INFORMATION ASSURANCE and Security Module 1

Engr. Dennis S. Tibe, MIT, PCpE

The Security Problem in Computing

1.1 The Meaning of Computer Security

- The meaning of the term computer security has evolved in recent years. Before the problem of data security became widely publicized in the media, most people's idea of computer security focused on the physical machine.

The Security Problem in Computing

1.1 The Meaning of Computer Security

3 main reasons why computer facilities are being protected ;

- To prevent theft or of damage to the hardware
- To prevent theft of or damage to the information
- To prevent disruption of service

The Security Problem in Computing

1.1 The Meaning of Computer Security

- **Computer security** is security applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the whole Internet.

The Security Problem in Computing

1.1 The Meaning of Computer Security

- The field covers all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction, and are of growing importance in line with the increasing reliance on computer systems of most societies worldwide.

The Security Problem in Computing

1.1 The Meaning of Computer Security

- It includes physical security to prevent theft of equipment, and information security to protect the data on that equipment. It is sometimes referred to as "cyber security" or "IT security", though these terms generally do not refer to physical security (locks and such).

The Security Problem in Computing

1.1 The Meaning of Computer Security

Important terms used in computer security ;

1. Vulnerability
2. Backdoors
3. Denial-of-service attack
4. Direct Access Attack
5. Eavesdropping

The Security Problem in Computing

1.1 The Meaning of Computer Security

Important terms used in computer security ;

6. Spoofing
7. Tampering
8. Repudiation
9. Information Disclosure
10. Elevation of Privilege

The Security Problem in Computing

1.1 The Meaning of Computer Security

Important terms used in computer security ;

11. Exploits
12. Indirect Attacks
13. Computer Crime

The Security Problem in Computing

1.1 The Meaning of Computer Security

- **Vulnerability** is a weakness which allows an attacker to reduce a system's information assurance. **Vulnerability** is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

The Security Problem in Computing

1.1 The Meaning of Computer Security

- To exploit **vulnerability**, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.

The Security Problem in Computing

1.1 The Meaning of Computer Security

- A **backdoor** in a computer system, is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected.

The Security Problem in Computing

1.1 The Meaning of Computer Security

- Unlike other exploits, **denials-of-service attacks** are not used to gain unauthorized access or control of a system. They are instead designed to render it unusable. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once.

The Security Problem in Computing

1.1 The Meaning of Computer Security

- **Direct-access attack**. An unauthorized user gaining physical access to a computer (or part thereof) can perform many functions, install different types of devices to compromise security, including operating system modifications, software worms, key loggers, and covert listening devices.

The Security Problem in Computing

1.1 The Meaning of Computer Security

- **Eavesdropping** is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, programs such as Carnivore and Narus Insight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers.

The Security Problem in Computing

1.1 The Meaning of Computer Security

- **Spoofing** of user identity describes a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

The Security Problem in Computing

1.1 The Meaning of Computer Security

- **Tampering** describes an intentional modification of products in a way that would make them harmful to the consumer.
- **Repudiation** describes a situation where the authenticity of a signature is being challenged.

The Security Problem in Computing

1.1 The Meaning of Computer Security

- **Information Disclosure** (Privacy breach or Data leak) describes a situation where information, thought as secure, is released in an untrusted environment.
- **Elevation of Privilege** describes a situation where a person or a program want to gain elevated privileges or access to resources that are normally restricted to him/it.

The Security Problem in Computing

1.1 The Meaning of Computer Security

- An **exploit** is a piece of software, a chunk of data, or sequence of commands that takes advantage of a software "bug" or "glitch" in order to cause unintended or unanticipated behaviour to occur on computer software, hardware, or something electronic (usually computerized).

The Security Problem in Computing

1.1 The Meaning of Computer Security

- An indirect attack is an attack launched by a third-party computer. By using someone else's computer to launch an attack, it becomes far more difficult to track down the actual attacker. There have also been cases where attackers took advantage of public anonymizing systems, such as the tor onion router system.

The Security Problem in Computing

1.1 The Meaning of Computer Security

- **Computer crime:** Computer crime refers to any crime that involves a computer and a network.

The Security Problem in Computing

1.2 Top 10 Cyber Crime Prevention Tips

1. **Use Strong Passwords**

   Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

The Security Problem in Computing

1.2 Top 10 Cyber Crime Prevention Tips

2. Secure your computer

o **Activate your firewall** Firewalls are the first line of cyber defense; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.

The Security Problem in Computing

1.2 Top 10 Cyber Crime Prevention Tips

2. Secure your computer

- **Use anti-virus/malware software** Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.

The Security Problem in Computing

1.2 Top 10 Cyber Crime Prevention Tips

2. Secure your computer

- **Block spyware attacks** Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.

The Security Problem in Computing

1.2 Top 10 Cyber Crime Prevention Tips

3. Be Social-Media Savvy

Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!

The Security Problem in Computing

1.2 Top 10 Cyber Crime Prevention Tips

4. Secure your Mobile Devices

Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

The Security Problem in Computing

1.2 Top 10 Cyber Crime Prevention Tips

5. Install the latest operating system updates

Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

The Security Problem in Computing

1.2 Top 10 Cyber Crime Prevention Tips

6. Protect your Data

Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location.

The Security Problem in Computing

1.2 Top 10 Cyber Crime Prevention Tips

7. **Secure your wireless network**

   Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. “Hot Spots”, are also vulnerable. Avoid conducting financial or corporate transactions on these networks

The Security Problem in Computing

1.2 Top 10 Cyber Crime Prevention Tips

8. Protect your e-identity

Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g. online purchases) or privacy settings are enabled (e.g. accessing/using social networking sites).

The Security Problem in Computing

1.2 Top 10 Cyber Crime Prevention Tips

9. Avoid being scammed

Always think before you click on a link or file of unknown origin. Don’t feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.

The Security Problem in Computing

1.2 Top 10 Cyber Crime Prevention Tips

Top 10 Cyber Crime Prevention Tips

10. Call the right person for help

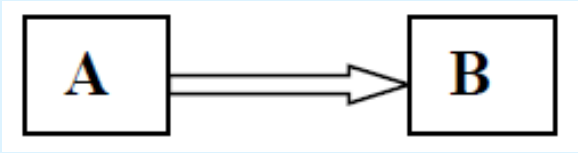
Don’t panic! If you are a victim, if you encounter illegal Internet content (e.g. child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician.

The Security Problem in Computing

1.3 Principles of Security

1. ***Confidentiality:***

   The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the content of the message.

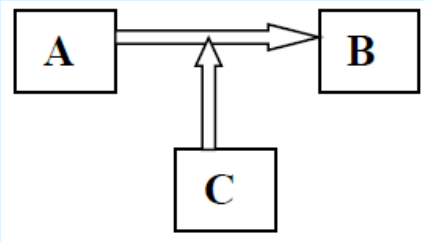


The Security Problem in Computing

1.3 Principles of Security

2. ***Integrity:***

   The confidential information sent by A to B which is accessed by C without the permission or knowledge of A and B.



1.3 Principles of Security

3. Authentication:

Authentication mechanism helps in establishing proof of identification.

1.3 Principles of Security

4. ***Access Control:***

   Access control specifies and control who can access what.

1.3 Principles of Security

5. Availability:

It means that assets are accessible to authorized parties at appropriate times.

The Security Problem in Computing

1.3 Attacks

We want our security system to make sure that no data are disclosed to unauthorized parties.

- Data should not be modified in illegitimate ways
- Legitimate user can access the data

The Security Problem in Computing

1.3 Attacks

- **Types of attacks**

Attacks are grouped into two types:

- *Passive attacks:* does not involve any modification to the contents of an original message
- *Active attacks:* the contents of the original message are modified in some ways.

The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

- Encryption is the process of encoding a message so that its meaning is not obvious; decryption is the reverse process, transforming an encrypted message back into its normal, original form.

The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

- Alternatively, the terms encode and decode or encipher and decipher are used instead of encrypt and decrypt. That is, we say that we encode, encrypt, or encipher the original message to hide its meaning. Then, we decode, decrypt, or decipher it to reveal the original message.

The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

- A system for encryption and decryption is called a cryptosystem.
- The original form of a message is known as plaintext, and the encrypted form is called cipher text.

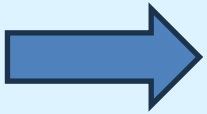
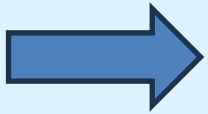
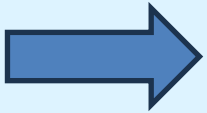
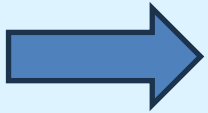
The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

- The original form of a message is known as plaintext, and the encrypted form is called cipher text. For convenience, we denote a plaintext message *P* as a sequence of individual characters *P* = <*p*1, *p*2, …, *pn*>. Similarly, cipher text is written as *C* = <*c*1, *c*2, …,*cm*>.

The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

- Plain Text  Encryption  Cipher Text
- Cipher Text  Decryption  Plain Text

The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

- *Cryptanalyst:* a person who studies encryption and encrypted message and tries to find the hidden meanings (to break an encryption).
- *Confusion:* a technique for ensuring that ciphertext has no clue about the original message.
- *Diffusion:* increases the redundancy of the plaintext by spreading it across rows and columns.

The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

Substitutions Cipher: It basically consists of substituting every plaintext character for a different cipher text character.

It is of two types

1. Mono alphabetic substitution cipher
2. Poly alphabetic substitution cipher

The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

Mono alphabetic substitution cipher:

Relationship between cipher text symbol and plain text symbol is 1:1.

- Additive cipher:

  Key value is added to plain text and numeric value of key ranges from 0 – 25.

The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

Example:

Plain text(P)- H E L LO (H=7,E=4,L=11,L=11,O=14)

Key (K)=15

Cipher text (C)= 7+15,4+15,11+15,11+15,14+15

= 22,19, 26,26,(29%26)=3

= W T A AD

The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

Polyalphabetic substitution cipher

In polyalphabetic cipher each occurrence of a character may have different substitution. The relationship between characters in plain text and cipher text is 1 to many.

The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

Polyalphabetic substitution cipher

Auto key cipher:

- In this cipher, key is a stream of subkeys in which subkey is used to encrypt the corresponding character in the plain text.

The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

Polyalphabetic substitution cipher

Auto key cipher:

- Here 1st subkey is predefined and 2nd subkey is the value of the 1st character of the plain text 3rd subkey is the value of the 2nd plain text and so on.

The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

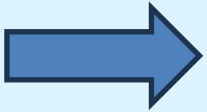
Example:

A T T A C K Key=12

0 19 19 0 2 10

12 0 19 19 0 2

Cipher text = (12,19,38 19,2 12)%26



M T M T C M

The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

Polyalphabetic substitution cipher

Vigener cipher:

- The key stream is the repetition of the initial secret key stream of length m. (1<=m<=26)

The Security Problem in Computing

1.4 Elementary Cartography: Substitution Cipher

Example:

Plaintext= A B C D E F G H

Ks= 0, 5, 8

A B C D E F G H (B=1 =>1+5=6=>G)

0 5 8 0 5 8 0 5

0 6 10 3 9 13 6 12 **A G K D J N G M <=** ciphertext

The Security Problem in Computing

1.5 Making Good Encryption Algorithm

- Each type of encryption is considered to have advantages and disadvantages. But there is a broader question: *What does it mean for a cipher to be "good"?* The meaning of good depends on the intended use of the cipher.

The Security Problem in Computing

1.5 Making Good Encryption Algorithm

- A cipher used by military personnel in the field has different requirements from one to be used in a secure installation with substantial computer support.

The Security Problem in Computing

1.5 Making Good Encryption Algorithm

Shannon's Characteristics of "Good" Ciphers

In 1949, Claude Shannon [SHA49] proposed several characteristics that identify a good cipher.

1. The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption.
2. The set of keys and the enciphering algorithm should be free from complexity.

The Security Problem in Computing

1.5 Making Good Encryption Algorithm

Shannon's Characteristics of "Good" Ciphers

3. The implementation of the process should be as simple as possible
4. Errors in ciphering should not propagate and cause corruption of further information in the message.
5. The size of the enciphered text should be no larger than the text of the original message.

The Security Problem in Computing

1.5 Making Good Encryption Algorithm

Properties of "Trustworthy" Encryption Systems

Commercial users have several requirements that must be satisfied when they select an encryption algorithm. Thus, when encryption is "commercial grade," or "trustworthy," it means that it meets these constraints:

The Security Problem in Computing

1.5 Making Good Encryption Algorithm

Properties of "Trustworthy" Encryption Systems

1. It is based on sound mathematics. Good cryptographic algorithms are not just invented; they are derived from solid principles.

The Security Problem in Computing

1.5 Making Good Encryption Algorithm

Properties of "Trustworthy" Encryption Systems

2. It has been analyzed by competent experts and found to be sound. Even the best cryptographic experts can think of only so many possible attacks, and the developers may become too convinced of the strength of their own algorithm. Thus, a review by critical outside experts is essential.

The Security Problem in Computing

1.5 Making Good Encryption Algorithm

Properties of "Trustworthy" Encryption Systems

3. It has stood the test of time. As a new algorithm gains popularity, people continue to review both its mathematical foundations and the way it builds on those foundations. Although a long period of successful use and analysis is not a guarantee of a good algorithm, the flaws in many algorithms are discovered relatively soon after their release.

The Security Problem in Computing

1.5 Making Good Encryption Algorithm

Properties of "Trustworthy" Encryption Systems

Cryptography algorithms (ciphers) can be divided into two groups: *symmetric key cryptography algorithms* and *asymmetric cryptography algorithms*. Figure shows the taxonomy

The Security Problem in Computing

1.5 Making Good Encryption Algorithm

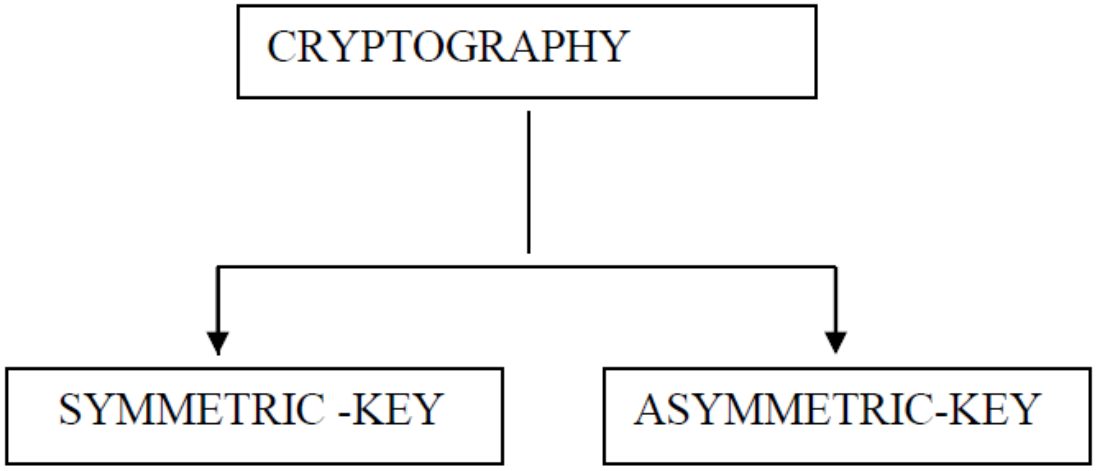


Fig :Categories of Cryptography

The Security Problem in Computing

1.5 Making Good Encryption Algorithm

Properties of "Trustworthy" Encryption Systems

1. Symmetric·Key Cryptography

In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

The Security Problem in Computing

1.5 Making Good Encryption Algorithm

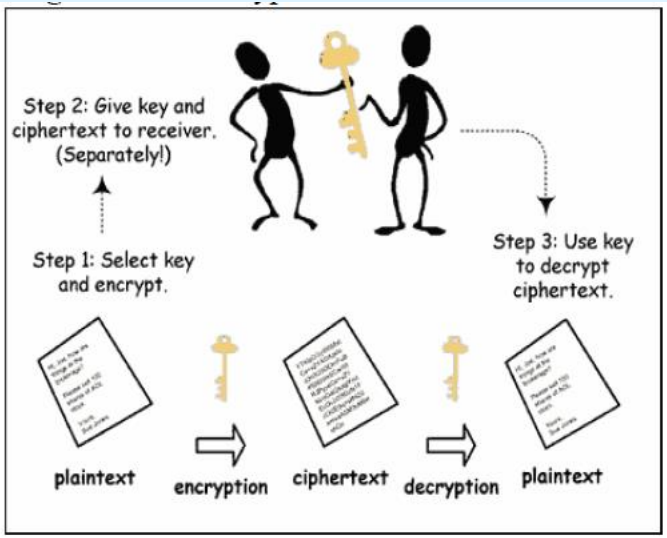


Fig :Symmetric-key Cryptography

The Security Problem in Computing

1.5 Making Good Encryption Algorithm

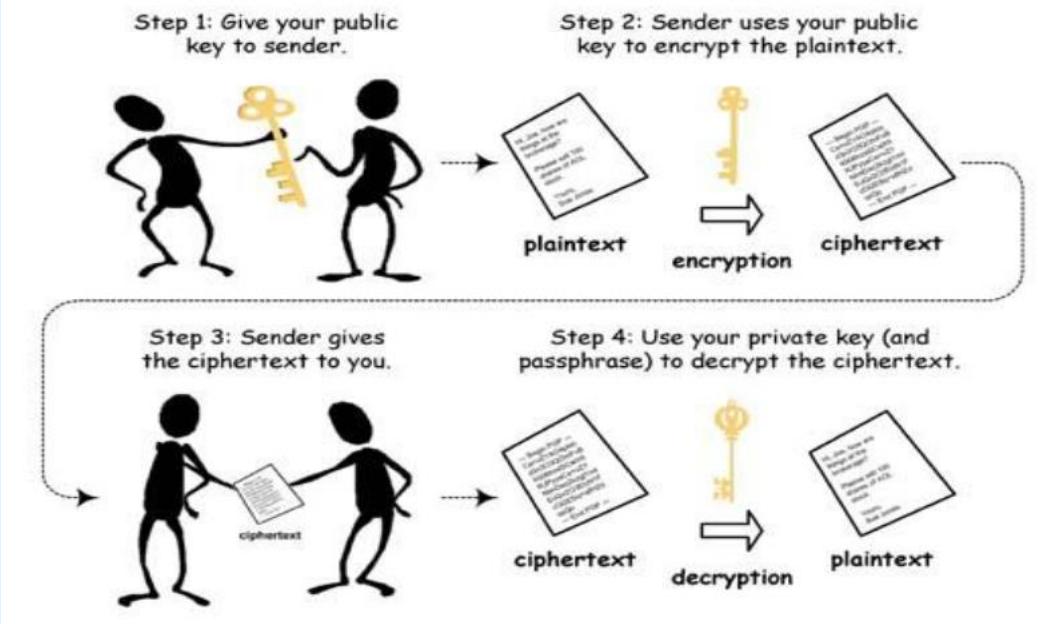
Properties of "Trustworthy" Encryption Systems

2. Asymmetric-Key Cryptography:

In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.

The Security Problem in Computing

1.5 Making Good Encryption Algorithm



The Security Problem in Computing

1.6 Privacy Key Crypto System

- **Symmetric encryption** (also called *private-key encryption* or *secret-key encryption*) involves using the same key for encryption and decryption.
- Encryption involves applying an operation (an algorithm) to the data to be encrypted using the private key to make them unintelligible.
- The slightest algorithm (such as an exclusive OR) can make the system nearly tamper proof.

The Security Problem in Computing

1.6 Privacy Key Crypto System

- ***Stream cipher:*** Stream ciphers convert one symbol of plaintext directly into a symbol of ciphertext.

Advantages:

- Speed of transformation: algorithms are linear in time and constant in space.
- Low error propagation: an error in encrypting one symbol likely will not affect subsequent symbols.

1.6 Privacy Key Crypto System

Disadvantages:

- Low diffusion: all information of a plaintext symbol is contained in a single ciphertext symbol.
- Susceptibility to insertions/ modifications: an active interceptor who breaks the algorithm might insert spurious text that looks authentic.

1.6 Privacy Key Crypto System

- ***Block ciphers***: It encrypt a group of plaintext symbols as one block.

  Advantages:

  - High diffusion: information from one plaintext symbol is diffused into several ciphertext symbols.
  - Immunity to tampering: difficult to insert symbols without detection.

1.6 Privacy Key Crypto System

Disadvantages:

- Slowness of encryption: an entire block must be accumulated before encryption / decryption can begin.
- Error propagation: An error in one symbol may corrupt the entire block. Simple substitution is an example of a stream cipher. Columnar transposition is a block cipher.

The Security Problem in Computing

1.7 Data Encryption Standards

- The Data Encryption Standard (DES), a system developed for the U.S. government, was intended for use by the general public. It has been officially accepted as a cryptographic standard both in the United States and abroad.

The Security Problem in Computing

1.7 Data Encryption Standards

- The DES algorithm is a careful and complex combination of two fundamental building blocks of encryption: substitution and transposition. The algorithm derives its strength from repeated application of these two techniques, one on top of the other, for a total of 16 cycles.

The Security Problem in Computing

1.7 Data Encryption Standards

- The sheer complexity of tracing a single bit through 16 iterations of substitutions and transpositions has so far stopped researchers in the public from identifying more than a handful of general properties of the algorithm.

The Security Problem in Computing

1.7 Data Encryption Standards

- The algorithm begins by encrypting the plaintext as blocks of 64 bits. The key is 64 bits long, but in fact it can be any 56-bit number. (The extra 8 bits are often used as check digits and do not affect encryption in normal implementations.)

1.7 Data Encryption Standards

Features:

✓ Block size = 64 bits

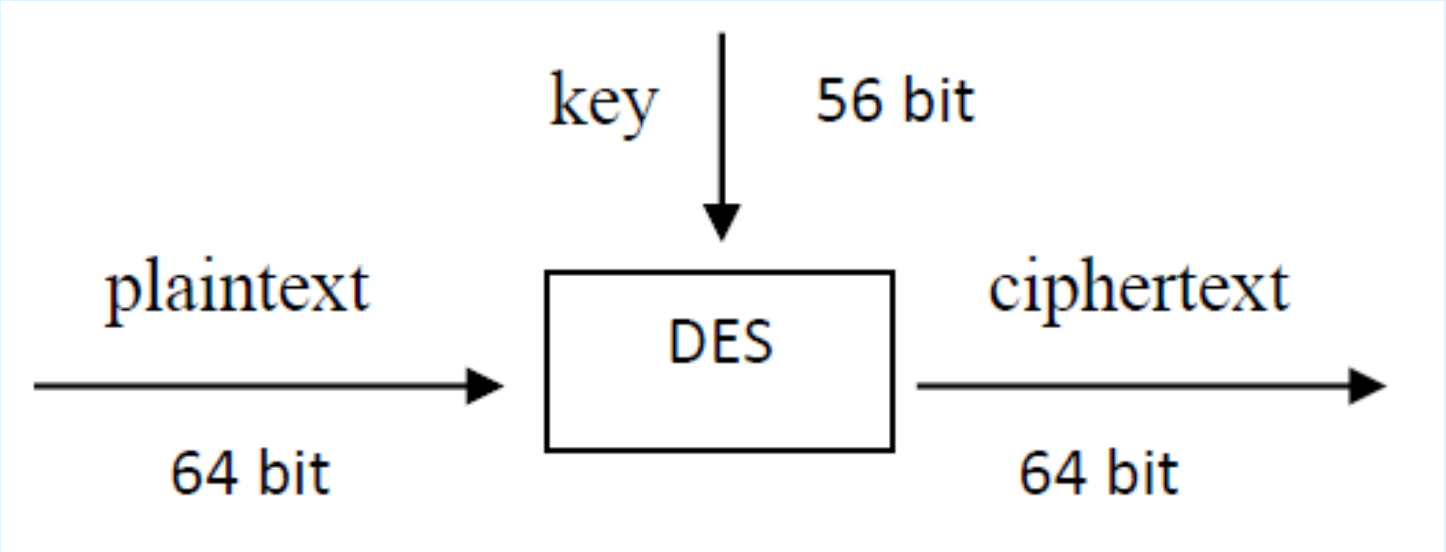
✓ Key size = 56 bits (in reality, 64 bits, but 8 are used as parity-check bits for error control, see next slide)

✓ Number of rounds = 16

✓ 16 intermediary keys, each 48 bits

The Security Problem in Computing

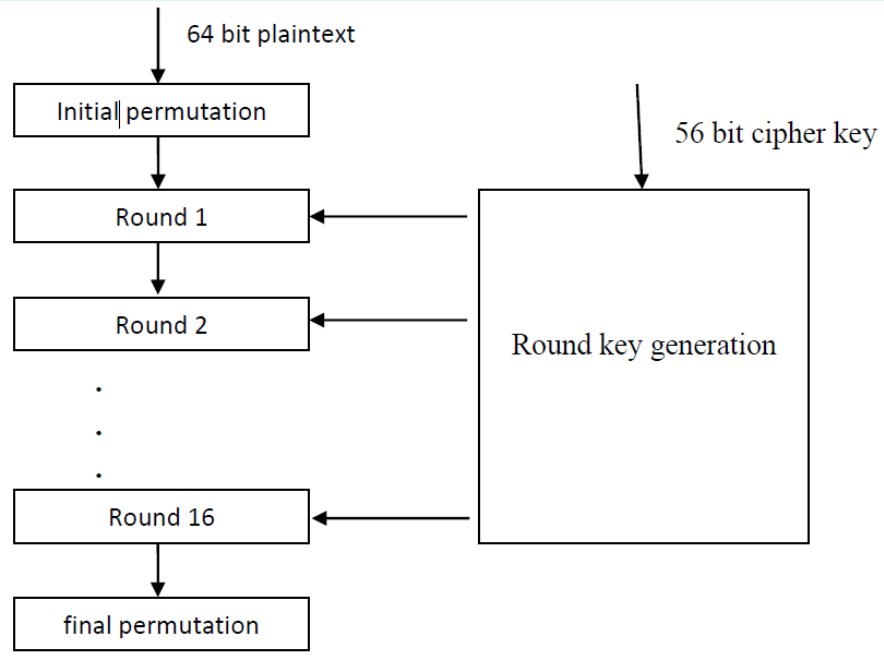
1.7 Data Encryption Standards



The Security Problem in Computing

1.7 Data Encryption Standards

Working Principle:



1.7 Data Encryption Standards

- **Security of the DES**

  Since its was first announced, DES has been controversial. Many researchers have questioned the security it provides. Much of this controversy has appeared in the open literature, but certain DES features have neither been revealed by the designers nor inferred by outside analysts.

The Security Problem in Computing

1.8 The AES Encryption Algorithm

- The AES is likely to be the commercial-grade symmetric algorithm of choice for years, if not decades.
- AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware.

The Security Problem in Computing

1.8 The AES Encryption Algorithm

- Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.
- By contrast, the Rijndael specification *per se* is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

The Security Problem in Computing

1.8 The AES Encryption Algorithm

- AES operates on a 4×4 column-major order matrix of bytes, termed the *state*, although some versions of Rijndael have a larger block size and have additional columns in the state.
- Most AES calculations are done in a special finite field.

The Security Problem in Computing

1.8 The AES Encryption Algorithm

- The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext.

The Security Problem in Computing

1.8 The AES Encryption Algorithm

- The number of cycles of repetition are as follows:
  - 10 cycles of repetition for 128-bit keys.
  - 12 cycles of repetition for 192-bit keys.
  - 14 cycles of repetition for 256-bit keys.

The Security Problem in Computing

1.8 The AES Encryption Algorithm

- **High-level description of the algorithm**

1. *KeyExpansions*—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

1.8 The AES Encryption Algorithm

- **High-level description of the algorithm**

2. *InitialRound*

    1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

1.8 The AES Encryption Algorithm

- **High-level description of the algorithm**

3. Rounds

1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

1.8 The AES Encryption Algorithm

- **High-level description of the algorithm**

3. Rounds

2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

1.8 The AES Encryption Algorithm

- **High-level description of the algorithm**

3. Rounds

3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. AddRoundKey

1.8 The AES Encryption Algorithm

- **High-level description of the algorithm**

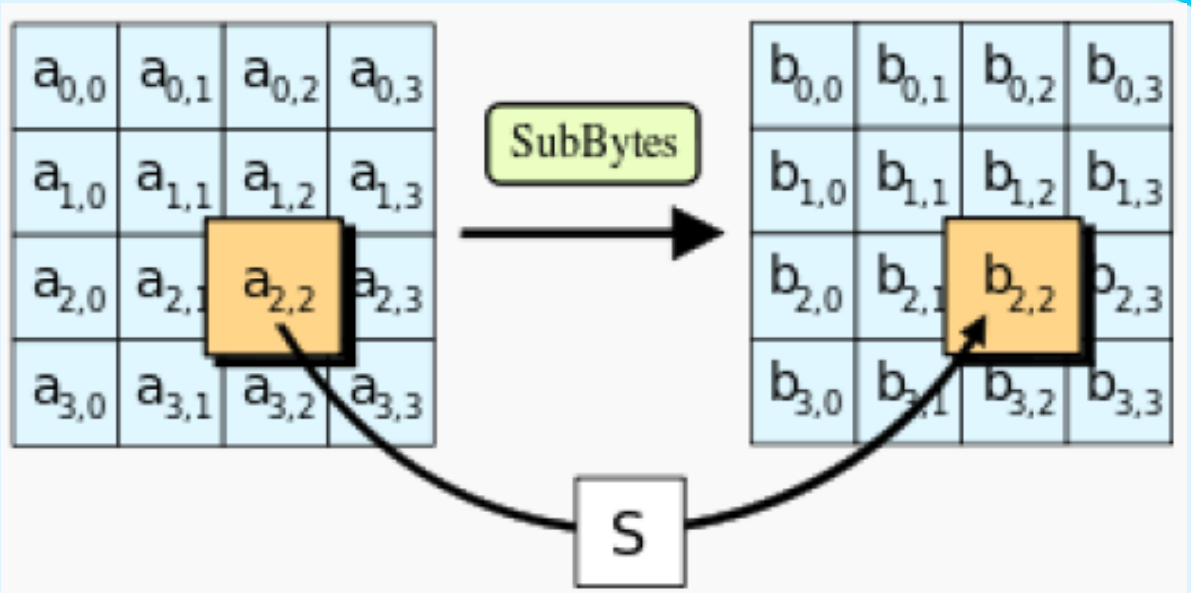
4. Final Round (no MixColumns)

1. SubBytes
2. ShiftRows
3. AddRoundKey.

The Security Problem in Computing

1.8 The AES Encryption Algorithm

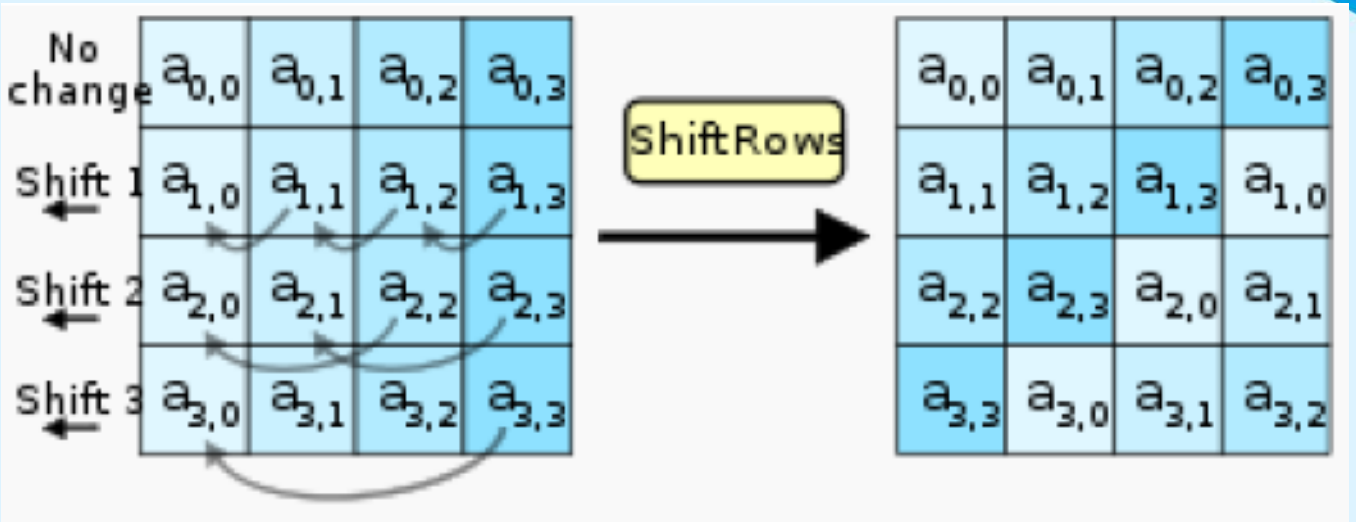
The SubBytes Steps



The Security Problem in Computing

1.8 The AES Encryption Algorithm

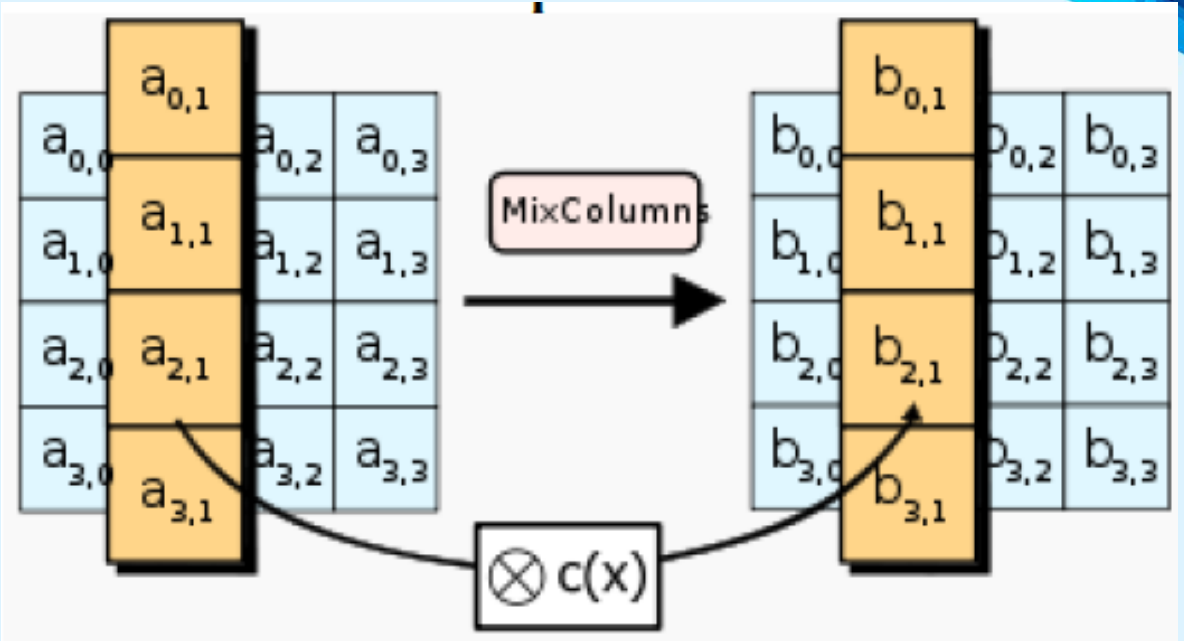
The ShiftRows Steps



The Security Problem in Computing

1.8 The AES Encryption Algorithm

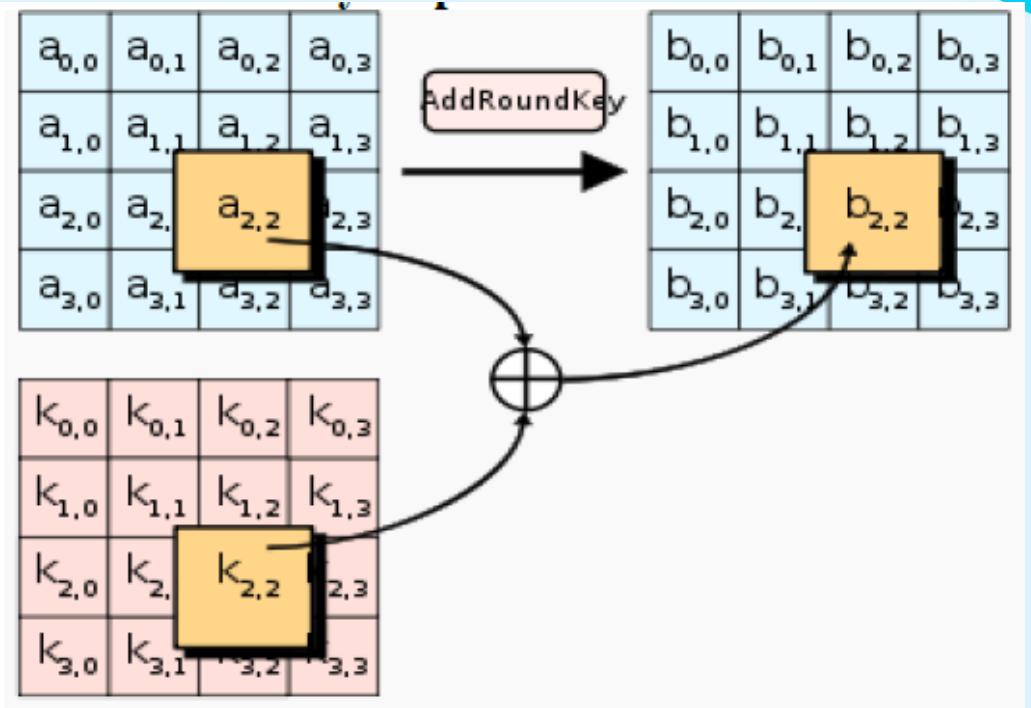
The MixColumns Steps



The Security Problem in Computing

1.8 The AES Encryption Algorithm

The AddRoundKey Steps



1.8 The AES Encryption Algorithm

➢ **Optimization of the Cipher**

- On systems with 32-bit or larger words, it is possible to speed up execution of this cipher by combining the SubBytes and ShiftRows steps with the MixColumns step by transforming them into a sequence of table lookups.

1.8 The AES Encryption Algorithm

➢ Optimization of the Cipher

- This requires four 256-entry 32-bit tables, and utilizes a total of four kilobytes (4096 bytes) of memory — one kilobyte for each table.

1.8 The AES Encryption Algorithm

➢ Optimization of the Cipher

- A round can then be done with 16 table lookups and 12 32-bit exclusive-or operations, followed by four 32-bit exclusive-or operations in the AddRoundKey steps.

1.8 The AES Encryption Algorithm

➢ Optimization of the Cipher

- Using a byte-oriented approach, it is possible to combine the SubBytes, ShiftRows, and MixColumns steps into a single round operation.

The Security Problem in Computing

1.9 Public Key Cryptosystem

- ***Public-key cryptography***, also known as ***asymmetric cryptography***, is a class of cryptographic algorithms which requires two separate keys, one of which is *secret* (or *private*) and one of which is *public*.

The Security Problem in Computing

1.9 Public Key Cryptosystem

- ***Public-key cryptography*** is often used to secure electronic communication over an open networked environment such as the internet.
- Open networked environments are susceptible to a variety of communication security problems such as man-in-the-middle attacks and other security threats.

The Security Problem in Computing

1.9 Public Key Cryptosystem

- The distinguishing technique used in *public-key cryptography* is the use of *asymmetric key algorithms*, where the key used to encrypt a message is not the same as the key used to decrypt it.

The Security Problem in Computing

1.9 Public Key Cryptosystem

- Each user has a pair of cryptographic keys – a *public encryption key* and a *private decryption key*. Similarly, a key pair used for digital signatures consists of a *private signing key* and a *public verification key*.

The Security Problem in Computing

1.9 Public Key Cryptosystem

- The public key is widely distributed, while the private key is known only to its proprietor.
- The keys are related mathematically, but the parameters are chosen so that calculating the private key from the public key is either impossible or prohibitively expensive.

1.9 Public Key Cryptosystem

- In contrast, symmetric-key algorithms – variations of which have been used for thousands of years – use a *single* secret key, which must be shared and kept private by both the sender and the receiver, for both encryption and decryption.

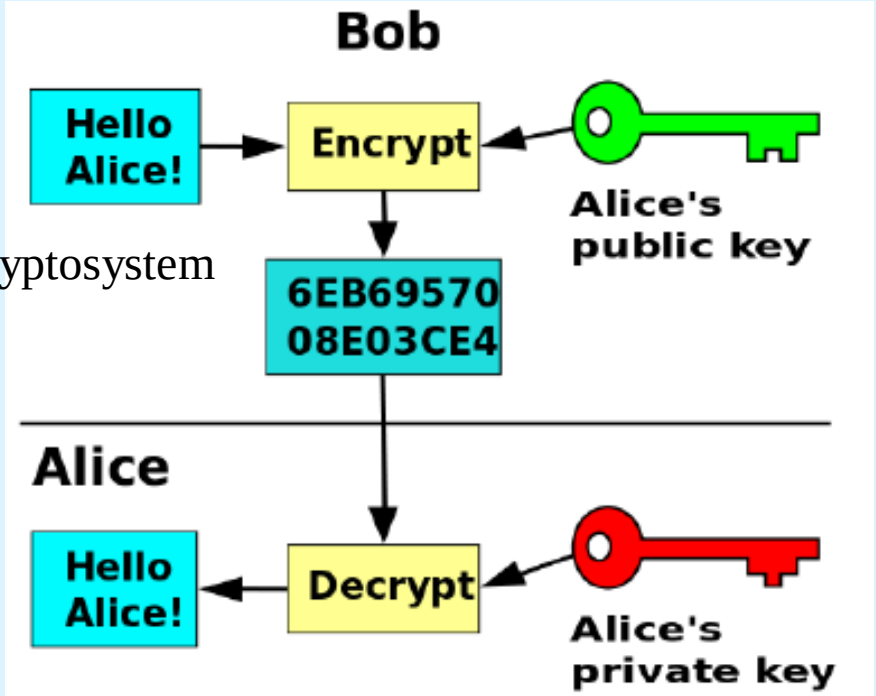
1.9 Public Key Cryptosystem

- To use a symmetric encryption scheme, the sender and receiver must securely share a key in advance.

The Security Problem in Computing

1.9 Public Key Cryptosystem

Public Key cryptosystem



Public Key cryptosystem

The Security Problem in Computing

1.10 Use of Encryption

- Encryption has long been used by militaries and governments to facilitate secret communication.
- It is now commonly used in protecting information within many kinds of civilian systems.

The Security Problem in Computing

1.10 Use of Encryption

- Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines.

The Security Problem in Computing

1.10 Use of Encryption

➢ Message verification

- Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message; for example, verification of a message authentication code (MAC) or a digital signature.

1.10 Use of Encryption

➢ PSEUDO-RANDOMNESS

- For cryptography, the use of pseudorandom number generators is insecure. When random values are required in cryptography, the goal is to make a message as hard to crack as possible, by eliminating the parameters used to encrypt the message from the message which it is carried.

The Security Problem in Computing

1.10 Use of Encryption

➢ HASHING

- *A **cryptographic hash function*** is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. These one-way hash functions have been called "the workhorses of modern cryptography".

1.10 Use of Encryption

➢ HASHING

- The input data is often called the *message*, and the hash value is often called the *message digest* or simply the *digest*.

The Security Problem in Computing

1.10 Use of Encryption

➢ HASHING

- The ideal cryptographic hash function has four main properties:
  1. easy to compute the hash value for any given message
  2. infeasible to generate a message that has a given hash
  3. infeasible to modify a message without changing the hash
  4. infeasible to find two different messages with the same hash.

1.10 Use of Encryption

➢ HASHING

- A cryptographic hash function must be able to withstand all known types of cryptanalytic attack.

1.10 Use of Encryption

➢ HASHING

At a minimum, it must have the following properties:

1. Pre-image resistance

- Given a hash *h* it should be difficult to find any message *m* such that *h = hash(m)*. This concept is related to that of one-way function. Functions that lack this property are vulnerable to preimage attacks.

1.10 Use of Encryption

➢ HASHING

At a minimum, it must have the following properties:

2. Second pre-image resistance

- Given an input *m*1 it should be difficult to find another input *m*2 such that *m*1 ≠ *m*2 and *hash*(*m*1) = *hash*(*m*2). Functions that lack this property are vulnerable to second-preimage attacks.

1.10 Use of Encryption

➢ HASHING

At a minimum, it must have the following properties:

3. Collision resistance

- This property is sometimes referred to as *strong collision resistance.* It requires a hash value at least twice as long as that required for preimage-resistance; otherwise collisions may be found by a birthday attack.

-end-