Symmetric Cryptography

Introduction to Computer Security
Naercio Magaia and Imran Khan

Contents

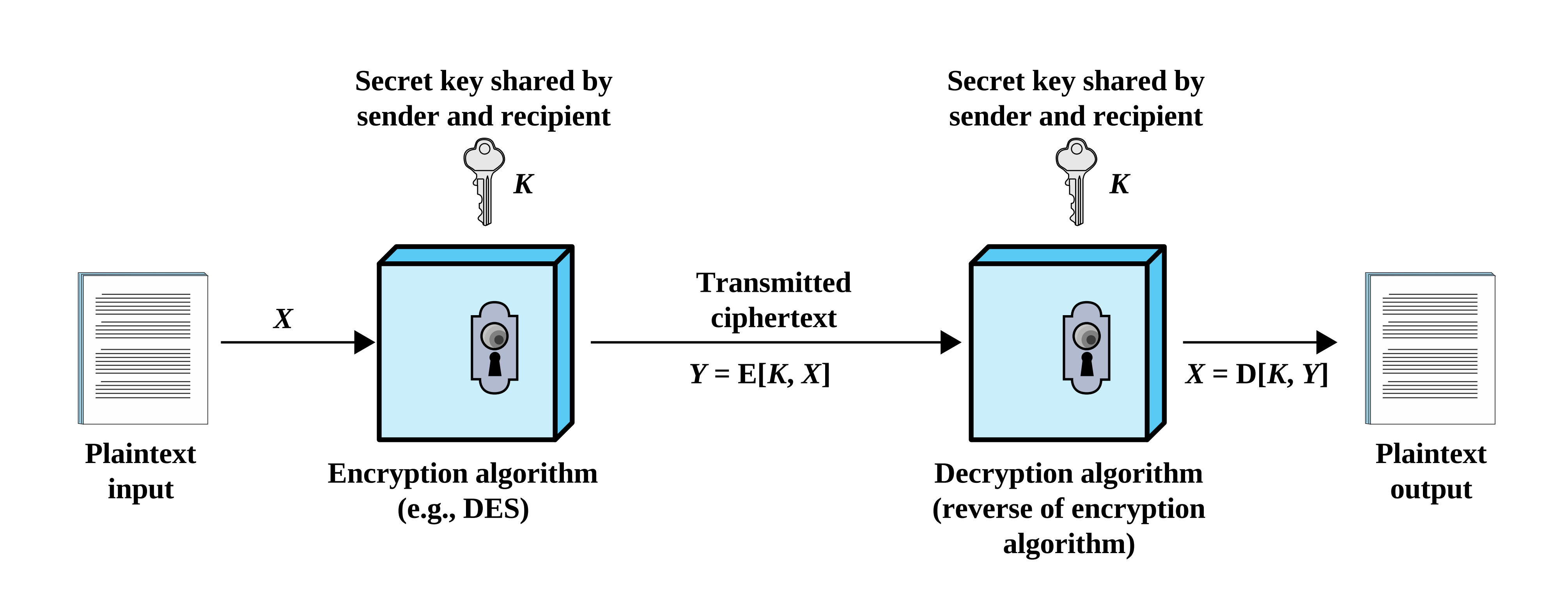
- Symmetric Encryption
  - Definitions
- Encryption Algorithms
- Confidentiality
- Block and Stream modes
- Message Authentication
- Hash Functions

Symmetric Encryption

- The universal technique for providing confidentiality for transmitted or stored data
- Also referred to as **conventional** or **single-key** encryption
- Two requirements for its secure use:
  - Need a strong encryption algorithm
  - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure

- **Plaintext:** The original message fed into the algorithm
- **Encryption algorithm:** The rules for substituting and transforming the plaintext
- **Secret Key:** The sequence of bytes that guides the encryption algorithm
- **Ciphertext:** The scrambled message out of the algorithm
- **Decryption algorithm:** The rules for substituting and transforming the ciphertext to return the plaintext

Symmetric Encryption Information Flow


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
$Y = E[K, X]$
$X = D[K, Y]$
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Attacking Symmetric Encryption

Cryptanalytic Attacks

- Rely on:
  - Nature of the algorithm
  - Some knowledge of the general characteristics of the plaintext
  - Some sample plaintext-ciphertext pairs
- **Exploits the characteristics** of the algorithm to attempt to deduce a specific plaintext or the key being used
  - If successful, all future and past messages encrypted with that key **are compromised**

Brute-Force Attacks

- Try **all possible keys** on some ciphertext until an intelligible translation into plaintext is obtained
  - On average **half of all possible keys** must be tried to achieve success

Data Encryption Standard (DES)

- The first widely used encryption scheme
  - FIPS PUB 46 (January 1977)
  - Referred to as the Data Encryption Algorithm (DEA)
  - Uses 64 bits plaintext block and 56 bit key to produce a 64 bits ciphertext block

- Strength concerns about:
  - the algorithm itself

    DES is the **most studied** encryption algorithm in existence

  - the use of a 56-bit key

    The speed of commercial off-the-shelf processors makes this key length **woefully inadequate**

Triple DES (3DES)

- Repeats basic DES algorithm three times using either two or three unique keys
- First standardized for use in financial applications in ANSI standard X9.17 in 1985
- Attractions:
  - 168-bit key length overcomes the vulnerability to brute-force attack of DES
  - Underlying encryption algorithm is the same as in DES
- Drawbacks:
  - Algorithm is sluggish in software
  - Uses a 64-bit block size

Advanced Encryption Standard (AES)

Needed a replacement for 3DES

- 3DES was not reasonable for long term use

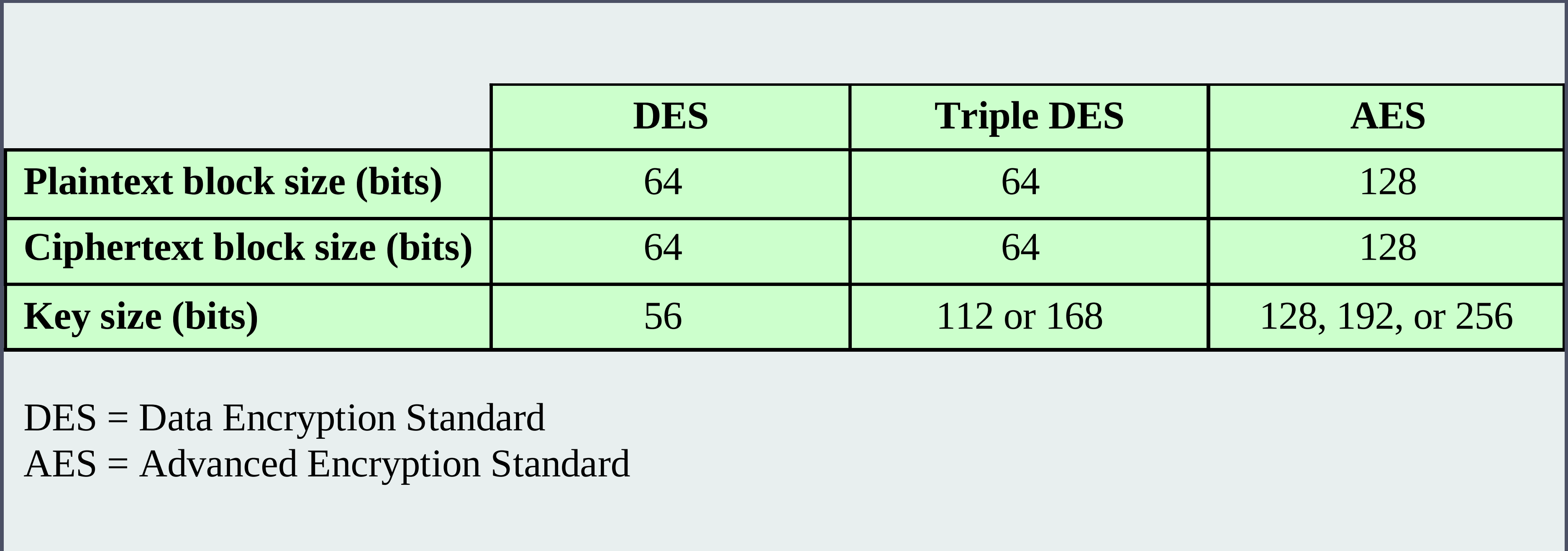
NIST called for proposals for a new AES in 1997

- Should have a security strength equal to or better than 3DES
- Significantly improved efficiency
- Symmetric block cipher
- 128 bits data and 128/192/256 bits keys

Selected Rijndael in November 2001

- Published as FIPS 197

Comparison of Three Popular Symmetric Encryption Algorithms



	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

Average Time Required for Exhaustive Key Search

Key size (bits)	**Cipher**	**Number of Alternative Keys**	**Time Required at 10^9 decryptions/s**	**Time Required at 10^{13} decryptions/s**
56	DES	$2^{56} \approx 7.2$ ´ 10^{16}	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4$ ´ 10^{38}	2^{127} ns = 5.3 ´ 10^{21} years	5.3 ´ 10^{17} years
168	Triple DES	$2^{168} \approx 3.7$ ´ 10^{50}	2^{167} ns = 5.8 ´ 10^{33} years	5.8 ´ 10^{29} years
192	AES	$2^{192} \approx 6.3$ ´ 10^{57}	2^{191} ns = 9.8 ´ 10^{40} years	9.8 ´ 10^{36} years
256	AES	$2^{256} \approx 1.2$ ´ 10^{77}	2^{255} ns = 1.8 ´ 10^{60} years	1.8 ´ 10^{56} years

Practical Security Issues

- Typically, symmetric encryption is applied to a unit of data larger than a single 64-bit or 128-bit block
- Electronic codebook (ECB) mode is the simplest approach to multiple-block encryption
  - Each block of plaintext is encrypted using the same key
  - Cryptanalysts may be able to exploit regularities in the plaintext
  - Can be massively parallelised
- Modes of operation
  - Alternative techniques (i.e., **Chaining** and **Streaming**) developed to increase the security of symmetric block encryption for large sequences
  - Overcomes the weaknesses of ECB

Block & Stream Ciphers

Block Cipher

- Processes the input one block of elements at a time
- Produces an output block for each input block
- Identical blocks generate identical output
- More common

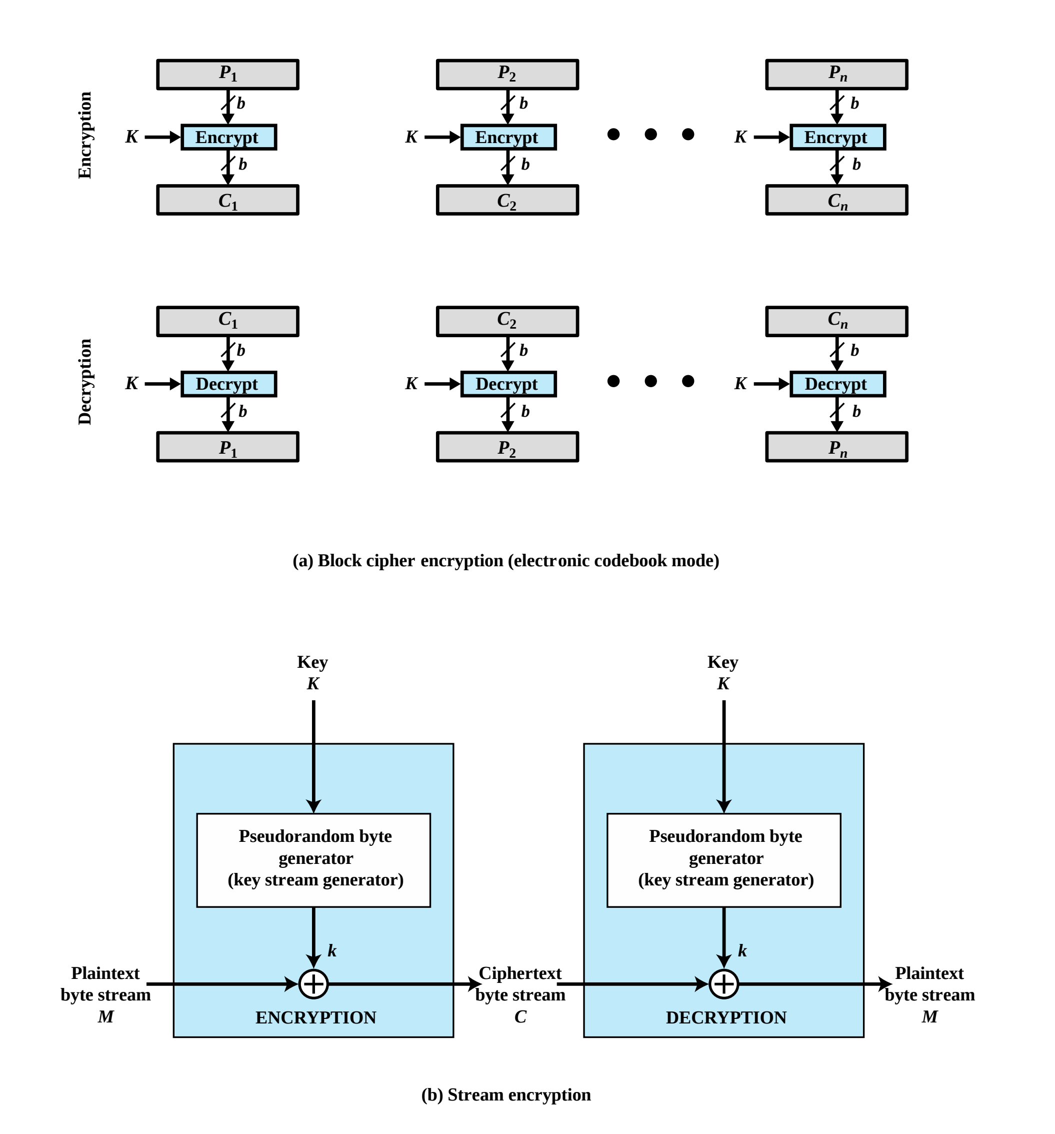
Cipher Block Chaining

- Process one block at a time
- Use the output of the current block XORed with the input of the next block
- Identical blocks generate different output

Stream Cipher

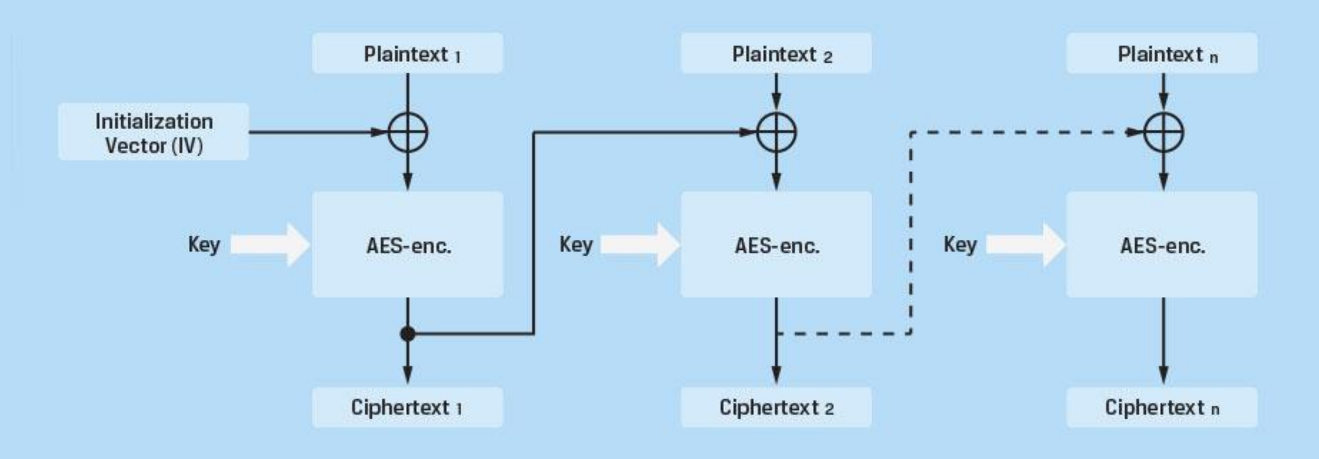
- Processes the input elements continuously
- Produces output one element at a time
- Primary advantage is that they are almost always faster and **use far less code**
- Encrypts plaintext **one byte at a time**
- **Pseudorandom stream** is one that is unpredictable without knowledge of the input key

Types of Symmetric Encryption

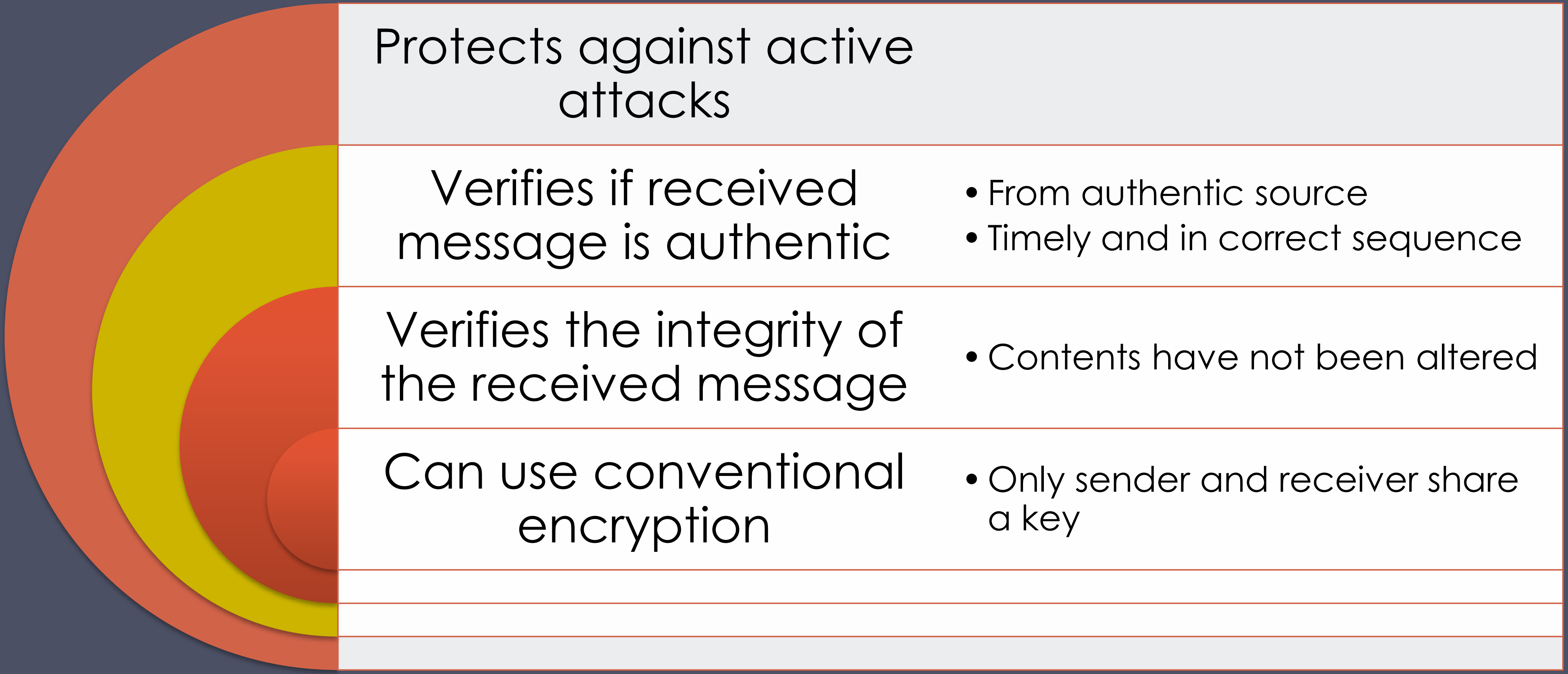


(a) Block cipher encryption (electronic codebook mode)

(b) Stream encryption



Message Authentication



Protects against active attacks

Verifies if received message is authentic

- From authentic source
- Timely and in correct sequence

Verifies the integrity of the received message

- Contents have not been altered

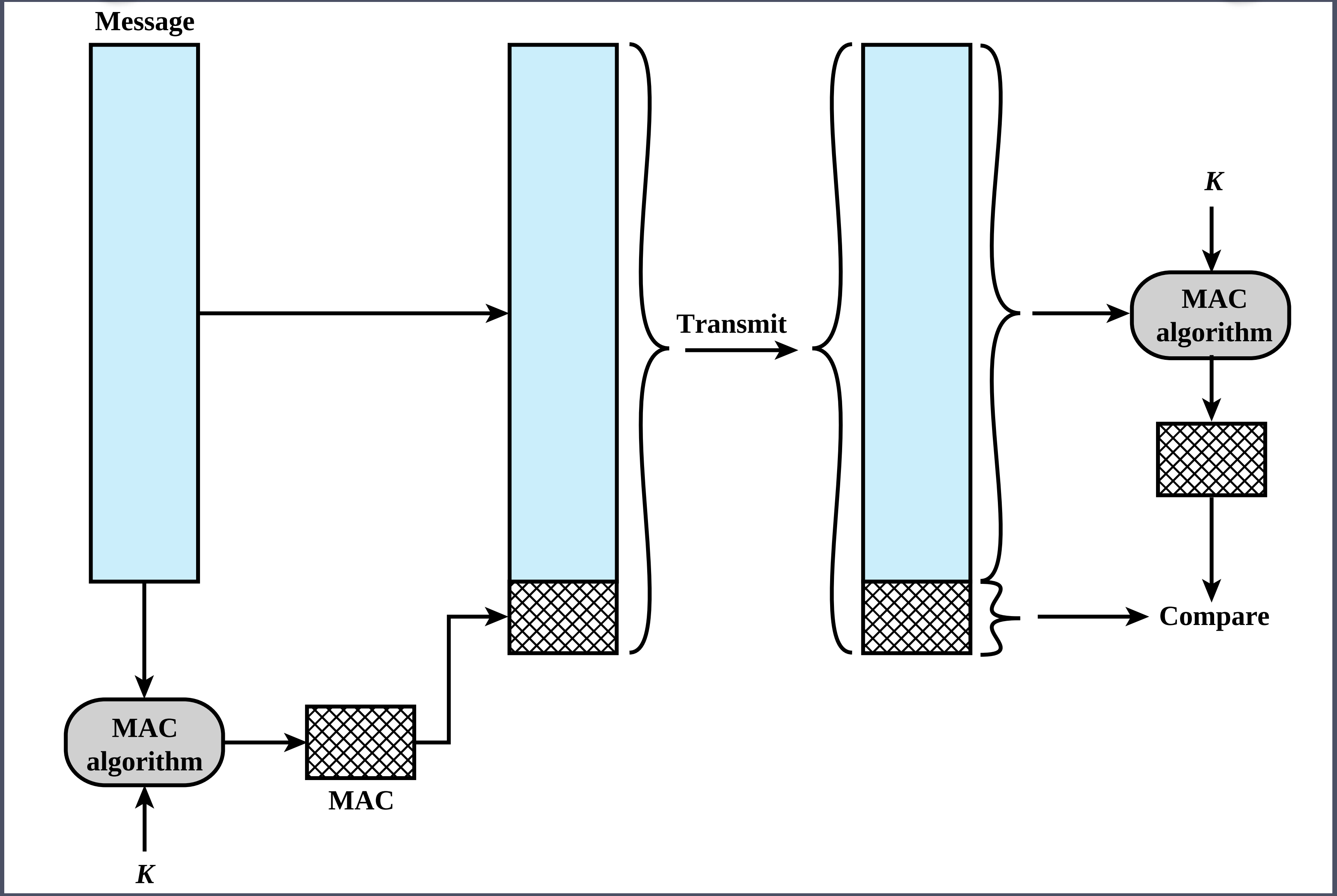
Can use conventional encryption

- Only sender and receiver share a key

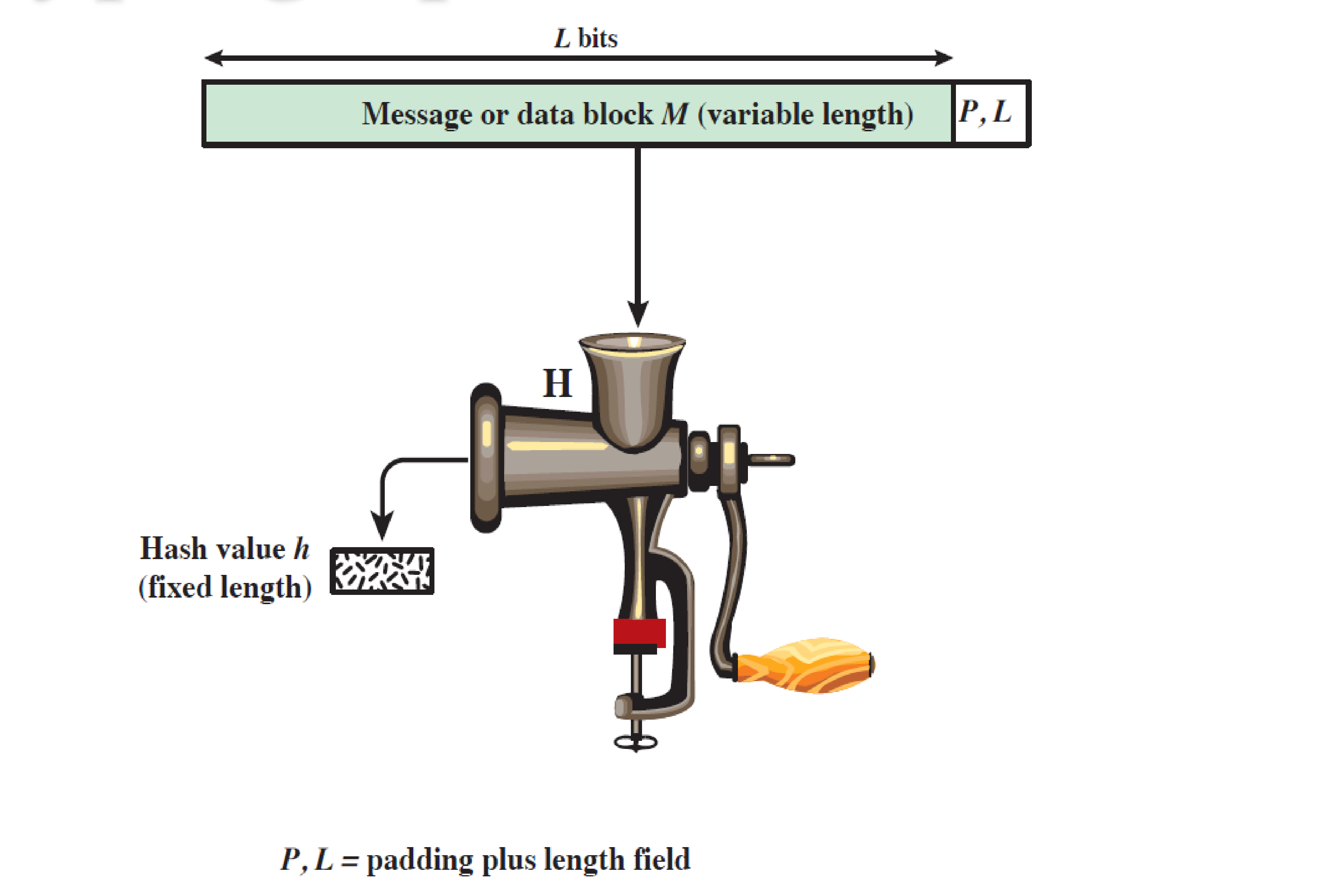
Message Authentication Without Confidentiality

- Message encryption by itself **does not provide** a secure form of authentication
- It is possible to **combine authentication and confidentiality** in a single algorithm by encrypting a message plus its authentication tag
- Typically message authentication is provided as a separate function from message encryption
- Situations in which message authentication without confidentiality may be preferable include:
    - There are a number of applications in which the same message is broadcast to a number of destinations
    - An exchange in which one side has a heavy load and cannot afford the time to decrypt all incoming messages
    - Authentication of a computer program in plaintext is an attractive service
- Thus, there is a place for both authentication and encryption in meeting security requirements

Message Authentication using MAC

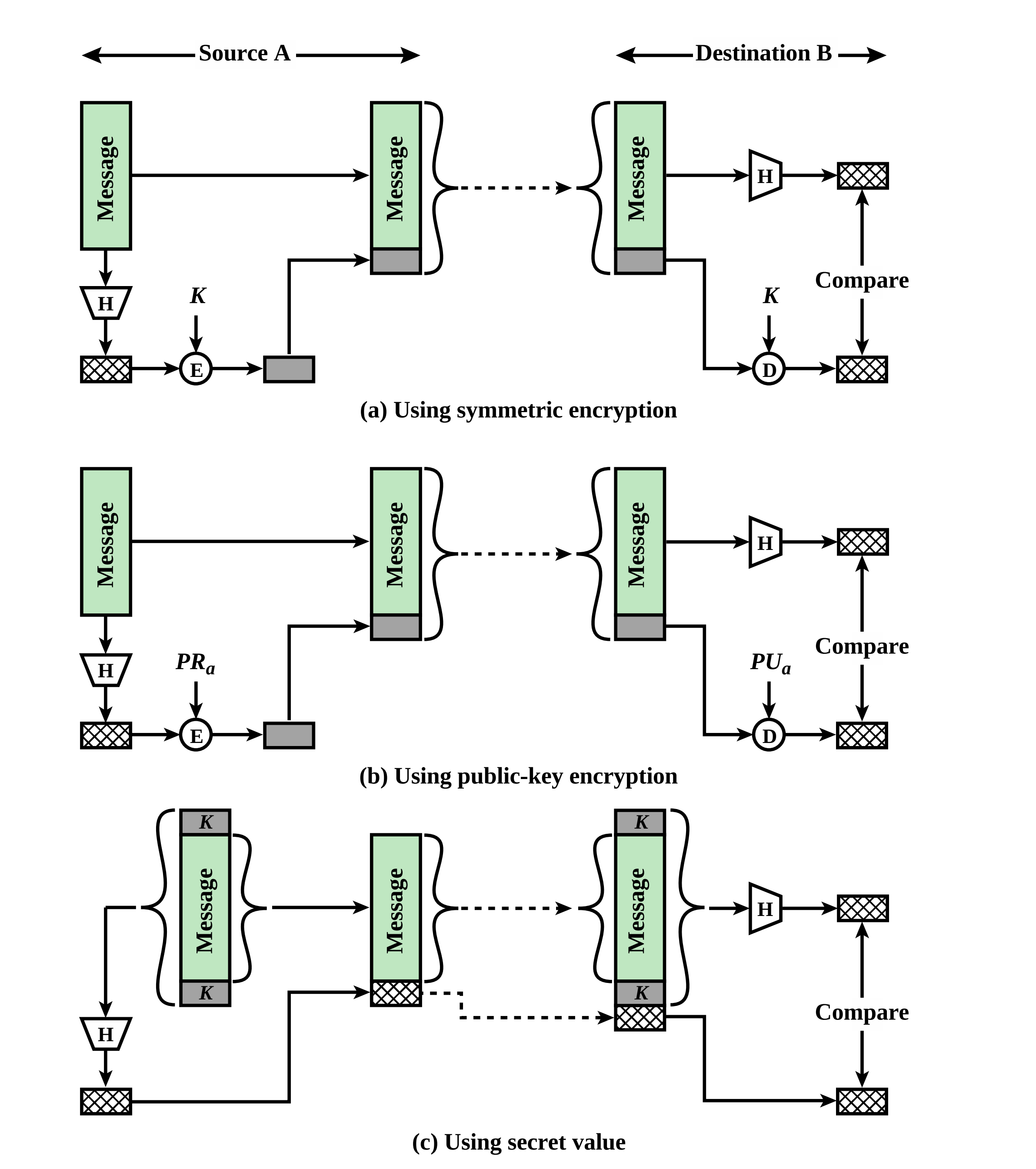


Cryptographic Hash Function



P, *L* = padding plus length field

Message Authentication using One-Way Hash Functions



(a) Using symmetric encryption

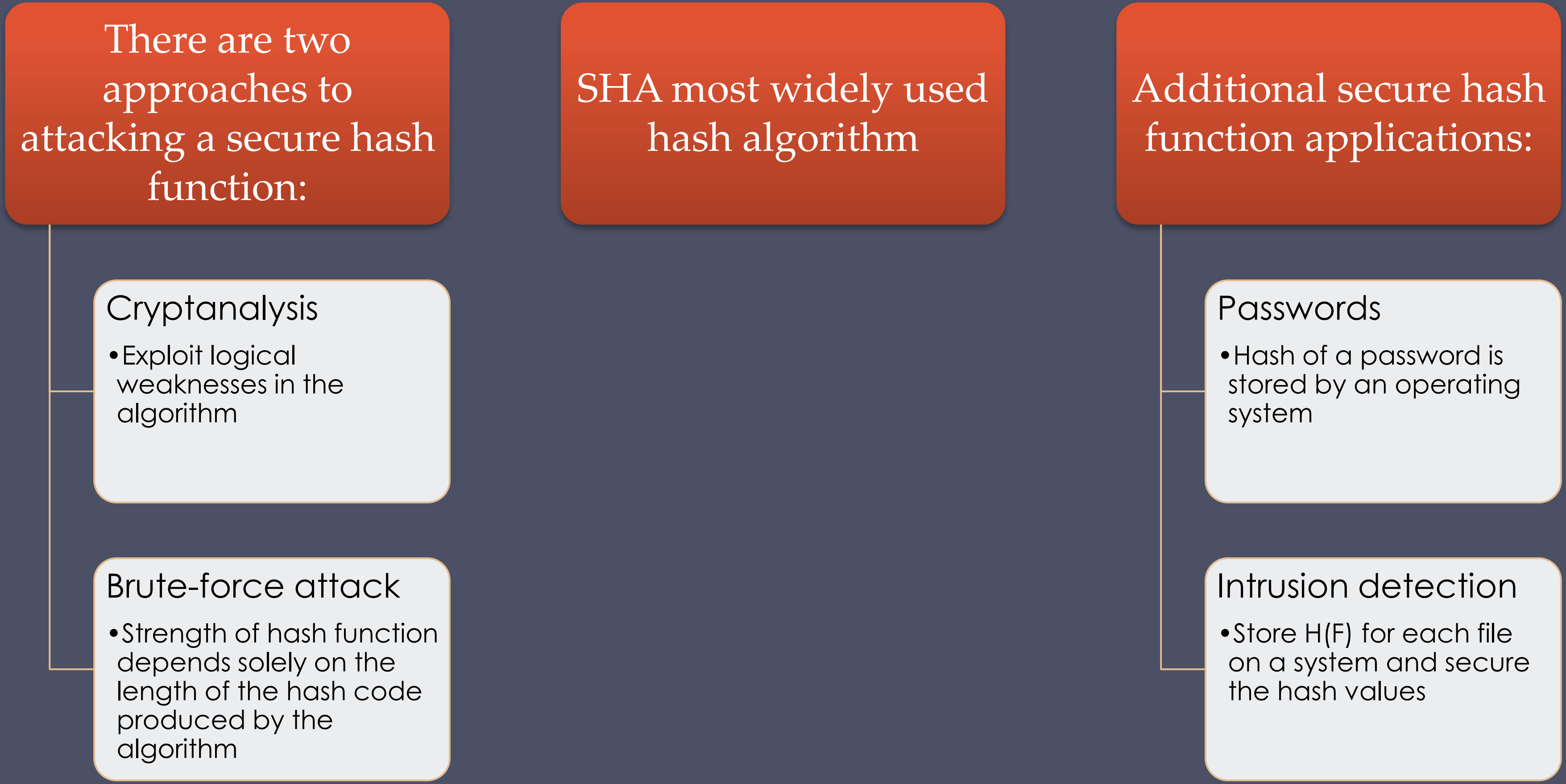
(b) Using public-key encryption

(c) Using secret value

To be useful for message authentication, a hash function H must have the following properties:

- Can be applied to a block of data of any size
- Produces a fixed-length output
- $H(x)$ is relatively easy to compute for any given x
- One-way or pre-image resistant
  - Computationally infeasible to find x such that $H(x) = h$
- Computationally infeasible to find $y \neq x$ such that $H(y) = H(x)$
- Collision resistant or strong collision resistance
  - Computationally infeasible to find any pair (x,y) such that $H(x) = H(y)$

Security of Hash Functions



There are two approaches to attacking a secure hash function:

Cryptanalysis

- Exploit logical weaknesses in the algorithm

Brute-force attack

- Strength of hash function depends solely on the length of the hash code produced by the algorithm

SHA most widely used hash algorithm

Additional secure hash function applications:

Passwords

- Hash of a password is stored by an operating system

Intrusion detection

- Store H(F) for each file on a system and secure the hash values

Conclusion

- Confidentiality with symmetric encryption
  - Symmetric encryption
  - Symmetric block encryption algorithms
  - Stream ciphers
- Message authentication and hash functions
  - Authentication using symmetric encryption
  - Message authentication without message encryption
  - Secure hash functions
  - Other applications of hash functions