Information Assurance and Security – ACIT 4630

Hesam Alizadeh

Week 5 – Winter 2024

Learning Outcomes

- Cryptography and its goals
- Asymmetric and symmetric encryption
- Hash functions
- Digital signatures

Cryptography

The practice and study of techniques for secure communication in the presence of third parties

Image Source

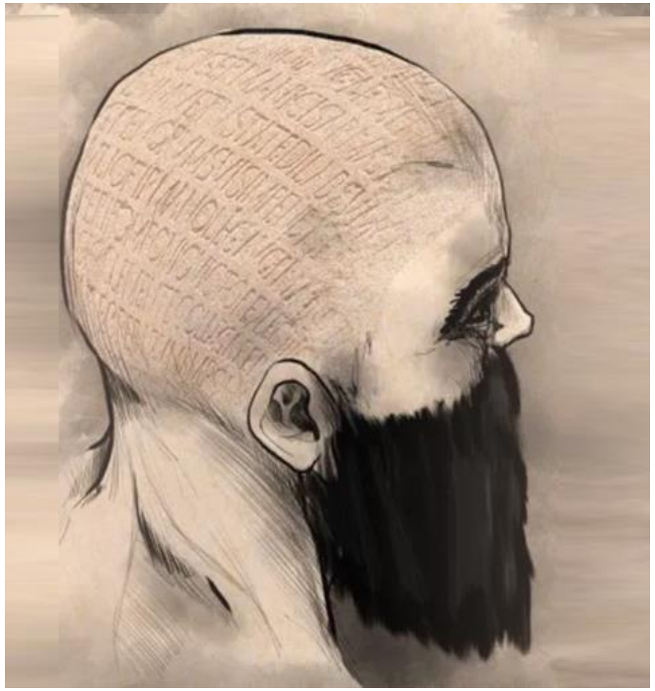


Image Source

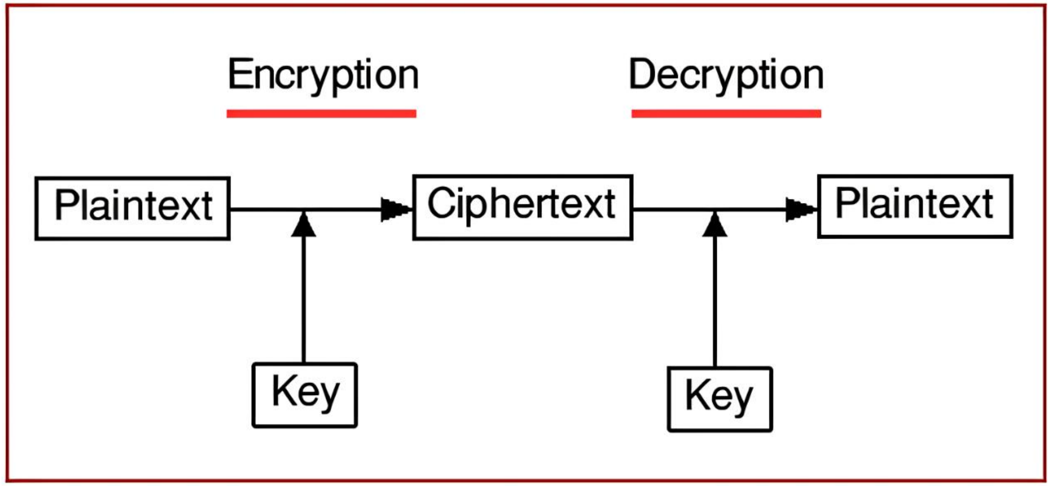
Cryptography objectives

- **Confidentiality** (no unauthorized access)
- **Integrity** (no unauthorized changes)
- **Authentication** (proof of identity)
- **Obfuscation** (hide sensitive data)
- **Non-repudiation** (verify the origin)

How does obfuscation work? What are some use cases of it?

Encryption/Decryption

The process of encoding information so that it's not readable by unauthorized individuals



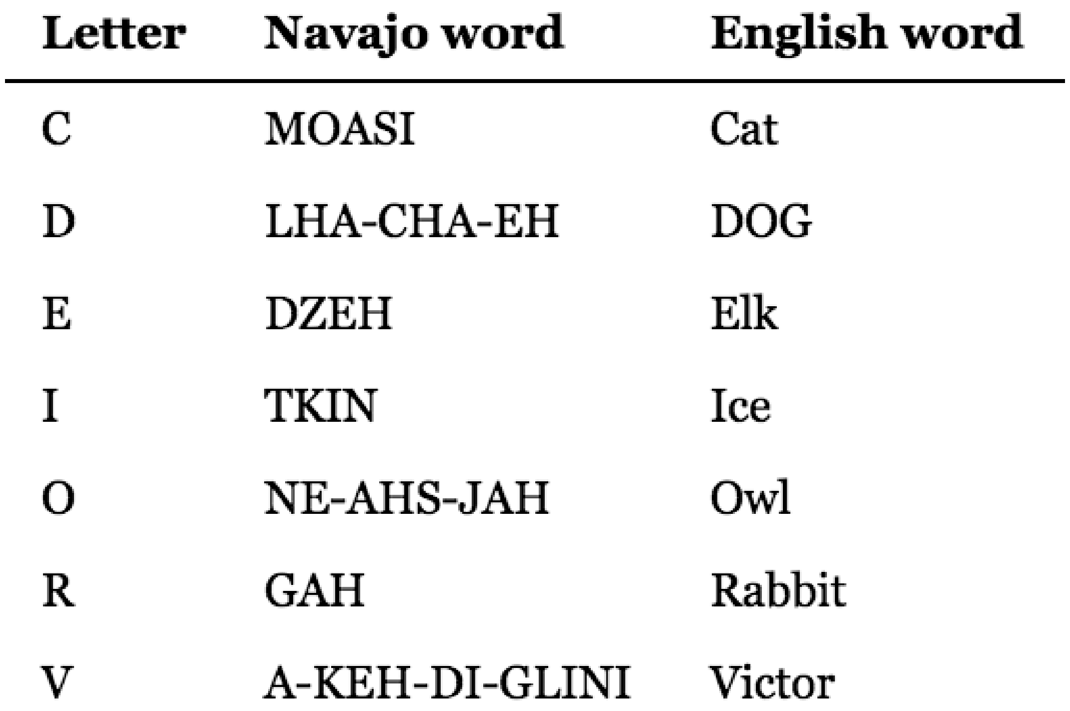
What are some everyday examples where encryption plays a crucial role?

Image Source

Code vs Ciphers

- **Code:** Substitute one word or phrase for another
- **Cipher**: Use mathematical algorithms to encrypt and decrypt messages

- What are benefits of using codes?



Letter	Navajo word	English word
C	MOASI	Cat
D	LHA-CHA-EH	DOG
E	DZEH	Elk
I	TKIN	Ice
O	NE-AHS-JAH	Owl
R	GAH	Rabbit
V	A-KEH-DI-GLINI	Victor

Image Source

Cipher processing techniques

- Stream Cipher

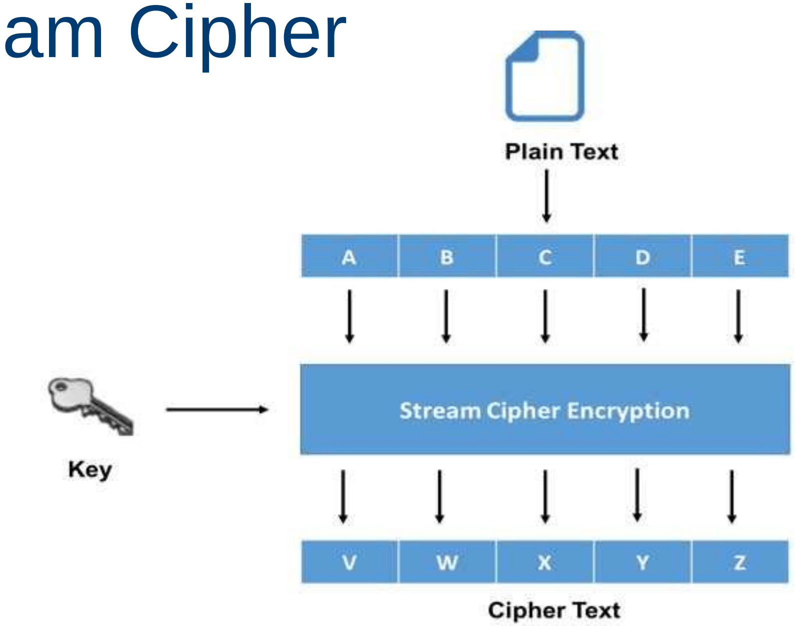


Image Source

- Block Cipher

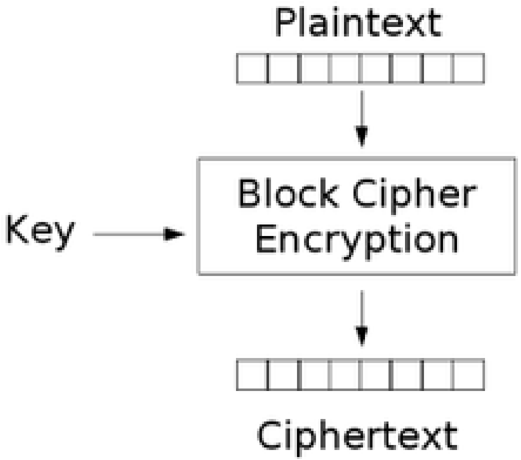


Image Source

In what scenarios might you choose a stream cipher over a block cipher, or vice versa?

Cipher building blocks

- Substitution
  - Change the characters

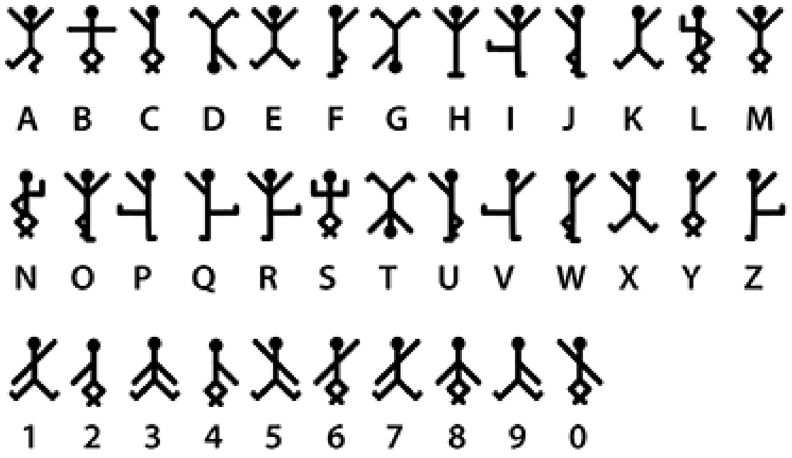
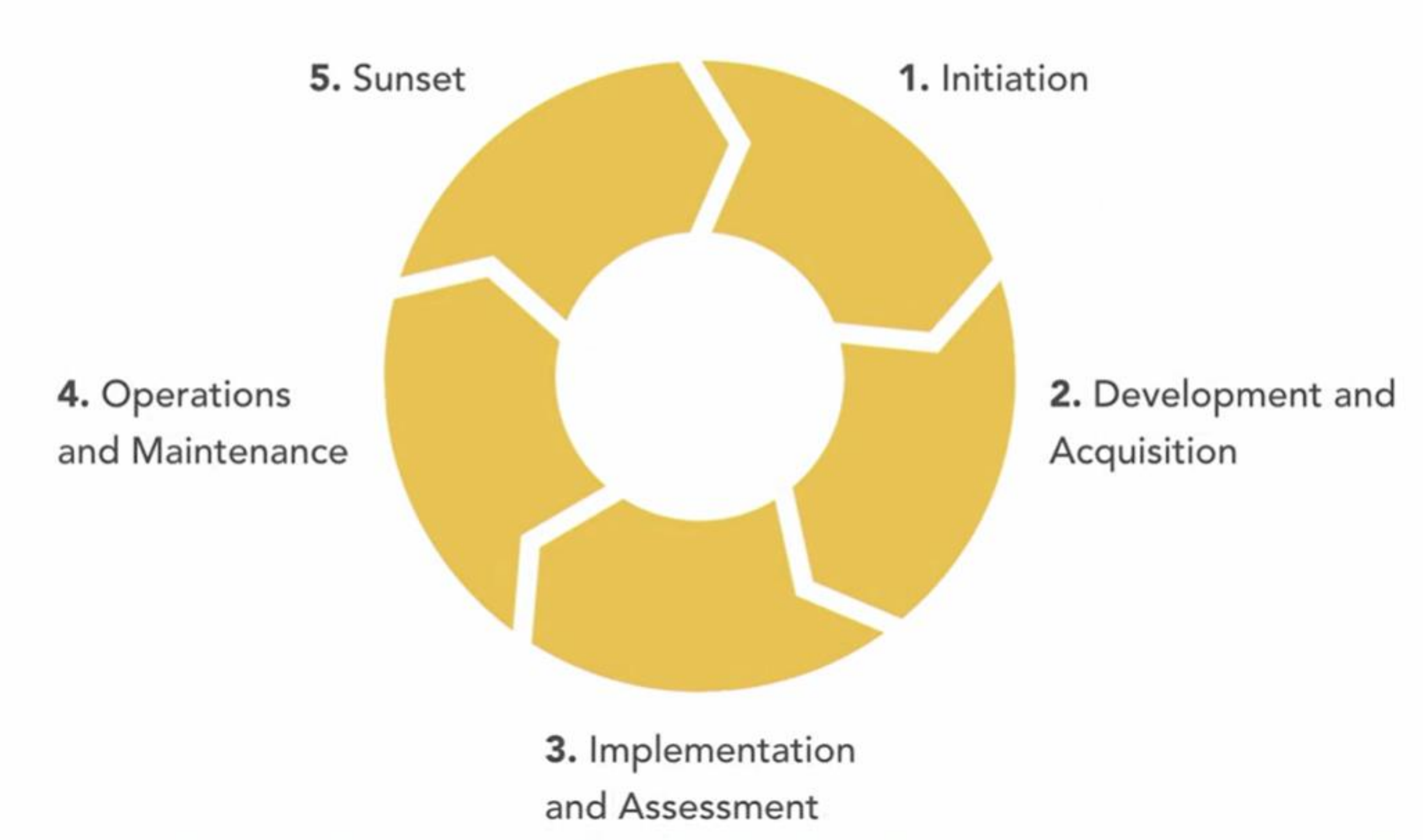


Image Source

- Transposition
  - Rearrange the characters

Image Source

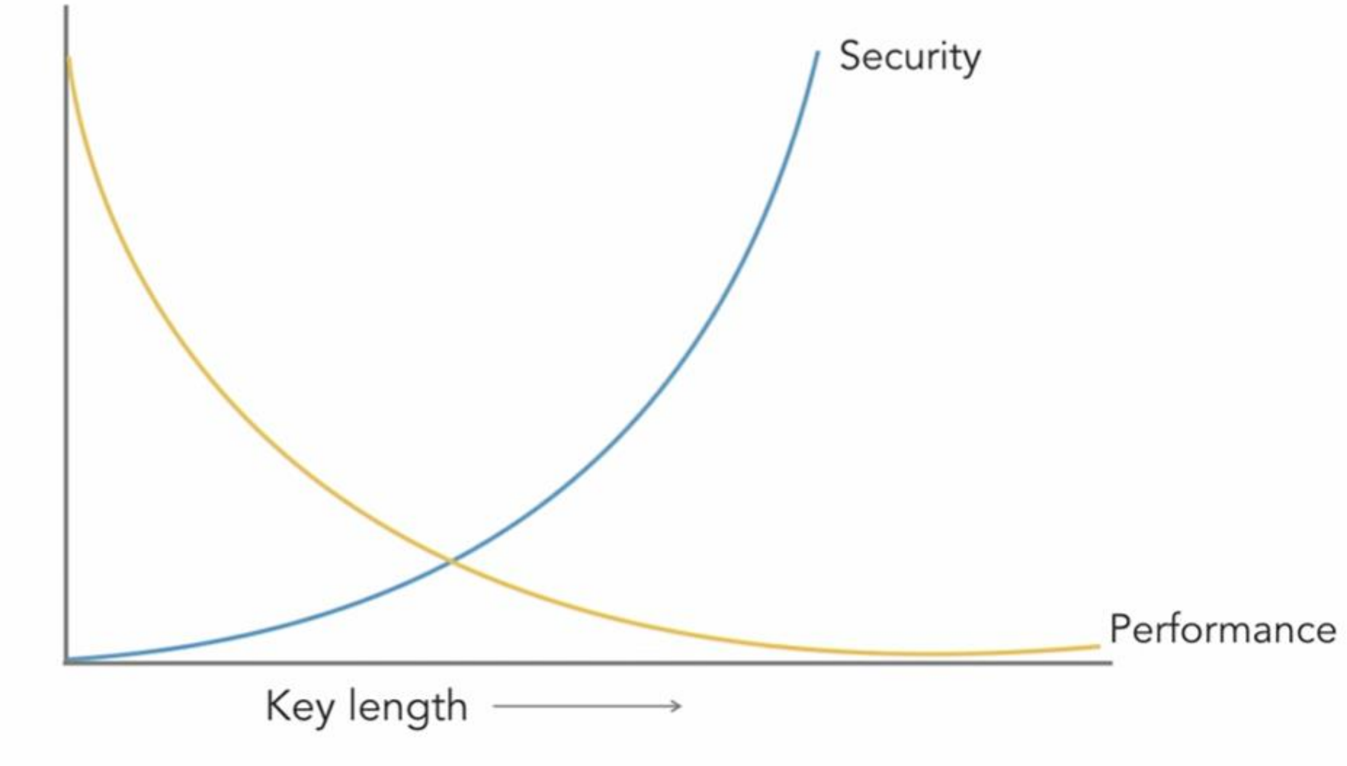
Cryptographic life-cycle


1. Initiation
2. Development and Acquisition
3. Implementation and Assessment
4. Operations and Maintenance
5. Sunset

Why is it important to continuously evolve cryptographic algorithms?

Choosing encryption algorithms

- Use proven algorithms
- Key length trade-off



Symmetric Cryptography

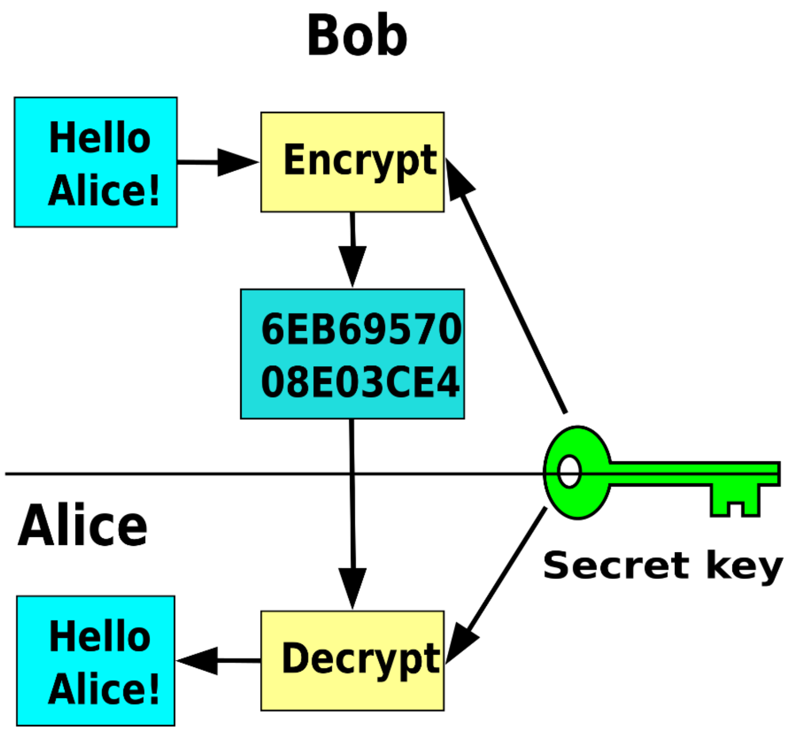


Image Source

Asymmetric Cryptography

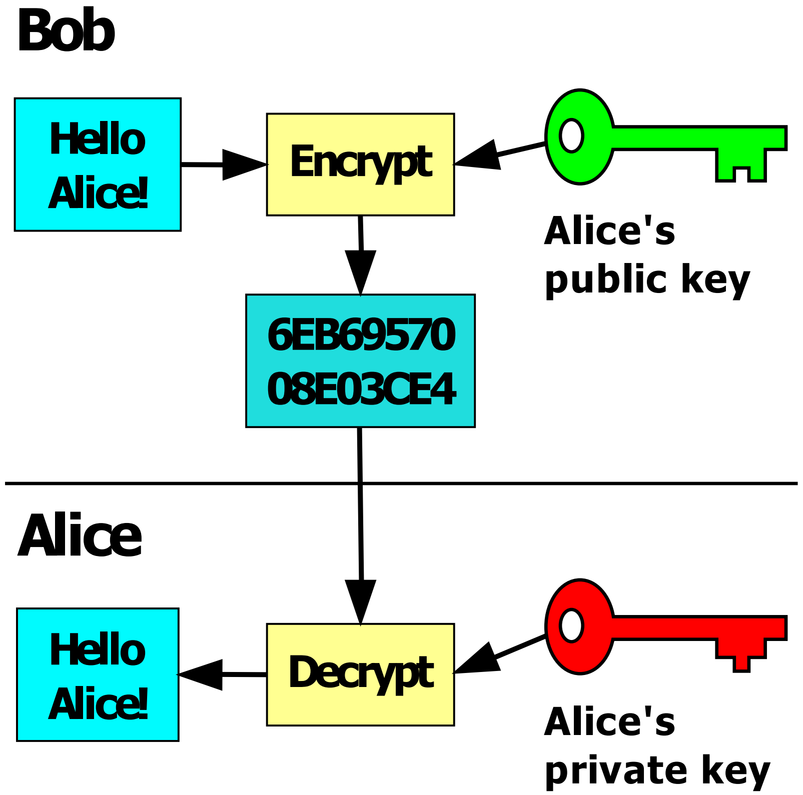


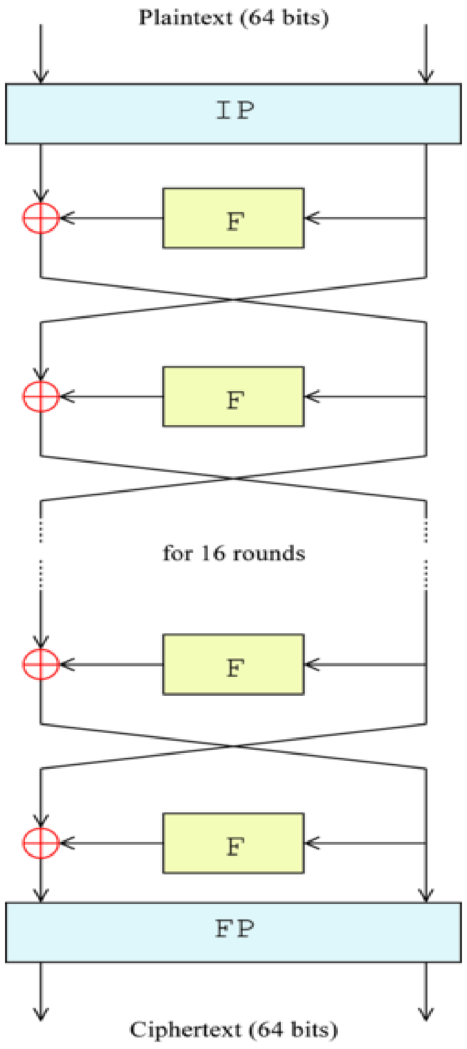
Image Source

Asymmetric vs Symmetric

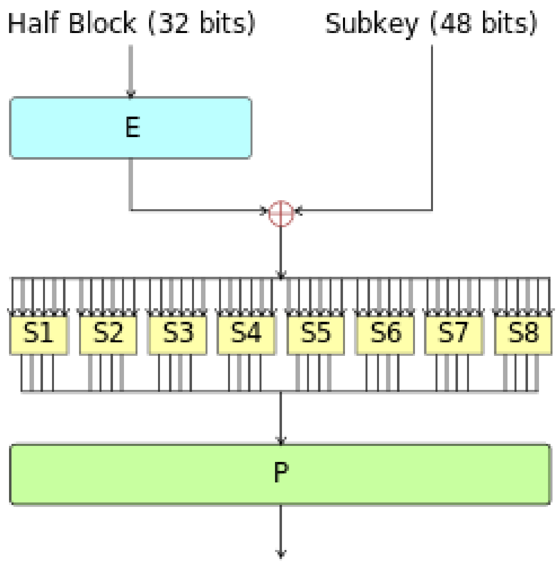
Criteria	Asymmetric	Symmetric
Key usage	Two keys: public and private	One key
Key distribution	Public keys are open, private keys are secret	Keys are exchanged securely
Key length	Longer keys (e.g. 2048 bits)	Shorter keys (e.g. 128 bits)
Encryption speed	Slower	Faster
Security level	Provides confidentiality, non-repudiation, and integrity	Less secure, provides only confidentiality
Examples	RSA, DSA, DH, ECC, etc.	AES, DES, 3DES, RC4, etc.

Data Encryption Standard (DES)

- Symmetric encryption algorithm
- 64-bit block cipher
- Key length: 56-bits
- Considered insecure
- DES vs 3DES

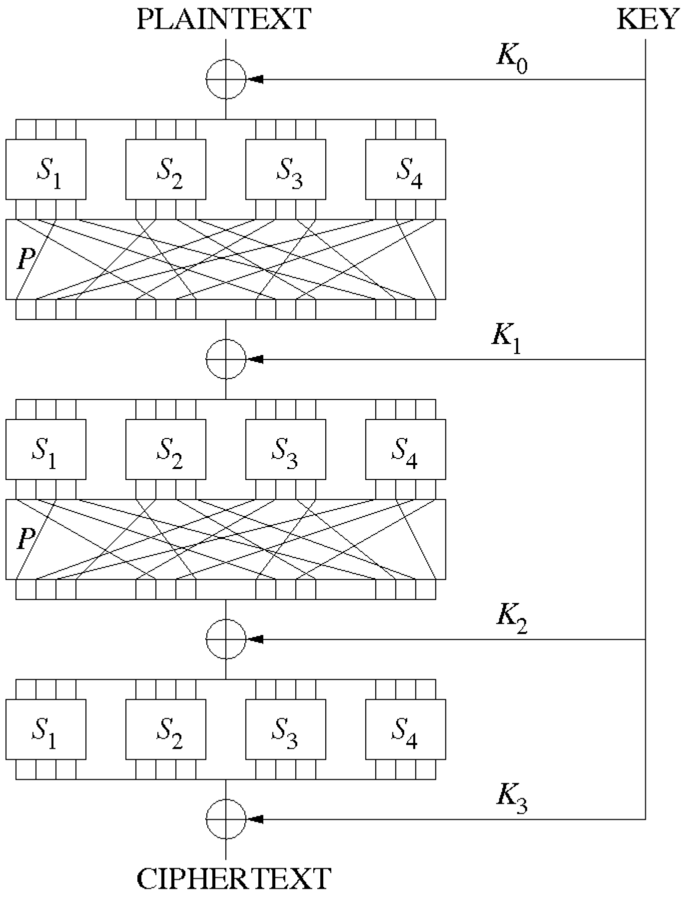


Feistel Function



Advanced Encryption Standard (AES)

- Symmetric encryption algorithm
  - Based on a substitution-permutation network (SP network)
- 128-bit block cipher
- Key length: 128/192/256-bits
- Considered secure



Rivest, Shamir, Adelman (RSA)

- Asymmetric encryption algorithm
- Variable key length: between 1,024 and 4,096 bits
- Considered secure
- Select two very large prime numbers to create private and public keys
- Why do you think RSA has become a cornerstone in secure digital communications?

Hash Functions

Generating a unique fixed-size number (hash) from a message of an arbitrary length

- Cryptography properties:
  - **One-way function**: No way to find a message m given hash(m)
  - **Collision-resistance**: Find two different inputs with same hash value
- What are some applications of cryptography hash functions?

Hash Functions (Cont.)

- Message Digest 5 (MD5)
  - 128-bit hash
  - Collision resistance broken in 2013
- Secure Hash Algorithm (SHA)
  - SHA-1: 160-bit hash, insecure
  - SHA-2: Different families with different hash sizes (224, 256, etc.)
  - SHA-3: Different approach, user-selected hash size
- RACE Integrity Primitives Evaluation Message Digest (RIPEMD)

One-way Hash Functions – Applications

- Password verification (Registration & login)

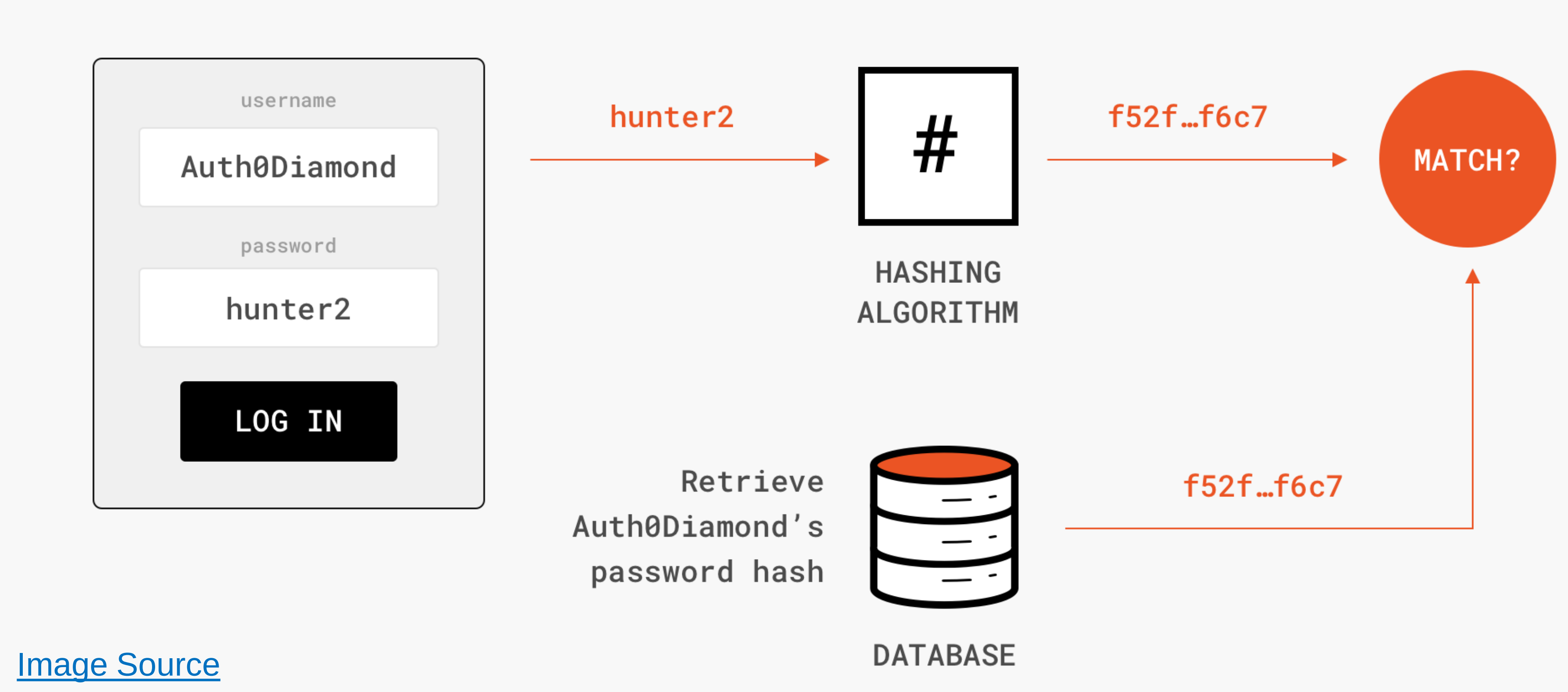


Image Source

HMAC

- Message Authentication Code (tag):
  - Short piece of info attached to the message
  - Provides authentication and integration
- Hash-based MAC:
  - Combine the message and a shared secret key and then apply the hashing function (as MAC) on the result

Digital Signatures

A mathematical scheme for verifying the authenticity of digital messages or documents.

- Hashing + asymmetric key algorithm
- Provides:
  - Authentication
  - Integrity
  - Non-repudiation

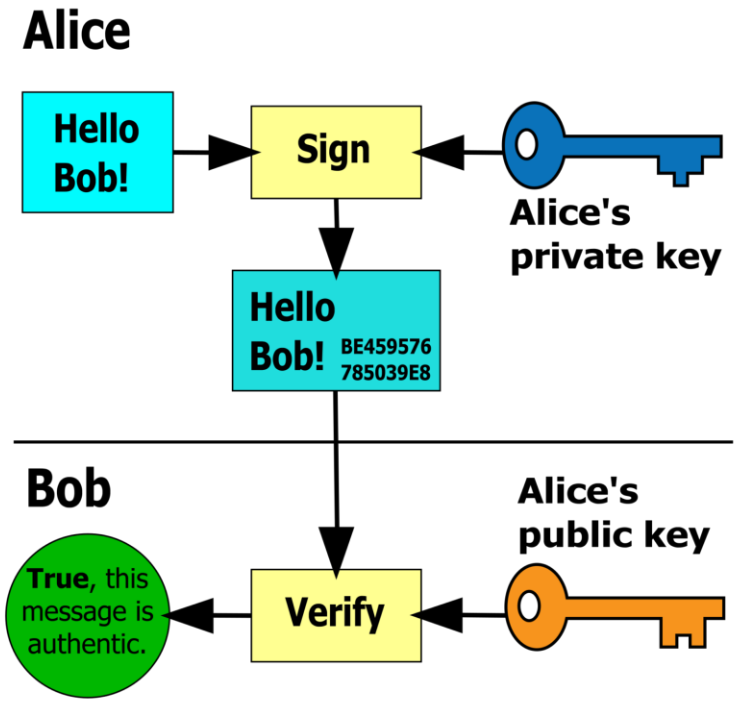


Image Source