Computer Security

Session 3: Cryptographic Tools: Symmetric Encryption

Dr. Fuad A. Ghaleb

Department: Computer Science

School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia

2020-2021 (II)

Cryptographic Tools

1. Confidentiality with Symmetric Encryption
2. Message Authentication and Hash Functions

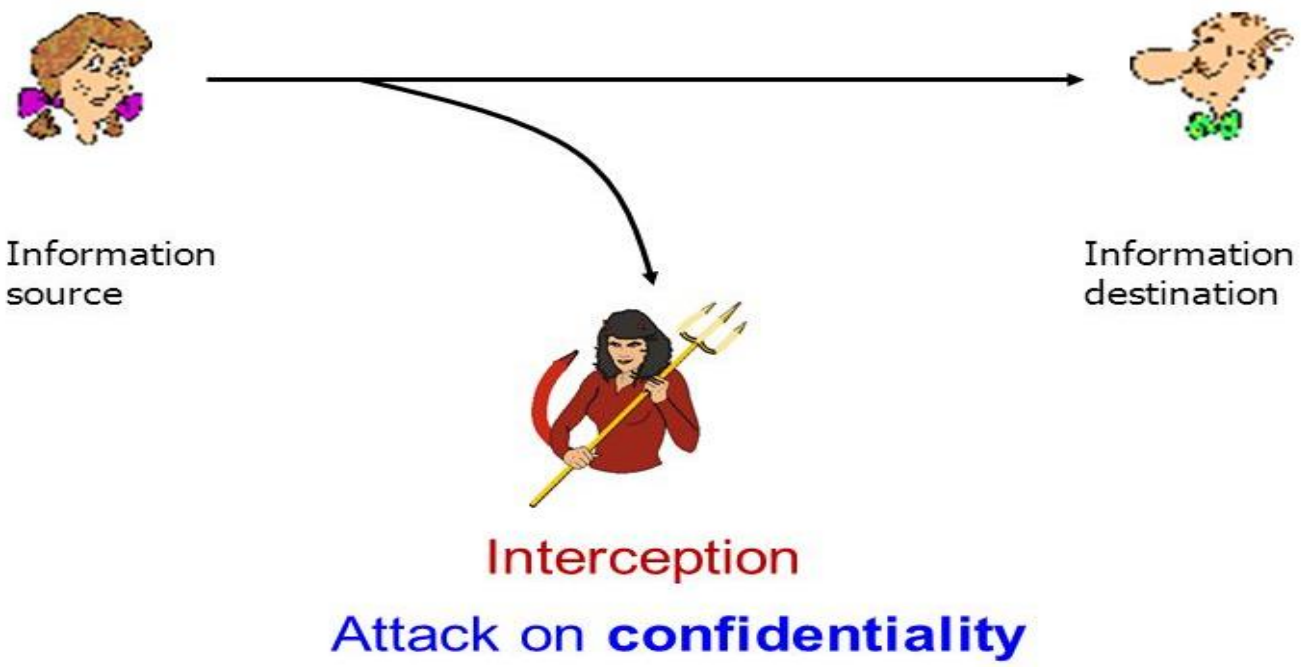
Learning Objectives

After studying this session, you should be able to:

- Explain the basic operation of symmetric block encryption algorithms.
- Compare and contrast block encryption and stream encryption.
- Discuss the use of secure hash functions for message authentication.
- List other applications of secure hash functions.
- Apply Symmetric Encryption Algorithms in many applications

Confidentiality and Privacy Attack

- Encryption protects against passive attack (eavesdropping).

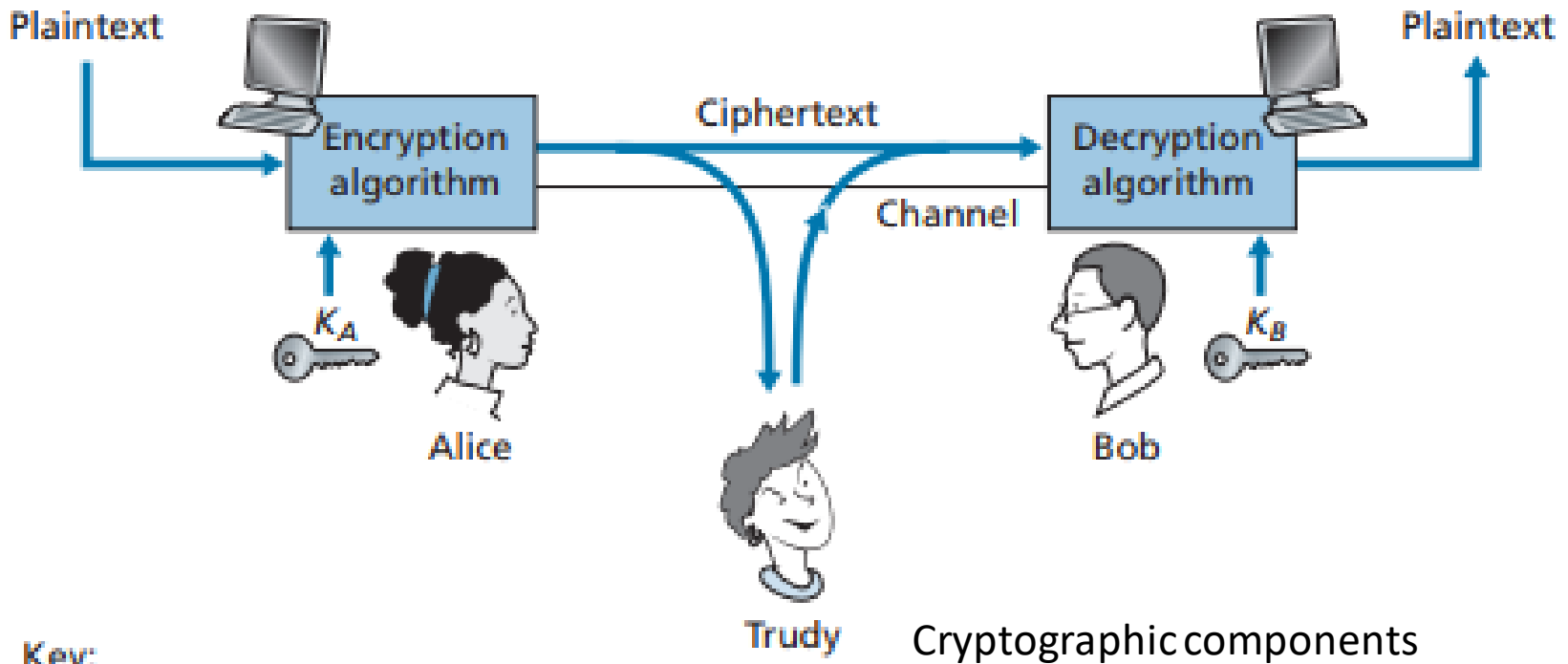


Cryptography

- Confidentiality
- Privacy
- Integrity
- Authenticity
- Non-repudiation

Cryptography

Cryptographic techniques allow a sender to disguise data so that an intruder can gain no information from the intercepted data



Cryptographic components

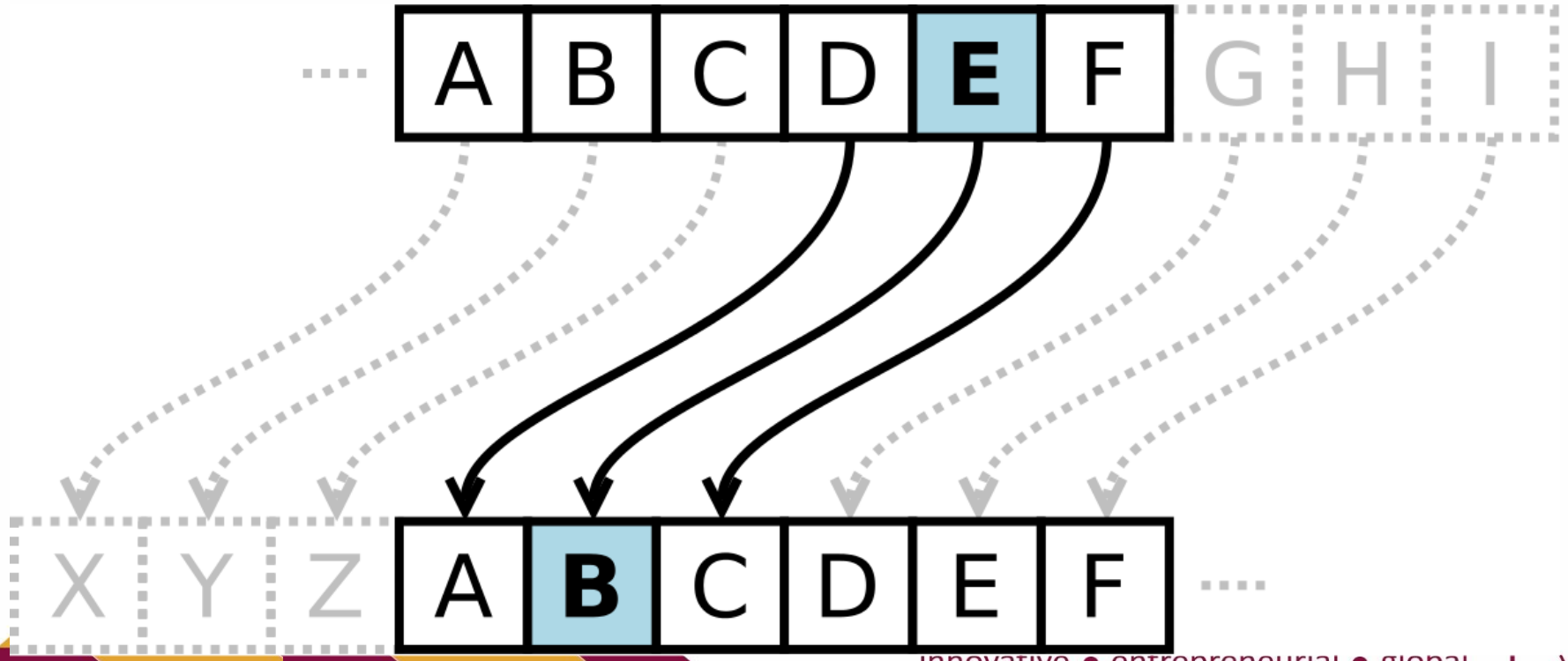
The History of Encryption

The History of Encryption

- Messages must be changed in such a way that they cannot be read easily by any party that intercepts them but can be decoded easily by the intended recipient. A few historical methods of encryption will be examined.
  - The Caesar Cipher
  - ROT 13
  - Multi-Alphabet Substitution
  - Rail Fence
  - Vigenère
  - Enigma

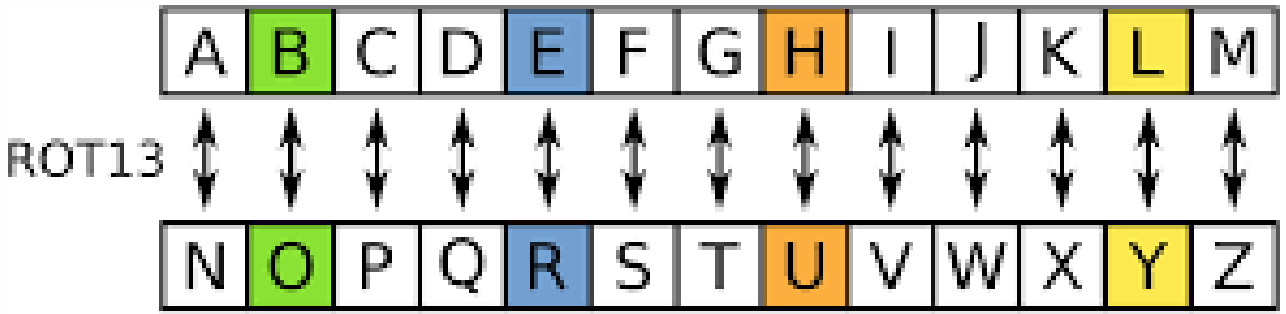
The Caesar Cipher

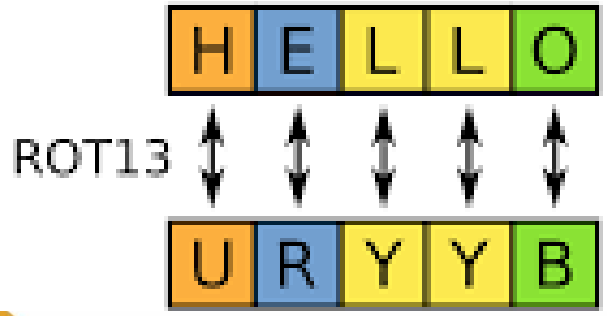
- You choose some number by which to shift each letter of a text.
  - "**A cat**" →shift by two letters→ **"C ecv"**



ROT 13

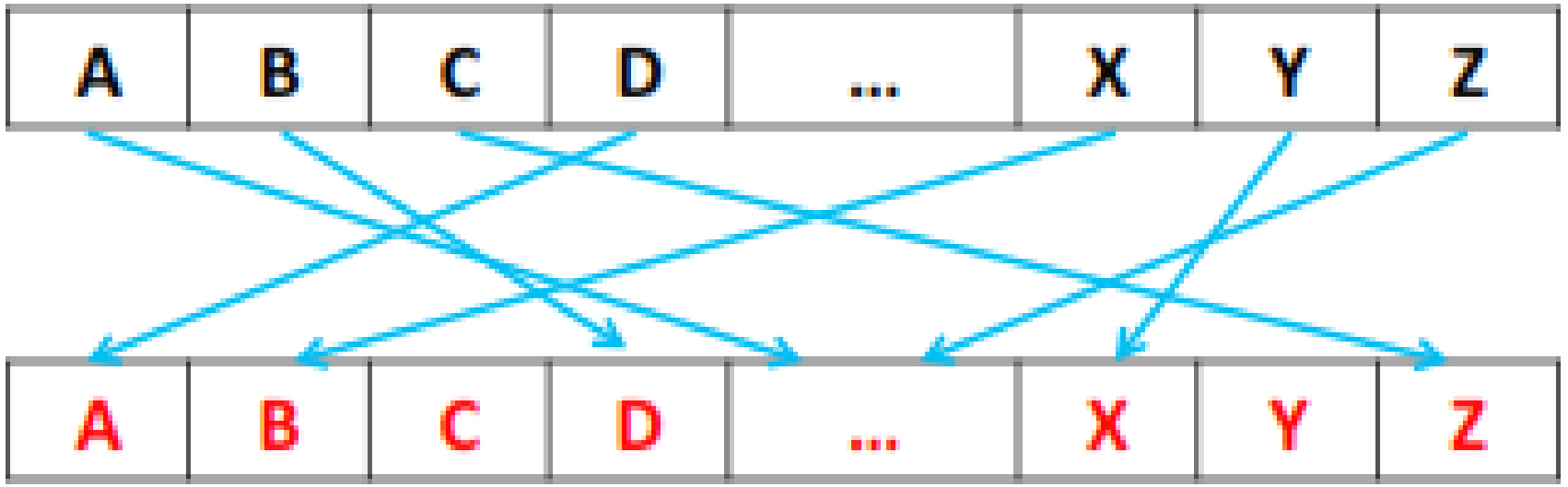
ROT 13 is another single alphabet substitution cipher. All characters are rotated 13 characters through the alphabet. For example the phrase **“A CAT”** will become **“N PNG”**.





Multi-Alphabet Substitution

- Example, if you select three substitution alphabets (12, 22, 13), then **“A CAT”** becomes **“C ADV”.**



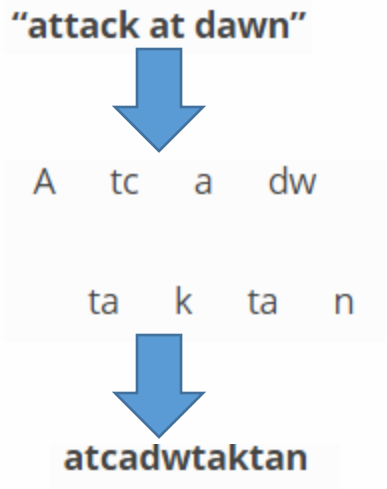
Rail Fence

- The rail fence cipher may be the most widely known transposition cipher. You simply take the message you wish to encrypt and alter each letter on a different row.

Original Message: Hello World

H				o			r			
	e		l			o		l		
		l					W			d

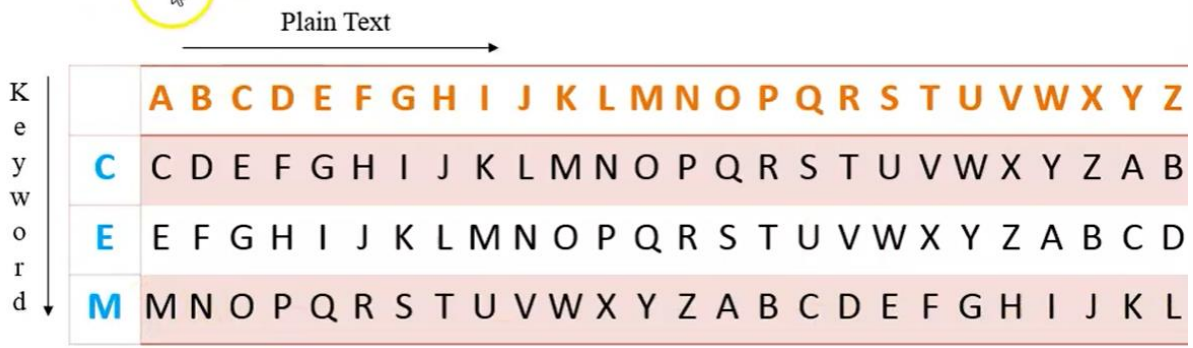
Encrypted Message: Horel ollWd



Vigenère Cipher

For Example,

Keyword: MEC



For Example,

Plain Text: I AM A STUDENT **Keyword: MEC**

Key	M	E	C	M	E	C	M	E	C	M	E
Plain Text	I	A	M	A	S	T	U	D	E	N	T
Cipher Text	U	E	O	M	W	V	G	H	G	Z	X

Modern Encryption Methods

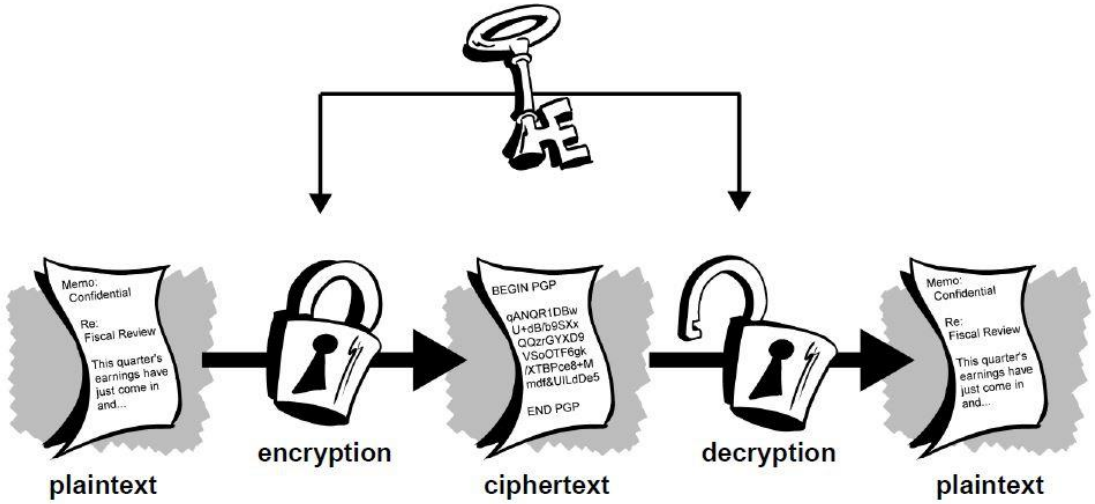
- Number theory forms most of the encryption algorithms.
- Modern encryption algorithm requires a sophisticated understanding of mathematics.
- **Symmetric Encryption**
- **Public Key Encryption: Asymmetric Encryption**

Confidentiality with Symmetric Encryption

Symmetric Encryption

Symmetric Block Encryption Algorithms

Stream Ciphers

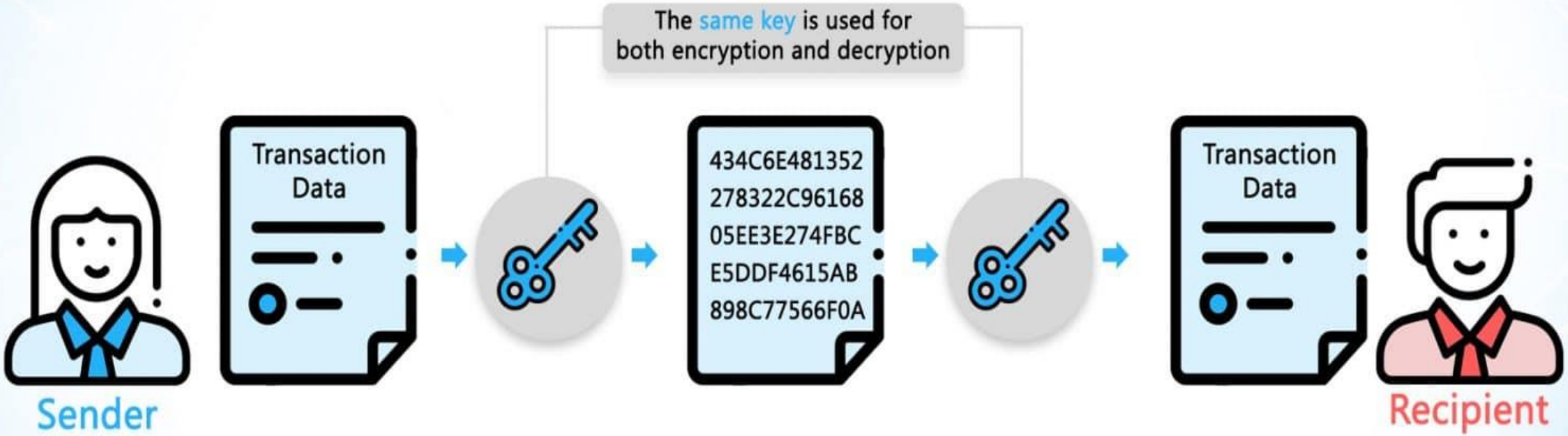


Confidentiality with Symmetric Encryption

- Symmetric Encryption
- Symmetric Block Encryption Algorithms
  - Data Encryption Standard (DES)
  - Triple DES
  - Advanced Encryption Standard (AES)
- Stream Ciphers

Symmetric-Key Cryptography

1 Plain Text — 2 Encryption — 3 Cipher Text — 4 Decryption — 5 Plain Text



Requirements for secure use of symmetric encryption

- The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.
  - The opponent should be unable to figure out the key
  - The opponent should be unable to decipher the ciphertext without the key
- The sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

If someone can discover **the key** and knows **the algorithm**, all communication using this key is readable.

Symmetric Block Encryption Algorithms

- Data Encryption Standard (DES), 1977 , block cipher published by the National Institute of Standards and Technology (NIST).
- Triple DES (3DES), 1985, encrypt–decrypt–encrypt process
- Advanced Encryption Standard (AES), 2001 Rijendael (NIST).

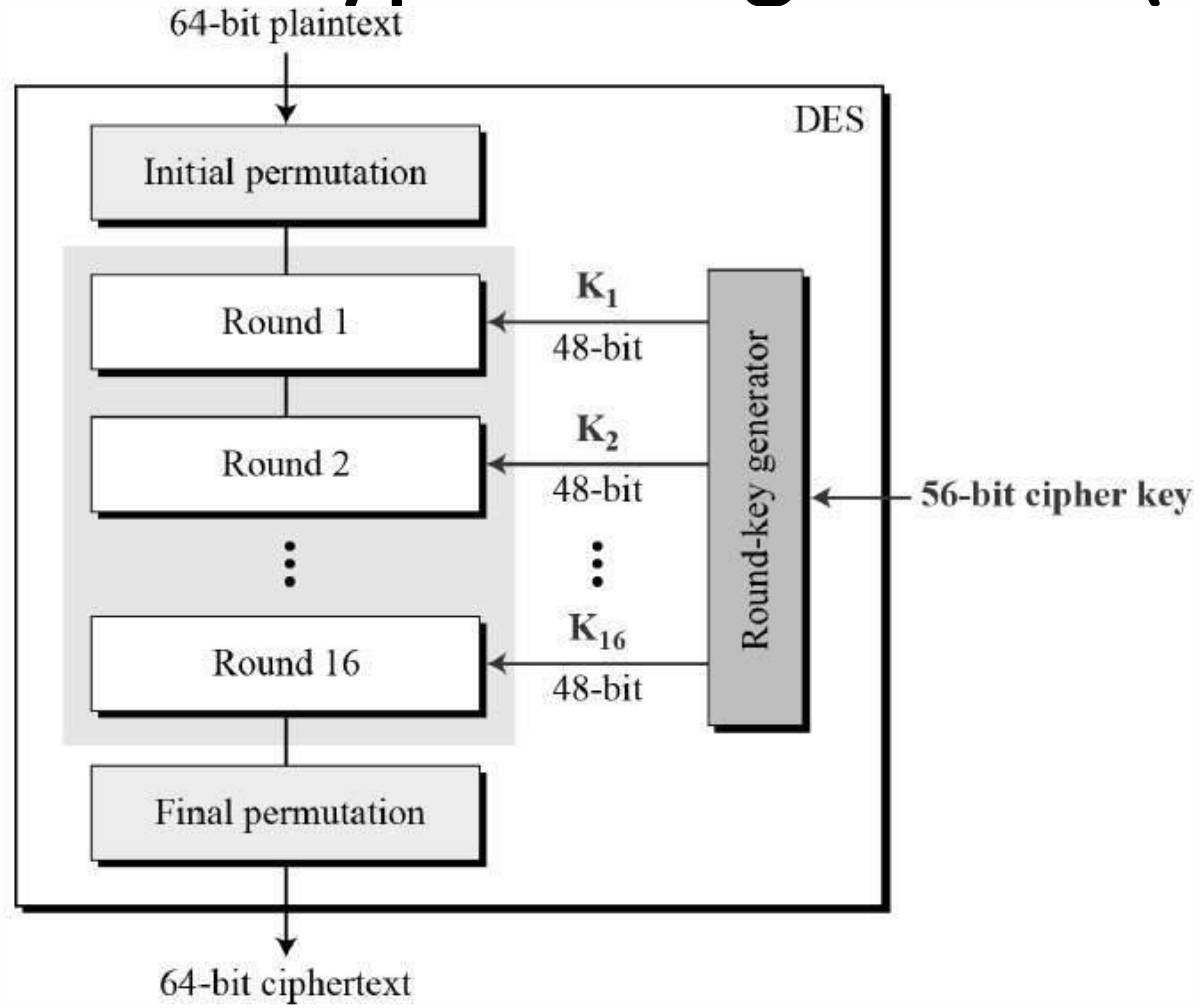
crypto chips

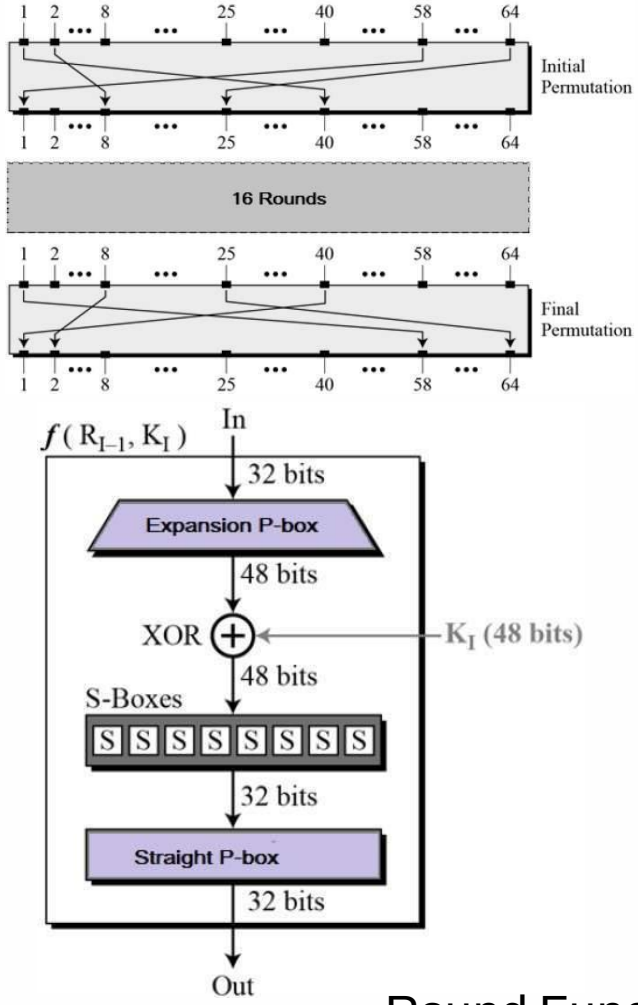
Data Encryption Standard (DES)

- The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted in **1977** by NIST
- Data Encryption Algorithm (DEA or DES algorithm) takes a plaintext block of **64 bits** and a key of **56 bits**, to produce a ciphertext block of 64 bits.
- Concerns about the strength of DES fall into two categories:
  - concerns about the algorithm itself,
  - concerns about the use of a 56-bit key.
- Today's **supercomputers** should be able to find a key in about an hour.

vulnerable against exhaustive key search attack

Data Encryption Algorithm (DEA)





Round Function

Attacking a Symmetric Encryption Scheme

There are two general approaches to attacking a symmetric encryption scheme.

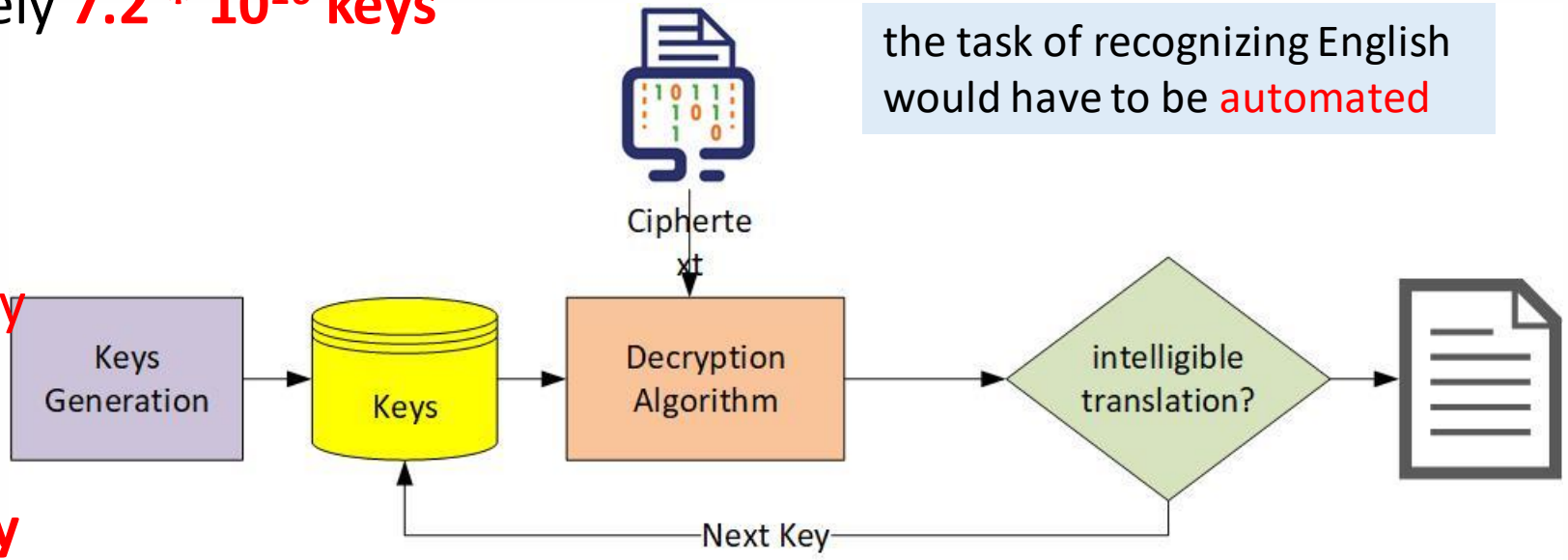
- **Cryptanalysis**: exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
  - knowledge of the encryption algorithm
  - knowledge of plaintext-ciphertext pairs
- **Brute-force attack**: is to try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained

Brute-force attack

With a key length of 56 bits, there are **2^{56}** possible keys, which is approximately **$7.2 * 10^{16}$ keys**

the task of recognizing English would have to be automated

OLD Multicore computers
can try one billion (10^9) key combinations per second



$7.2 * 10^7$ second = 834 Day

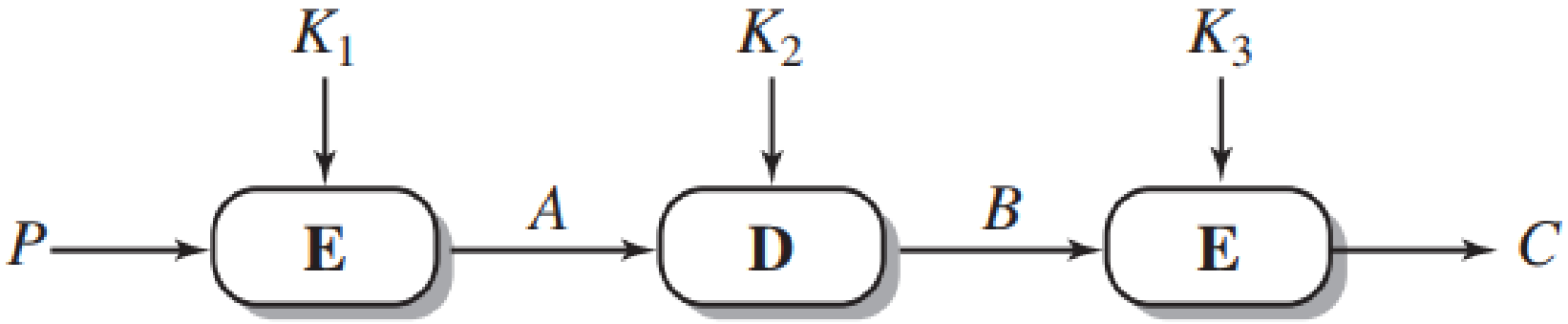
with contemporary **supercomputer** technology, a rate of **10^{13} encryptions/s** is reasonable

Triple DES

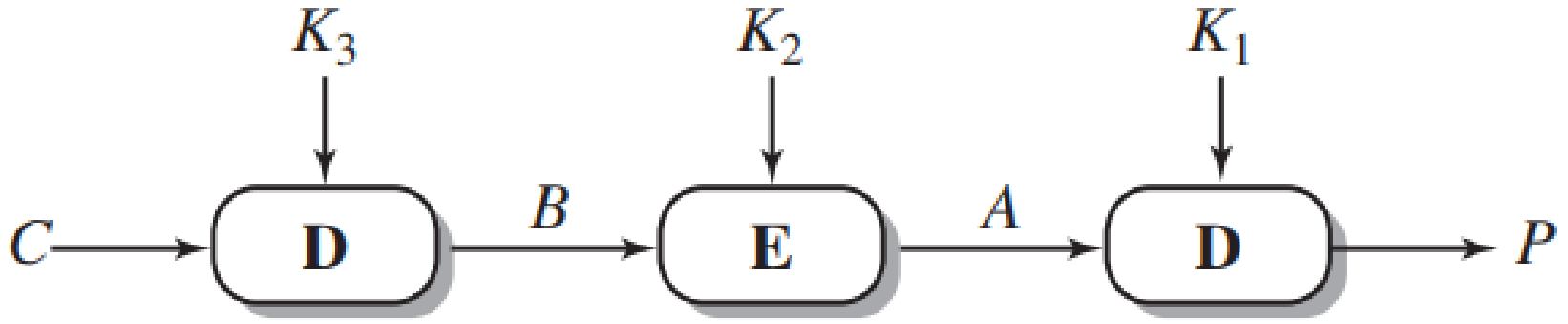
- Triple DES (3DES) was first standardized for use in financial applications in ANSI standard X9.17 in 1985
- The life of DES was extended by the use of triple DES (3DES), which involves repeating the basic DES algorithm three times, using either two or three unique keys, for a key size of 112 or **168 bits=56x3**.
  - With its 168-bit key length, it overcomes the vulnerability to brute-force attack of DES.
  - The underlying encryption algorithm in 3DES is the same as in DES.
- 3DES is very resistant to cryptanalysis.
- The main drawback is that 3DES is relatively sluggish in software (slow).
- A secondary drawback is that both DES and 3DES use a 64-bit block size.

Triple DES

What will be the result if K1=K2=K3?

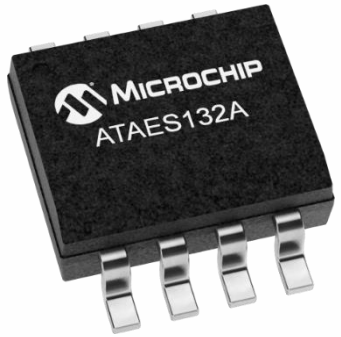


(a) Encryption



(b) Decryption

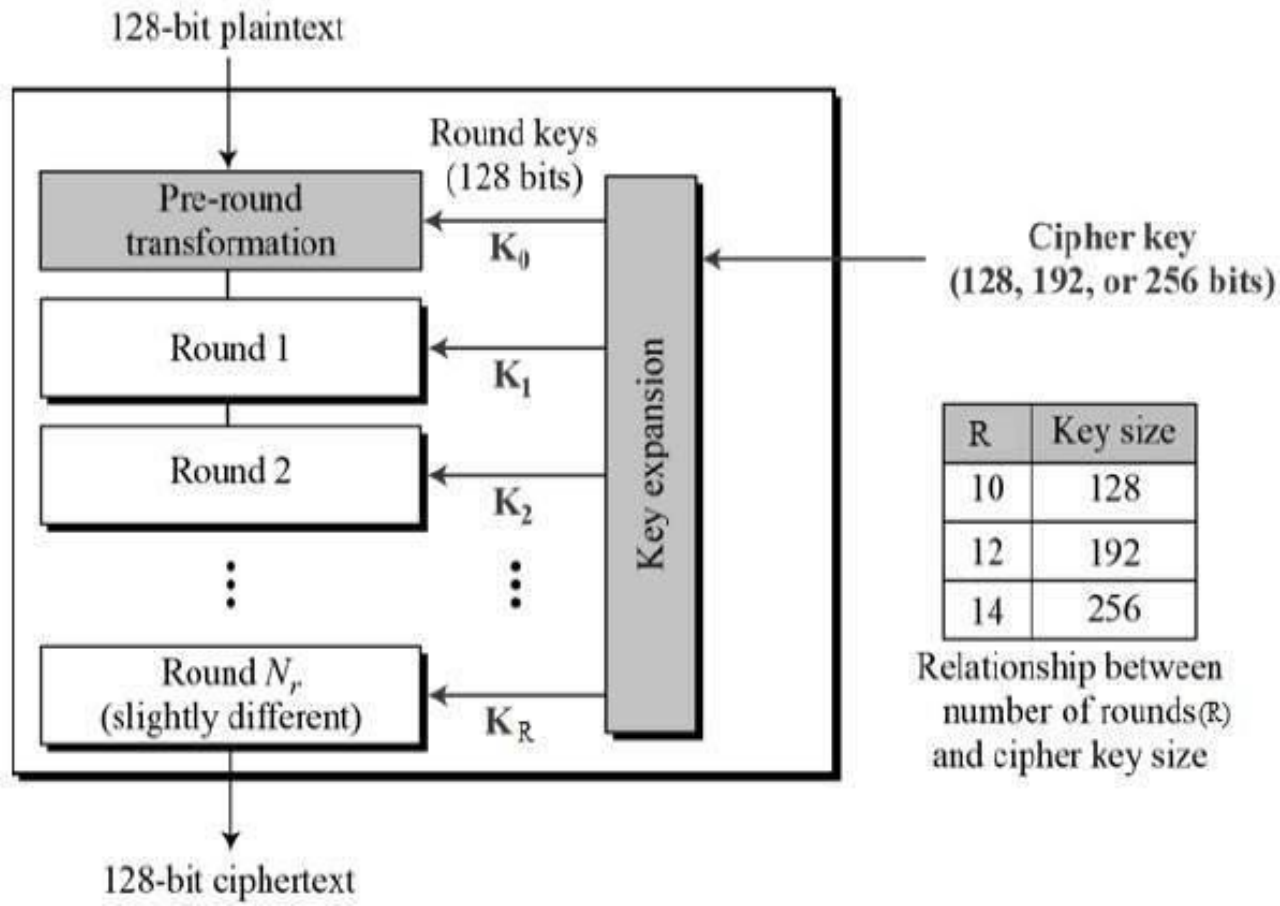
Advanced Encryption Standard (AES):



- Advanced Encryption Standard issued as a federal information processing standard FIPS 197 (November 2001).
- AES is intended to replace 3DES, **six time** faster than triple DES.
- Block length of 128 bits and a key length that can be 128, 192, or 256 bits.
- Evaluation criteria included security, computational efficiency, memory requirements, hardware and software suitability, and flexibility.
- AES algorithm designed by Rijndael.

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

Advanced Encryption Standard (AES)



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

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

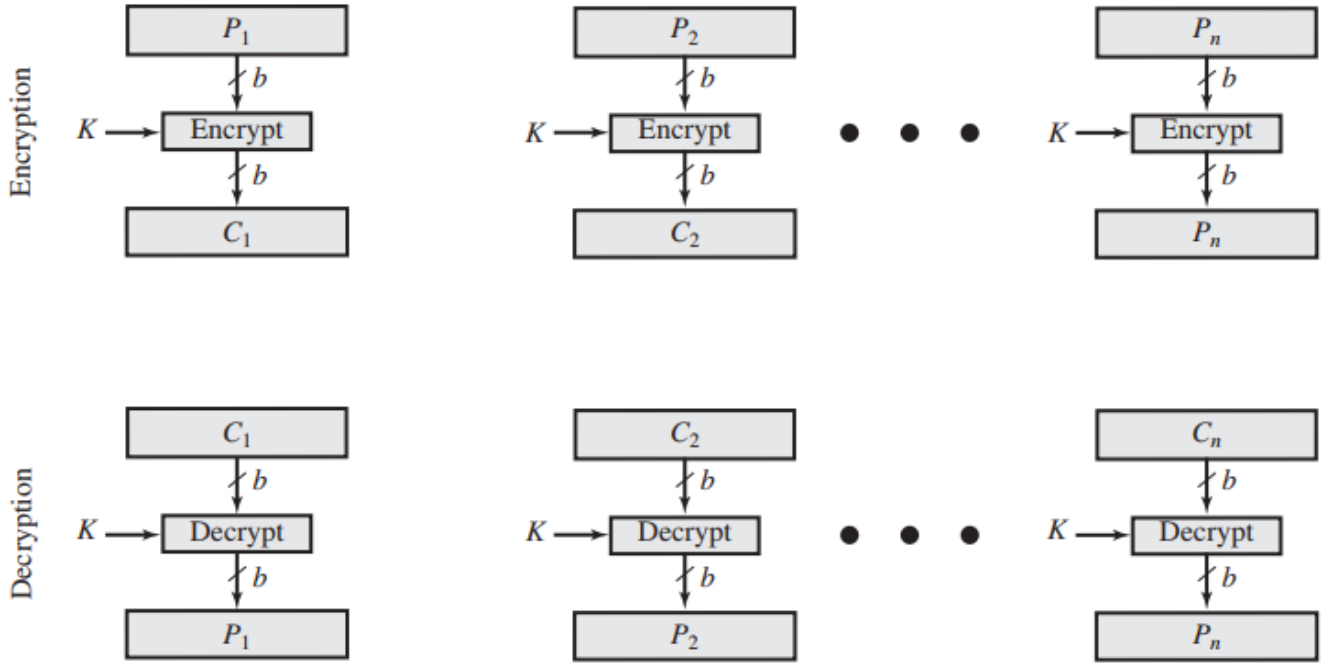
Average Time Required for Exhaustive Key Search

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

Practical Security Issues

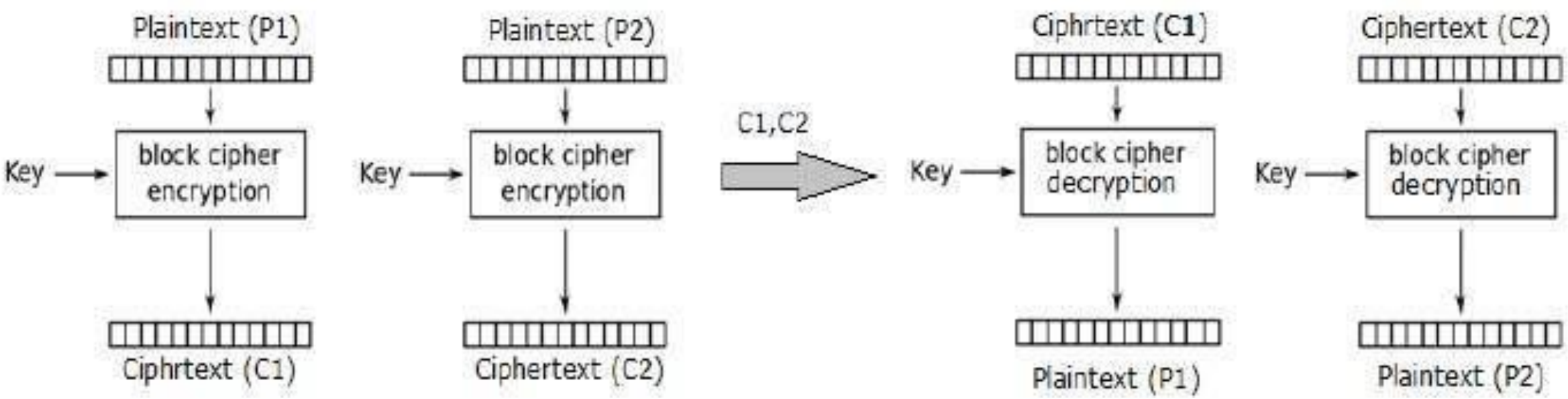
- Symmetric encryption is applied to a unit of data larger than a **single 64-bit or 128-bit block.**
- E-mail messages, network packets, database records, and other plaintext sources must be **broken up into a series of fixed- length block** for encryption by a symmetric block cipher.
- The simplest approach to multiple-block encryption is known as electronic code book (ECB) mode.

Real-time Applications (Data Streams)



Electronic Code Book (ECB) Mode

- This mode is a most straightforward way of processing a series of sequentially listed message blocks.

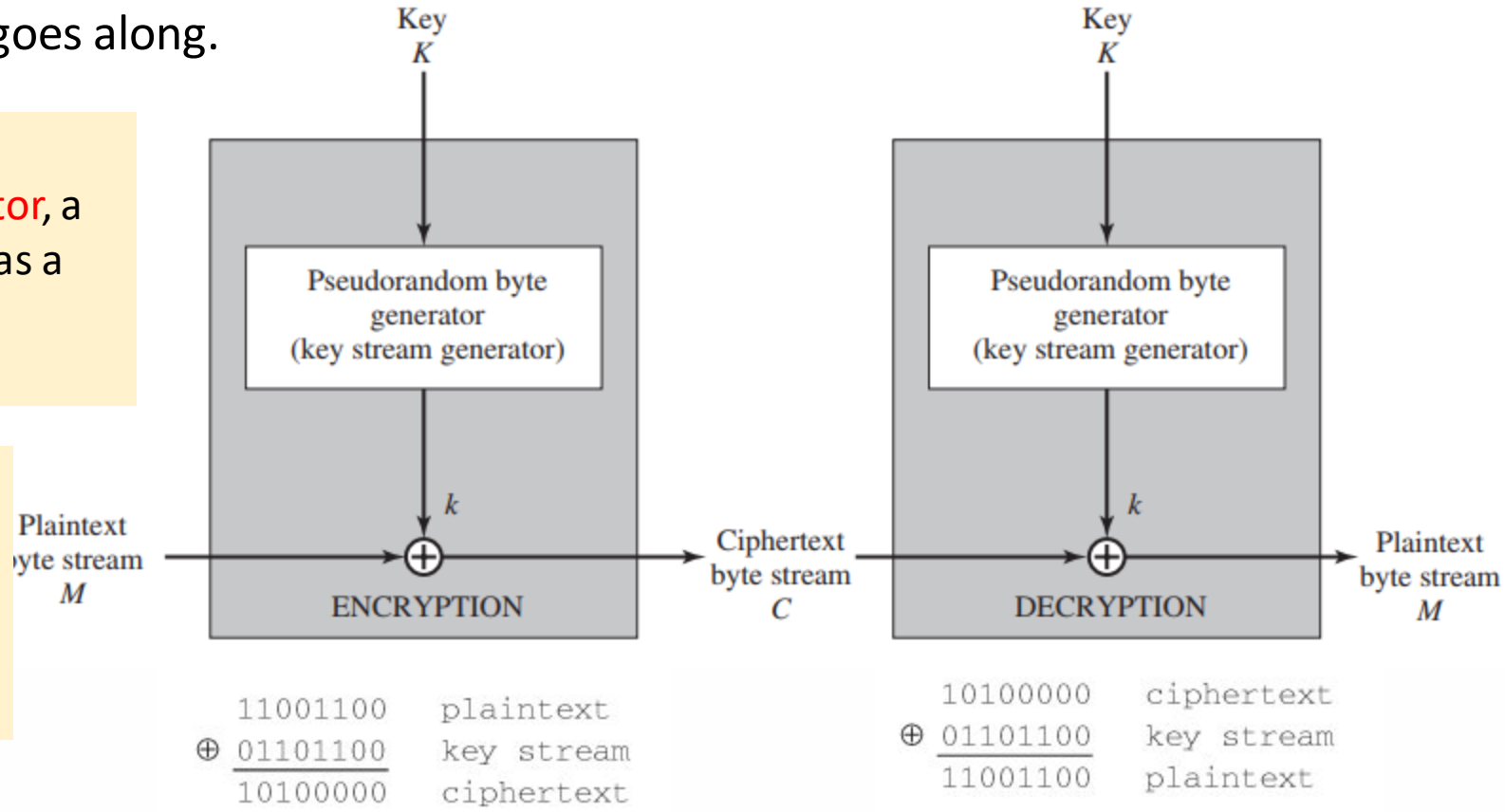


Stream Ciphers

A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

With a properly designed pseudorandom number generator, a stream cipher can be as secure as a block cipher of comparable key length.

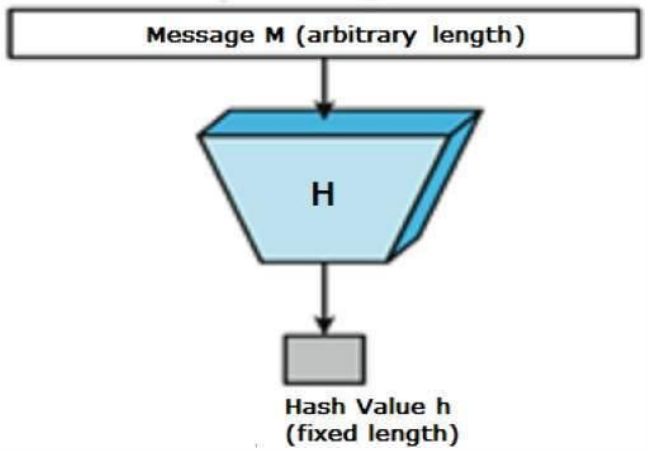
The primary advantage of a stream cipher is that stream ciphers are almost always faster and use far less code than do block ciphers.



Lab Activity 1: Symmetric Key Encryption

- Write a short message
- Create random Key and share it with your selected friend
- Use one of the following online tool to create a ciphertext
  - https://codebeautify.org/encrypt-decrypt
  - https://the-x.cn/en-us/cryptography/TripleDes.aspx
- Share the ciphertext with your classmate (using WhatsApp or e-mail
- Ask your friend to decrypt the ciphertext using the shared key

Message Authentication and Hash Functions

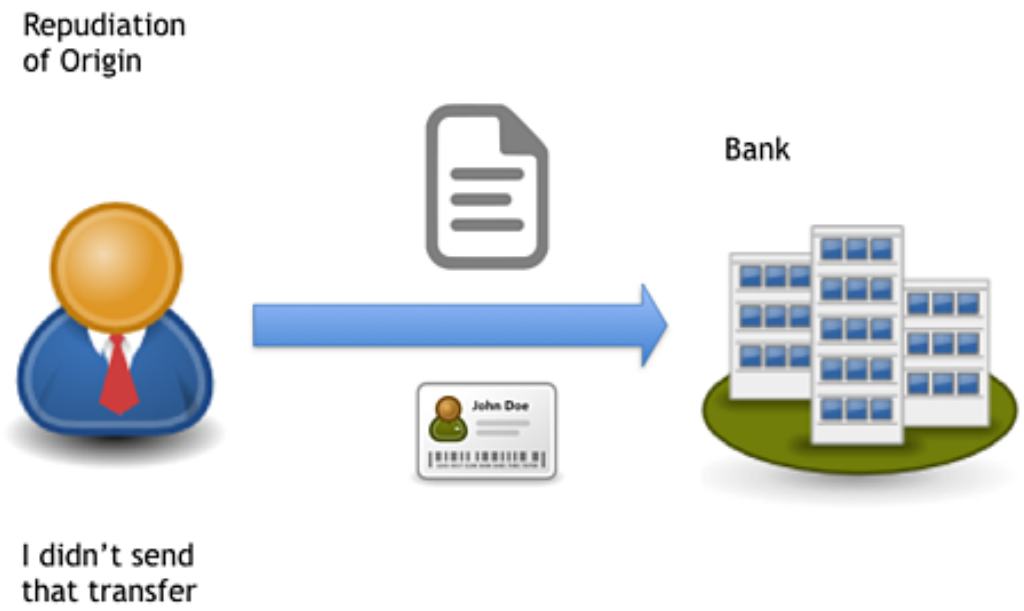


Integrity Attack

Masquerading Attack

Falsification Attack

Authenticity Attack

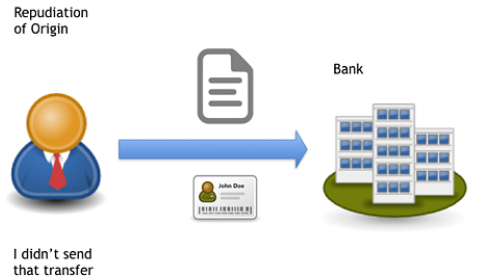


Message Authentication

- Encryption protects against passive attack (eavesdropping).
- Message Authentication Protecting against active attack (Integrity Attack)
  - Falsification Attack
  - Authenticity Attack
  - Repudiation Problem
- Data or Content Integrity and Message Origin (Authenticity)

Message Authentication and Hash Functions

- Authentication Using Symmetric Encryption
- Message Authentication without Message Encryption
  - Message Authentication Code
  - One-way Hash Function
- Secure Hash Functions
  - Hash Function Requirements
  - Security of Hash Functions
  - Secure Hash Function Algorithms
- Other Applications of Hash Functions
  - Passwords
  - Intrusion detection
  - Cryptocurrency



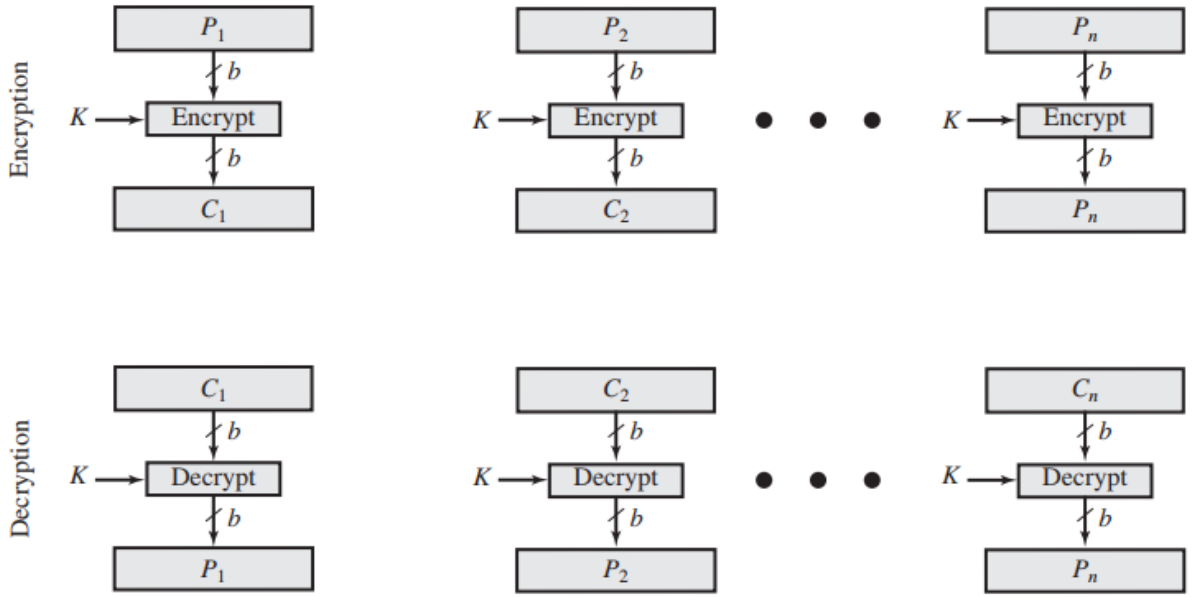
Message Authentication and Hash Functions

- **Message or data authentication is used to** protect against active attack (falsification of data and transactions). Data Integrity
- A message, file, document, or other collection of data is said to be authentic when it is genuine and came from its alleged source.
- Message or data authentication is a procedure that allows communicating parties to verify that received or stored messages are authentic.
- The two important aspects are to verify that the contents of the message have not been altered and that the source is authentic.

Authentication Using Symmetric Encryption

- If we assume that only the sender and receiver share a key (which is as it should be), then only the genuine **sender would be able to encrypt a message successfully for the other participant**, provided the **receiver can recognize a valid message**.

In the ECB mode of encryption, if an attacker reorders the blocks of ciphertext, then each block will still decrypt successfully.



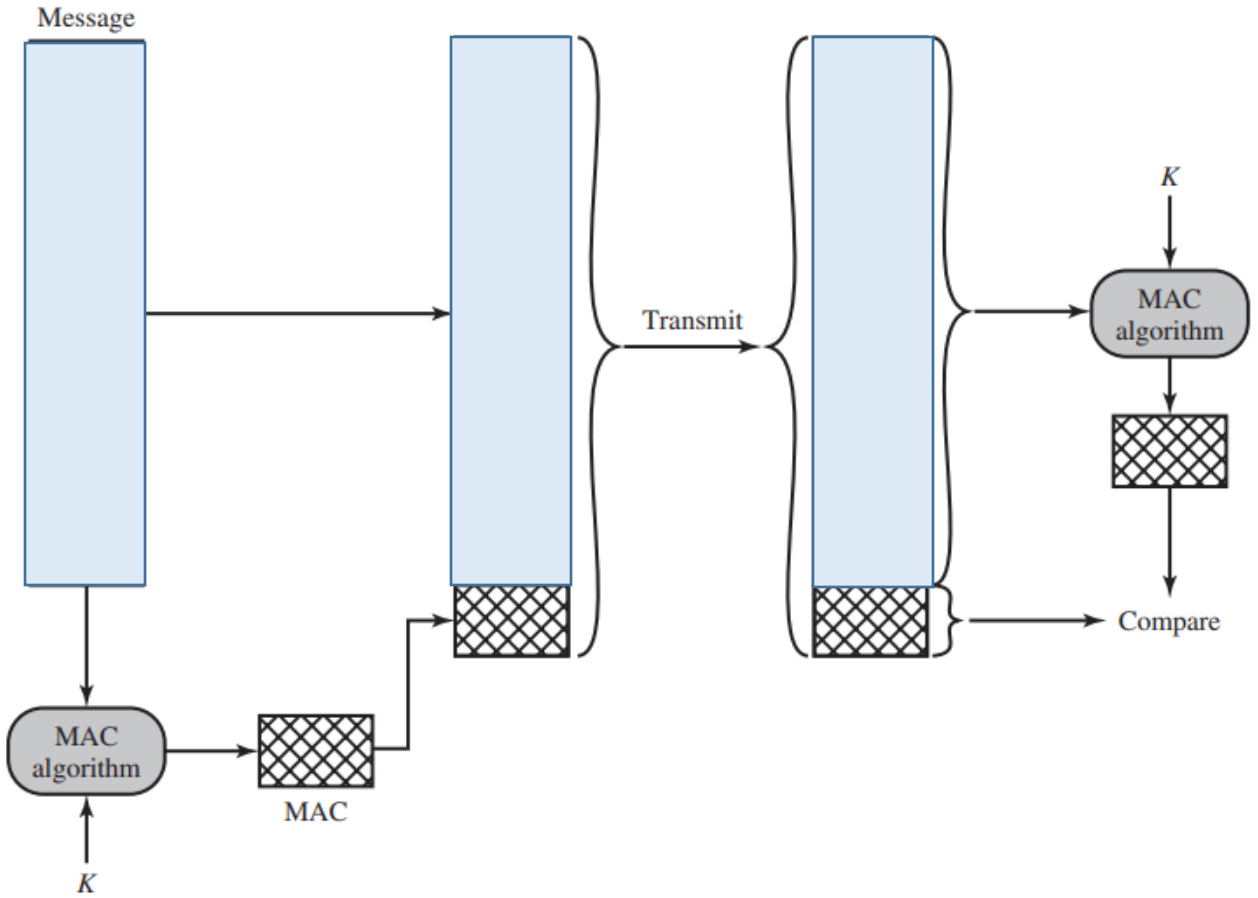
Message Authentication without Message Encryption

- An **authentication tag** is generated and appended to each message for transmission.
  - Message Origin? Message Authentication
  - Is the message altered? Data Integrity
- Why Message Authentication without Message Encryption?
  - Broadcast a Non-Confidential Data – Message Integrity Important
  - Random Checking for the Speed
  - Processor resources (**authentication tag** smaller than the size of the message)
- Message authentication can be achieved using:
  - Message Authentication Code
  - One-way Hash Function

Message Authentication Code (MAC)

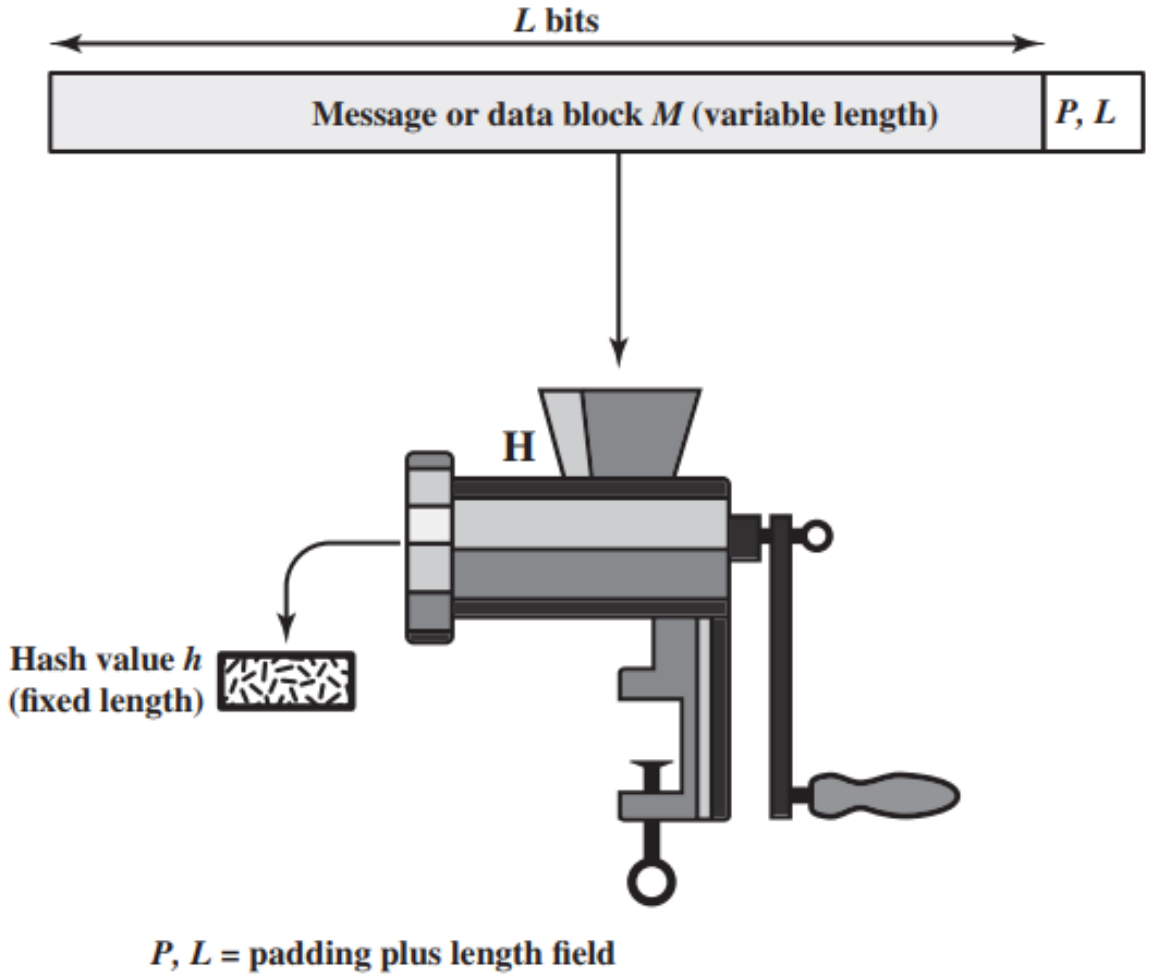
1. Use the MAC algorithm and shared K between user A and B to generate the MAC.
2. Append the MAC to the message and send it to B.
3. User B uses the MAC algorithm and shared K to generate a new MAC
4. User B compares the created MAC with the one created by user A.

- If an attacker alters the message but does not alter the code, then the receiver's calculation of the code will differ from the received code. If it matches, the receiver is assured that the message is from the alleged sender.



One-way Hash Function

- A hash function accepts a variable-size message M as input and produces a **fixed-size message** digest H(M) as output.
- Unlike the MAC, a hash function does not take a secret key as input.



Features of Hash Functions

- **Fixed Length Output (Hash Value)**
  - Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as **hashing the data**.
  - In general, the hash is much smaller than the input data, hence hash functions are sometimes called **compression functions**.
  - Since a hash is a smaller representation of a larger data, it is also referred to as a **digest**.
  - Hash function with n bit output is referred to as an **n-bit hash function**. Popular hash functions generate values between 160 and 512 bits.
- **Efficiency of Operation**
  - Generally for any hash function h with input x, computation of h(x) is a fast operation.
  - Computationally hash functions are much faster than a symmetric encryption.

Properties of Secure Hash Functions

- **Pre-Image Resistance**
  - it should be computationally hard to reverse a hash function.
  - if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z.
- **Second Pre-Image Resistance**
  - given an input and its hash, it should be hard to find a different input with the same hash.
  - if a hash function h for an input x produces hash value h(x), then it should be difficult to find any other input value y such that h(y) = h(x).
- **Collision Resistance**
  - it should be hard to find two different inputs of any length that result in the same hash.
  - for a hash function h, it is hard to find any two different inputs x and y such that h(x) = h(y).

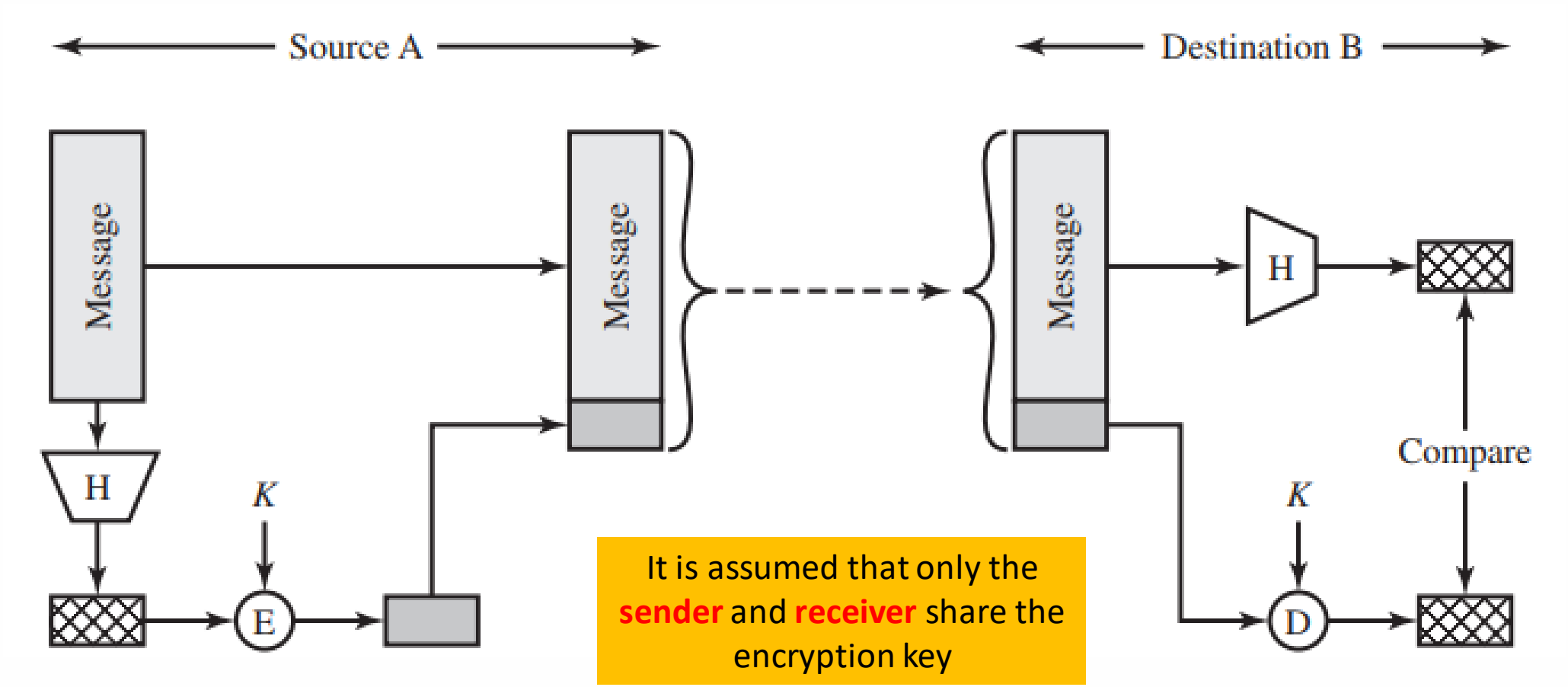
Popular Hash Functions

- Message Digest (MD)
  - MD5 was most popular and widely used hash function for quite some years.
  - The MD family comprises of hash functions MD2, MD4, MD5 and MD6. It was adopted as Internet Standard RFC 1321. It is a 128-bit hash function.
- Secure Hash Function (SHA), SHA-1, SHA-2, and SHA-3
- RIPEMD
- Whirlpool - This is a 512-bit hash function.

Secure Hash Function Algorithms

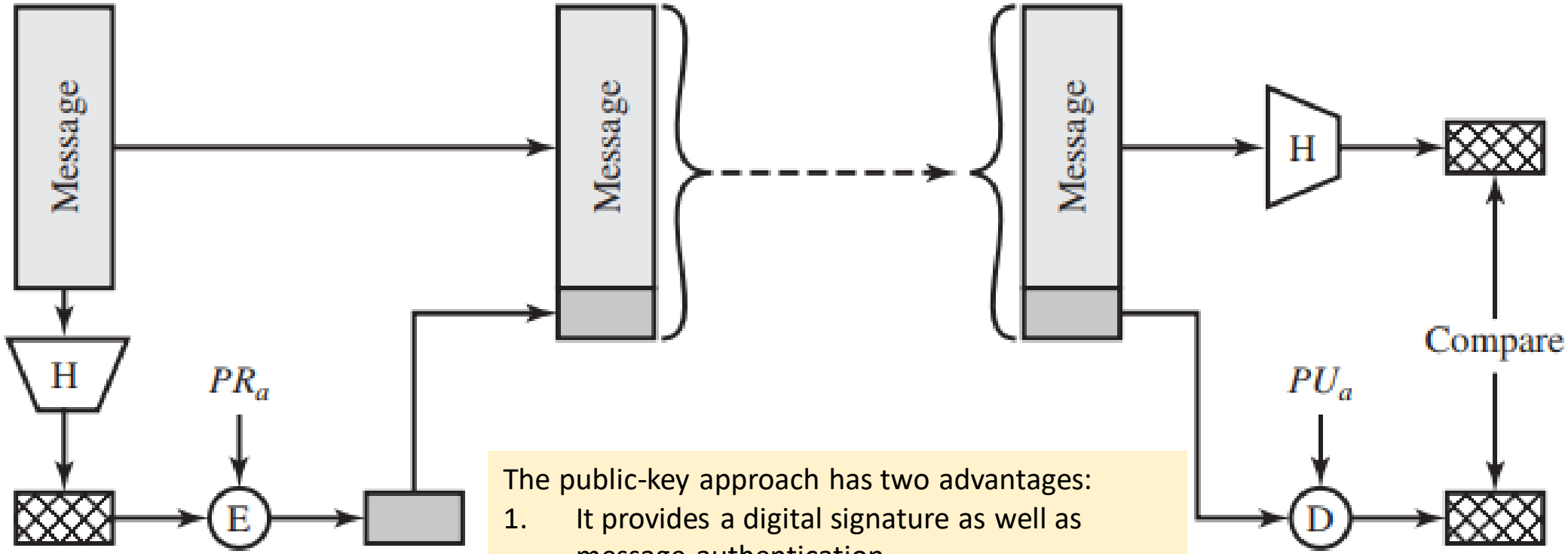
- Secure Hash Algorithm (SHA) – created by NIST published as FIPS 180 in 1993.
- SHA-1 **FIPS 180-1 in 1995- produces a hash value of 160 bits.**
- SHA-2 (SHA-**256,** SHA-**384, and** SHA-**512) by** NIST published as **FIPS 180-2 in 2002, (256, 384, and 512 bits)**
- SHA-3, NIST decided to standardize a new hash function that is very different from SHA-2 and SHA-1. SHA-3 was published in 2015 and is now available as an alternative to SHA-2.

Message Authentication Using a One-Way Hash Function - with Symmetric Encryption



It is assumed that only the **sender** and **receiver** share the encryption key

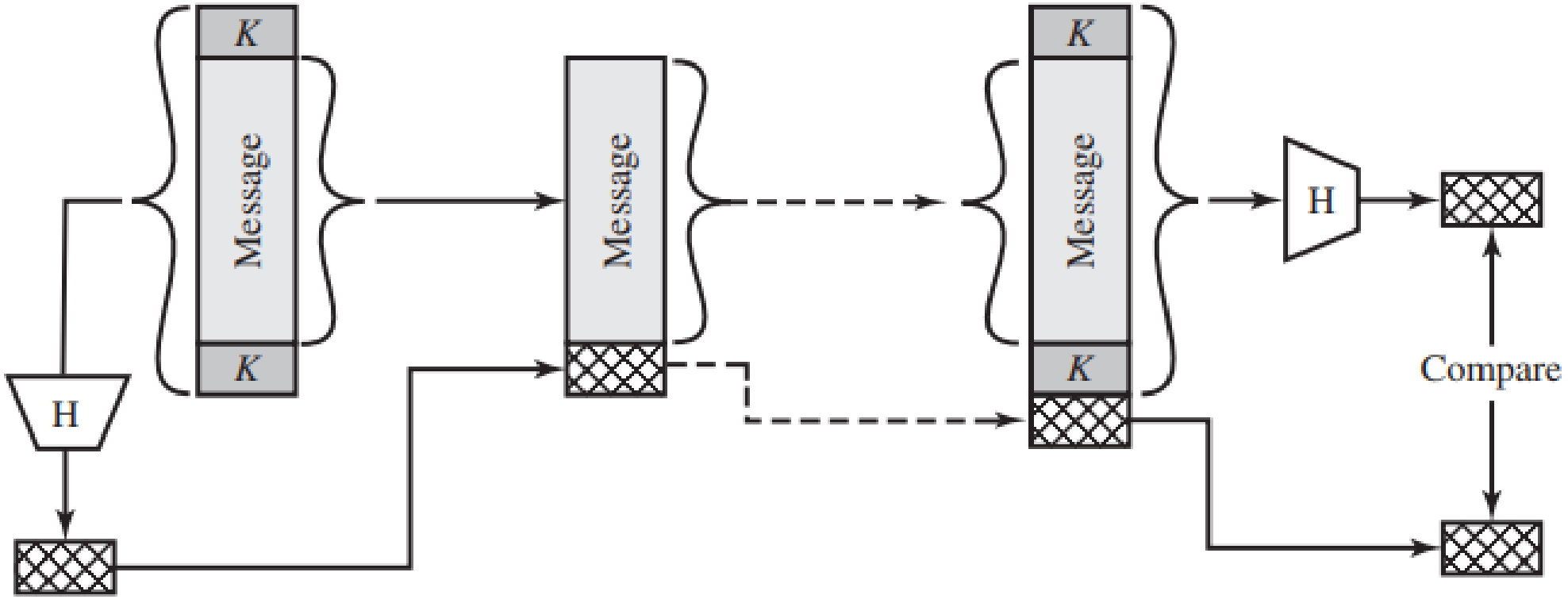
Message Authentication Using a One-Way Hash Function - with public-key encryption



The public-key approach has two advantages:

1. It provides a digital signature as well as message authentication,
2. it does not require the distribution of keys to communicating parties.

Message Authentication Using a One-Way Hash Function - with secret value



Avoids encryption of the whole messages

- Encryption software is quite slow.
- Encryption hardware costs are nonnegligible. Low-cost chip implementations of DES and AES are available, but the cost adds up if all nodes in a network must have this capability.
- Encryption hardware is optimized toward large data sizes.
- An encryption algorithm may be protected by a patent.

Secure Hash Functions

- The one-way hash function, or secure hash function, is important not only in message authentication but also in digital signatures.
- A hash function H must have the following properties:
  1. H can be applied to a block of data of any size.
  2. H produces a fixed-length output.
  3. H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
  4. For any given code h, it is computationally infeasible to find x such that H(x) = h. **one-way** or **preimage resistant.** It is easy to generate a code given a message, but virtually impossible to generate a message given a code.
  5. For any given block x, it is computationally infeasible to find $y \neq x$ with H(y) = H(x). **second preimage resistant** or **weak collision resistant.** It is impossible to find an alternative message with the same hash value as a given message.
  6. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y). **collision resistant** or **strong collision resistant**.

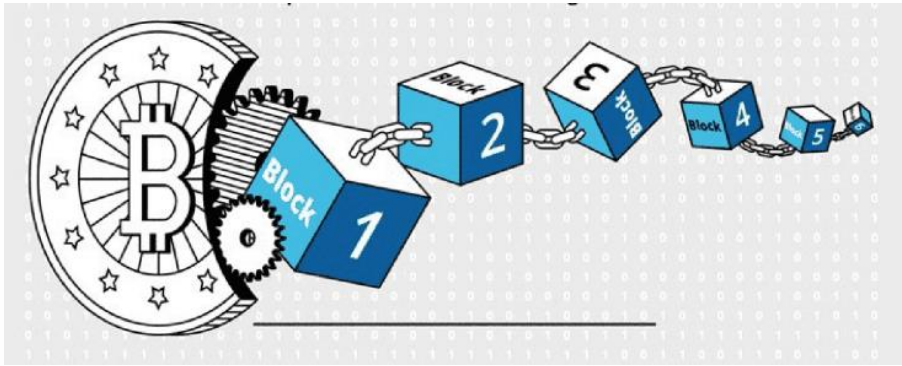
Security Of Hash Functions

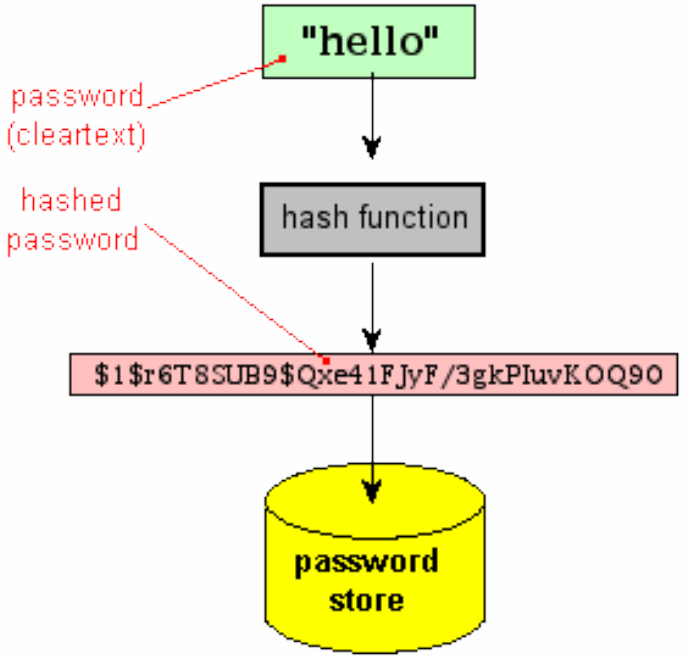
- Cryptanalysis involves exploiting logical weaknesses in the algorithm.
- Brute-force attack.
  - The strength of a hash function against brute-force attacks depends solely on the length of the hash code produced by the algorithm

Preimage resistant	2^n
Second preimage resistant	2^n
Collision resistant	$2^{n/2}$

Applications of Hash Functions

- Authenticity
- Digital Signature
- Block Chain
- Data Integrity
- Data Integrity Check
- Passwords Protection
- Intrusion Detection (Attack Signature)
- Anti-Virus/Anti-Malware or Malware Detection (File Signature)





Lab Activity 2: Using Hash Functions

- Use the following online md5 hash tool, https://www.md5hashgenerator.com/, to generate the hashes of the following:
  1. "The quick brown fox."
  2. "The quick brown fax."
- compare the MD5 hash values generated from each of the two sentences

Next Session

- Cryptographic Tools: Asymmetric Encryption