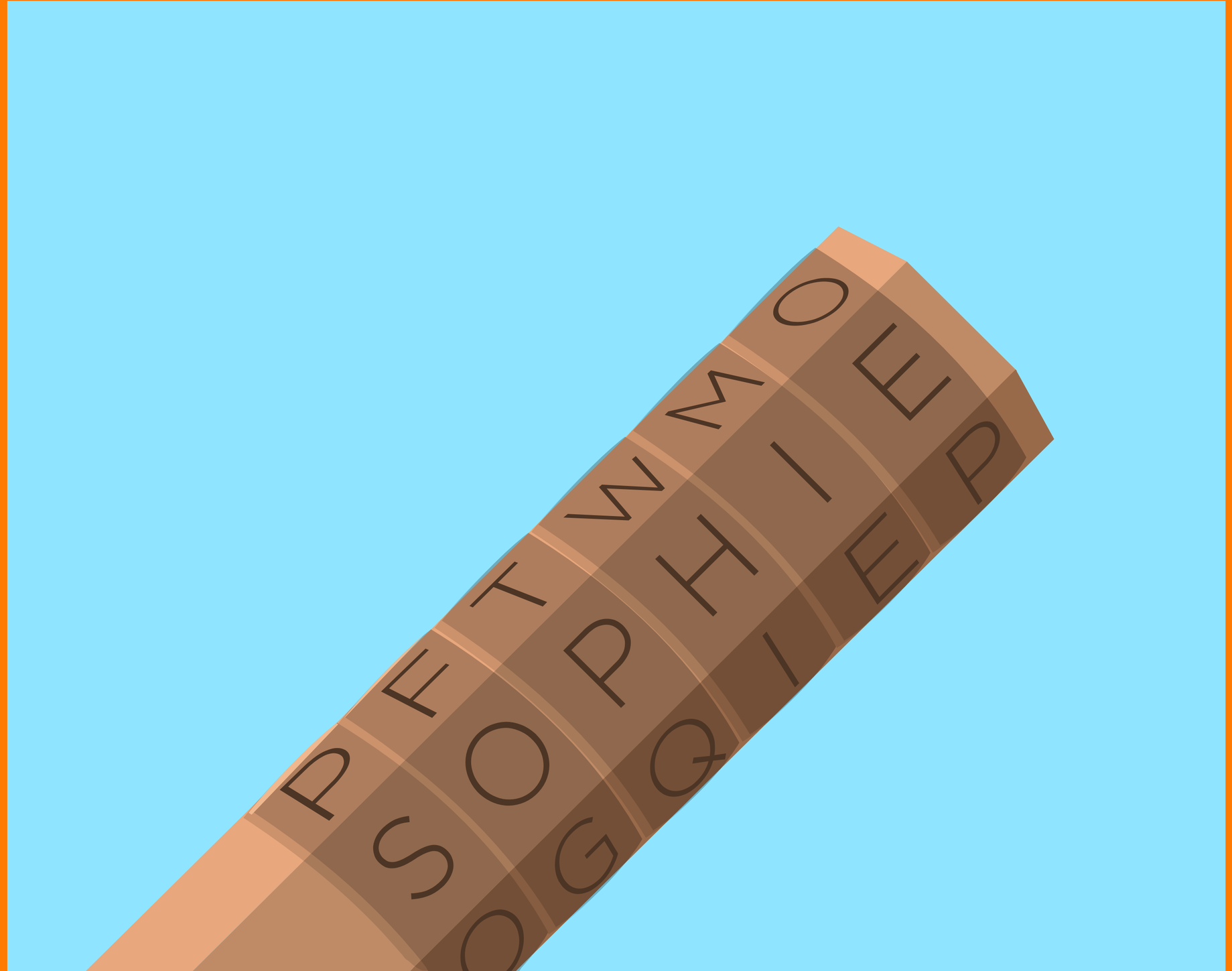
Quantum – Qubit logic

History of Significant Cryptographic Advances

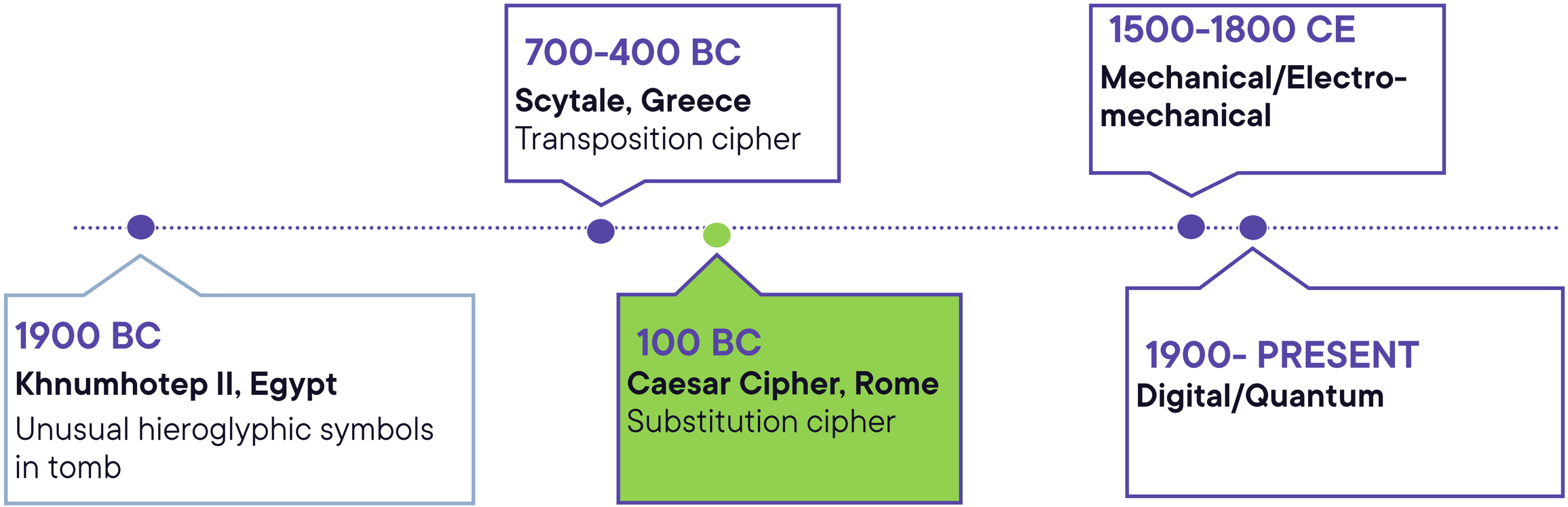


History of Significant Cryptographic Advances

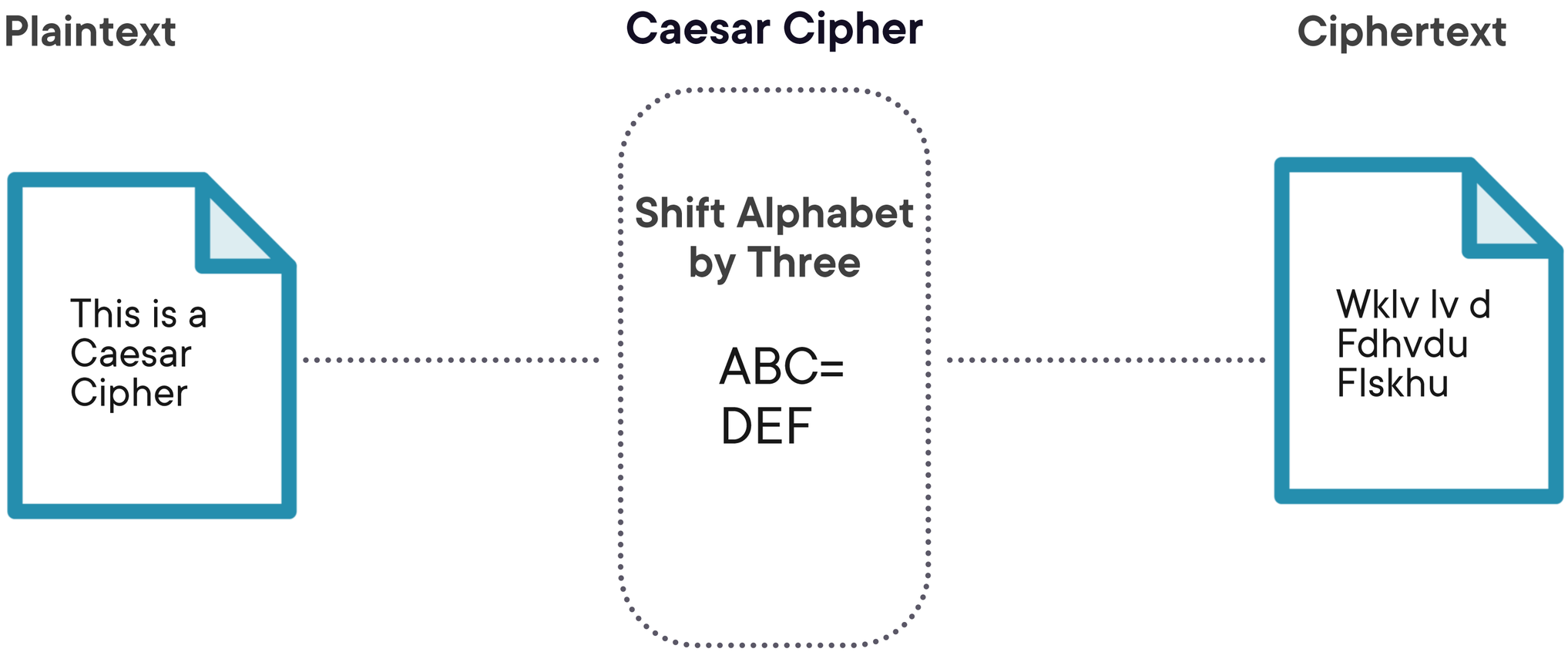




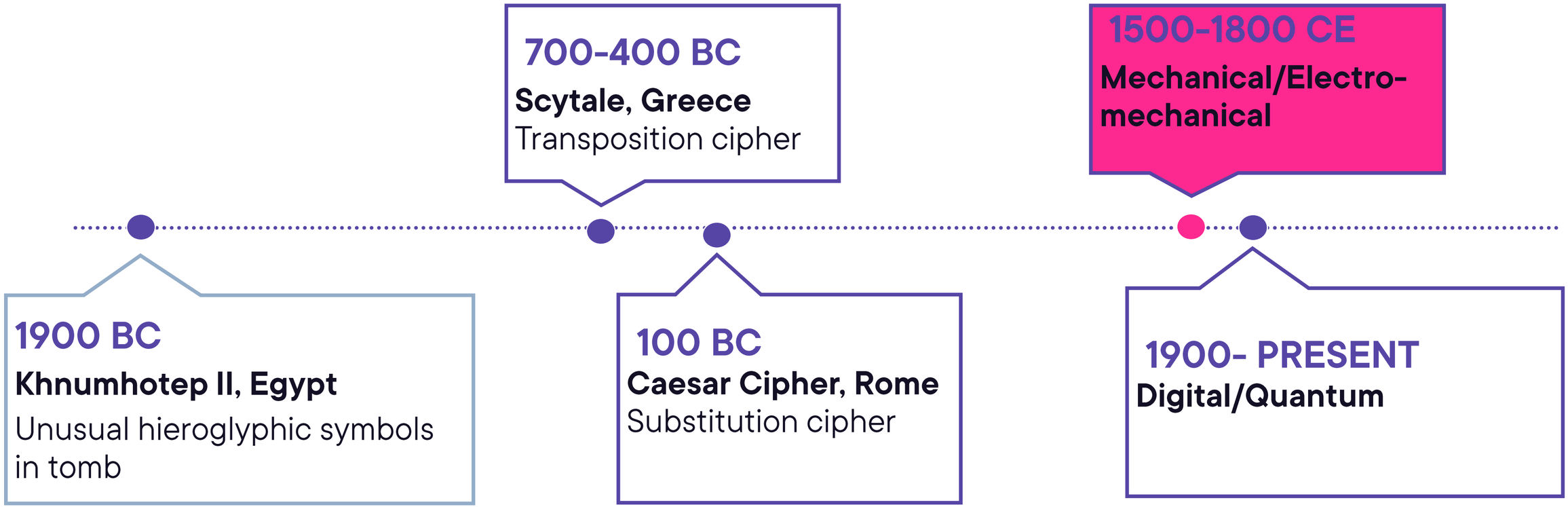
History of Significant Cryptographic Advances

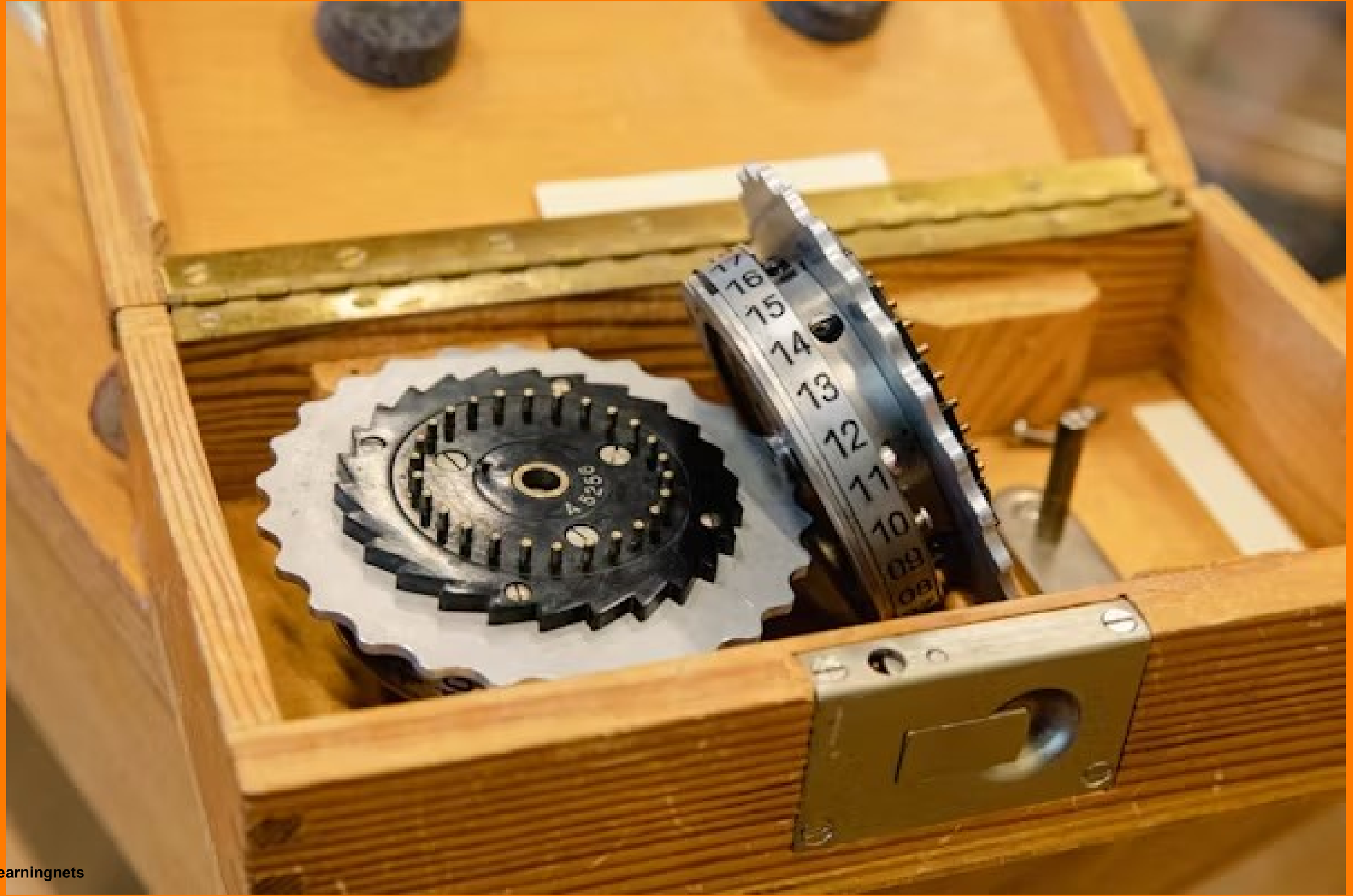


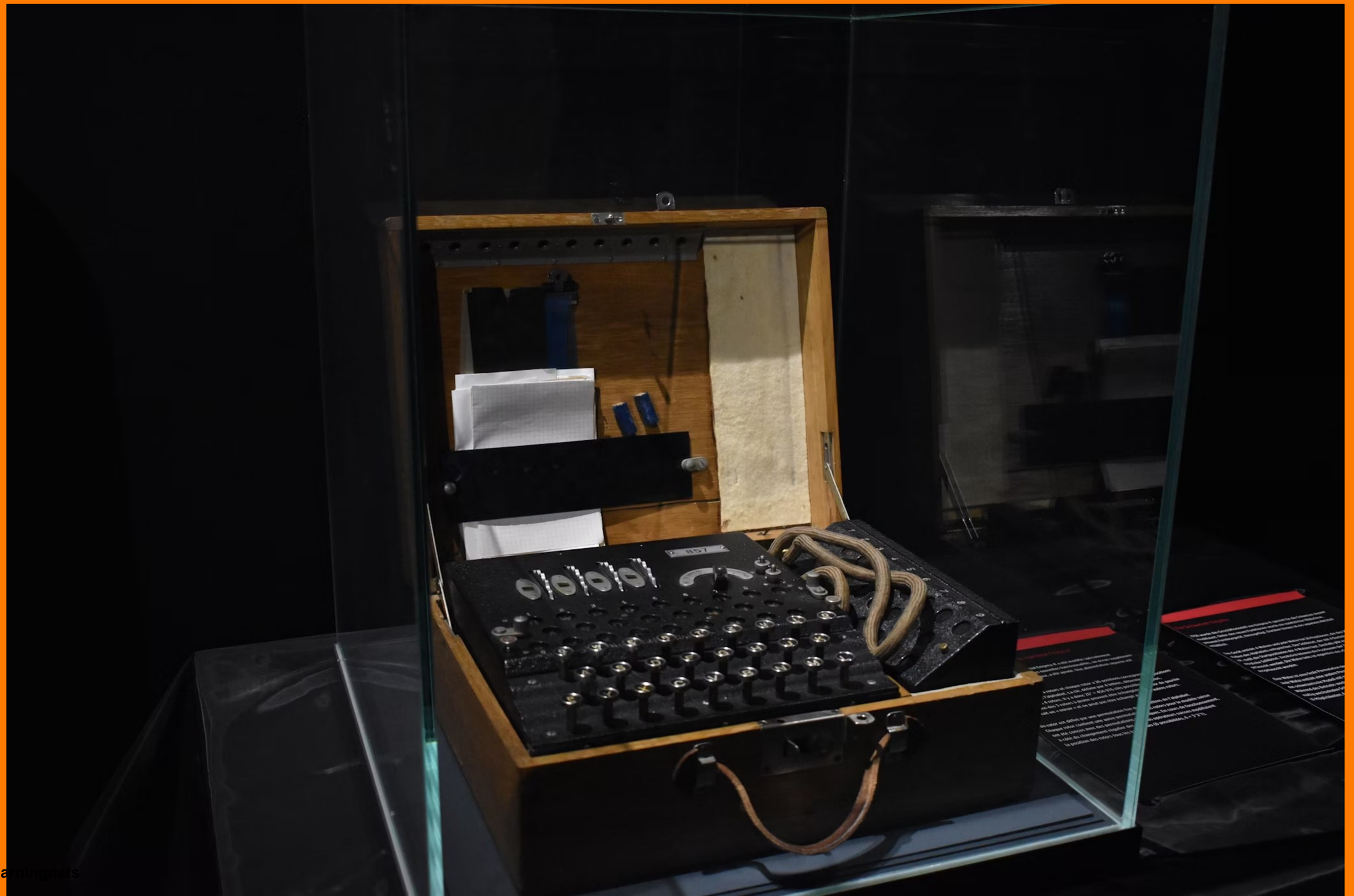
Caesar Cipher at Work



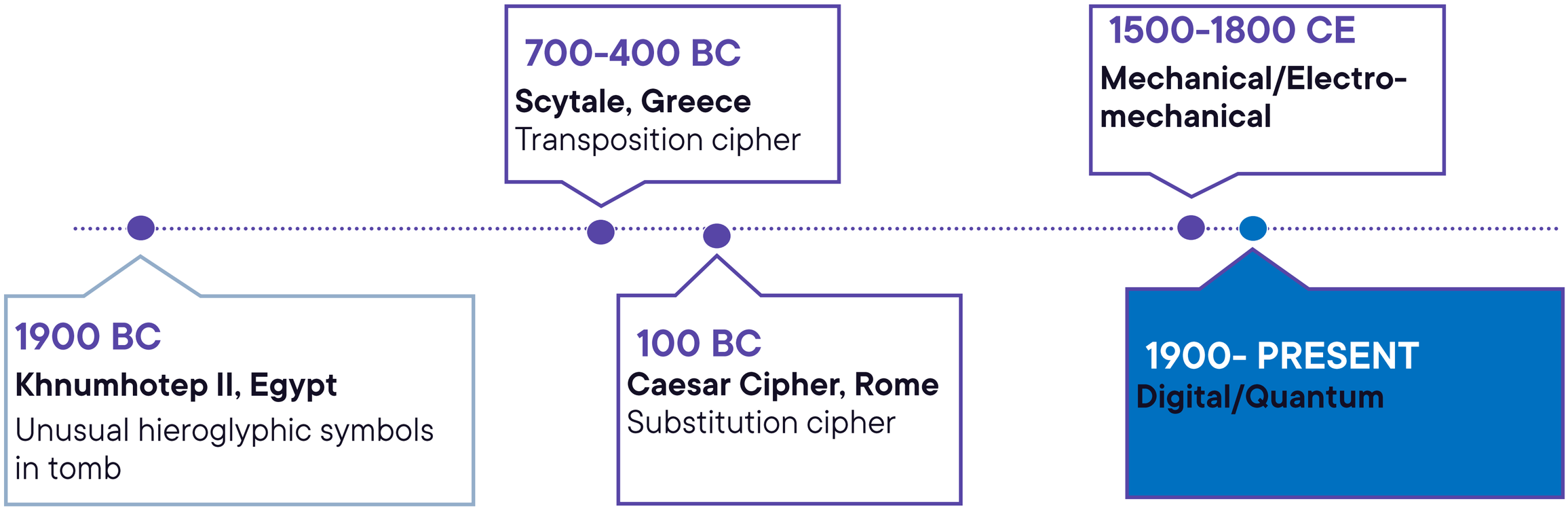
History of Significant Cryptographic Advances

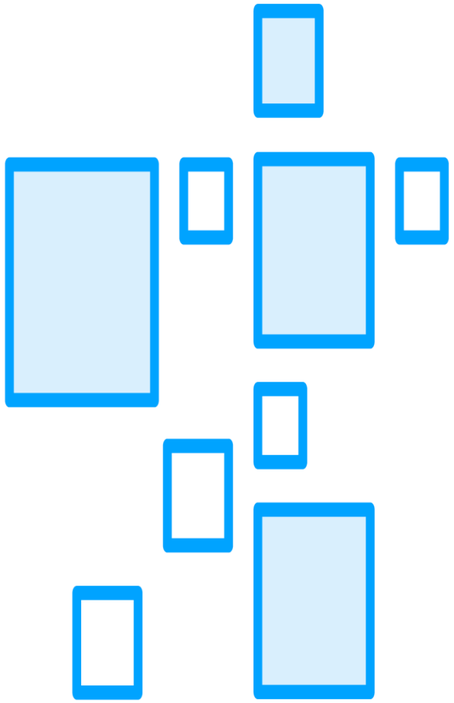






History of Significant Cryptographic Advances





Quantum key distribution

Cryptography entropy

Quantum cryptography/cryptanalysis entropic effect

NIST PQC (Post-Quantum Cryptography)

- CRYSTALS-Kyber
- CRYSTALS-Dilithium
- Falcon
- SPHINCS+

Demystification of Cryptography

Only Three Types of Keys

Symmetric Keys

Same key used for encryption is used for decryption.

Asymmetric Keys

Private and public key pair.

Demystification of Asymmetric Encryption

1.) Process Order

When one half of key-pair encrypts the other decrypts

2.) Public Key

Encryption objective is confidentiality and access control

3.) Private Key

Encryption objective is integrity, authenticity, and non-repudiation

4.) Digital Signature

Private key (encrypting) signing a digest

5.) Digital Certificate

Digital document containing DS of CA and public key of owner

Alternative Names for a Symmetric Key

Single key

Shared key

Secret key

Shared secret key

Session key

Don’t call a symmetric key a private key!

Use Cases for Three Keys

Confidentiality – Public key and Symmetric key

Access control - Public key and Symmetric key

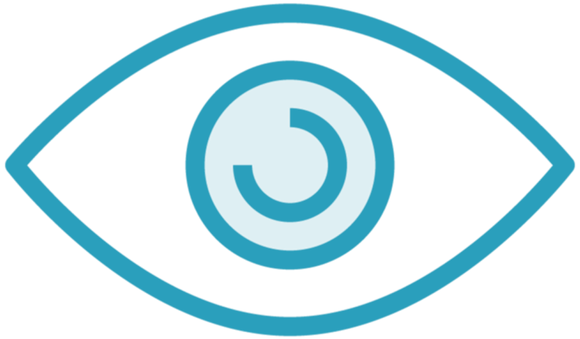
Authenticity – Private key

Integrity – Private key and Symmetric keyed-hash

Non-repudiation – Private key

Data Sensitivity Protection Requirements

Confidentiality vs. Privacy



Privacy
Related to people

Confidentiality
Related to resources

Intellectual property

Competitive advantage

Business data/information

Classification and categorization

ISO/IEC and NIST standards

Confidentiality Business Requirements

Privacy Business Requirements

Personally Identifiable Information (PII)

Direct and indirect identifiers

Human rights

Legal and regulatory

PCI-DSS

Up Next:

Apply Cryptographic Algorithms