Chapter 7

Cryptography Basics and Methods

Overview of Cryptography

- Understanding Physical Cryptography
- Understanding Mathematical Cryptography
- Understanding Quantum Cryptography

Understanding Physical Cryptography

- Physical cryptography refers to any method that doesn't alter the value using a mathematical process.
- Physical methods also include a method of encryption called *steganography*
- *Cipher* is a method used to encode characters to hide their value.
- *Ciphering* is the process of using a cipher to encode a message.

Understanding Physical Cryptography

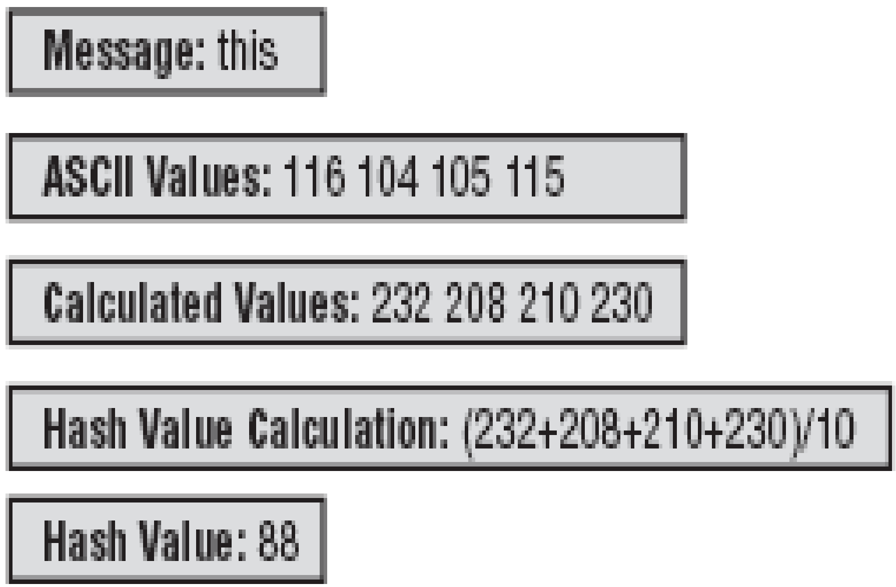
- The three primary types of ciphering methods
  - Substitution: is a type of coding or ciphering system that changes one character or symbol into another
    - Character substitution can be a relatively easy method of encrypting information
  - Transposition: (*transposition code)* involves transposing or scrambling the letters in a certain manner.
    - Typically, a message is broken into blocks of equal size, and each block is then scrambled.
  - Steganography: is the process of hiding one message in another.
    - Prevents analysts from detecting the real message.
    - You could encode your message in another file

Understanding Mathematical Cryptography

- Mathematical cryptography deals with using mathematical processes on characters or messages
- Hashing: refers to performing a calculation on a message and converting it into a numeric hash value
- *Hash value*
- *Checksum*
- *One-way process*

Understanding Mathematical Cryptography

- A simple hashing process



Understanding Physical Cryptography

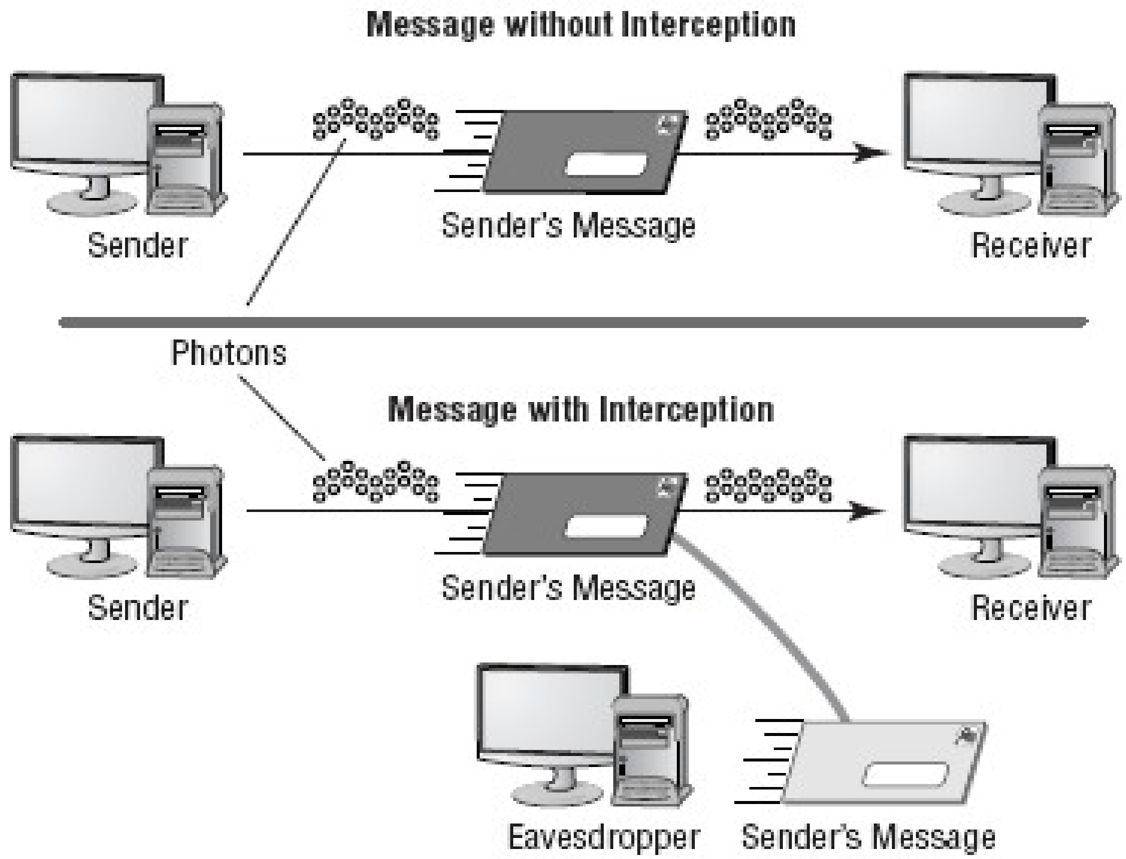
- **Working with Passwords**
  - Many password-generation systems are based on a one-way hashing approach.
  - Passwords should be as long and as complicated as possible.
  - Most security experts believe a password of 10 characters is the minimum that should be used if security is a real concern.
  - Mathematical methods of encryption are primarily used in conjunction with other encryption methods as part of authenticity verification.

Understanding Quantum Cryptography

- *Quantum cryptography* is a relatively new method of encryption.
- It may now be possible to create unbreakable ciphers using quantum methods.
- The process depends on a scientific model called the *Heisenberg Uncertainty Principle* for security
- A message is sent using a series of photons.

Understanding Physical Cryptography

- Quantum cryptography being used to encrypt a message



Cryptographic Algorithms

- The Science of Hashing
- Symmetric Algorithms
- Asymmetric Algorithms

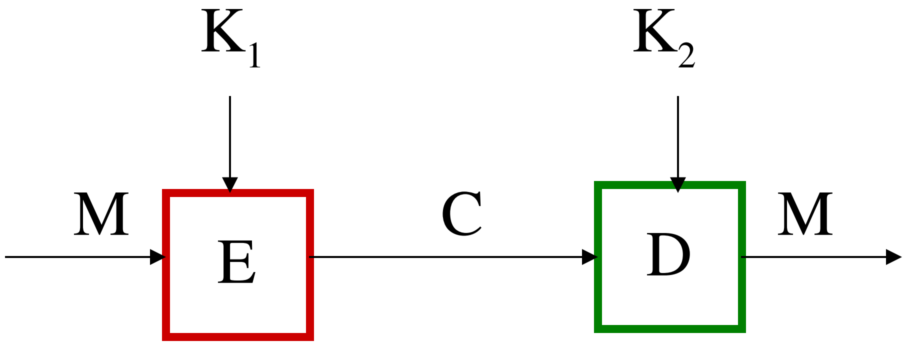
The Science of Hashing

- *Hashing* is the process of converting a message, or data, into a numeric value
- The numeric value that a hashing process creates is referred to as a *hash total* or *value*
- Hashing functions
  - A one-way hash doesn't allow a message to be decoded back to the original value.
  - A two-way hash allows a message to be reconstructed from the hash

The Science of Hashing

- **Secure Hash Algorithm (SHA):** was designed to ensure the
- integrity of a message.
  - The SHA is a one-way hash that provides a hash value that can be used with an encryption protocol.
  - Produces a 160-bit hash value.
  - SHA has been updated; the new standard is SHA-1.
- **Message Digest Algorithm (MDA):** creates a hash value and uses a one-way hash.
  - The hash value is used to help maintain integrity.
  - There are several versions of MD
  - the most common are MD5, MD4, and MD2.

Key Based Encryption/Decryption



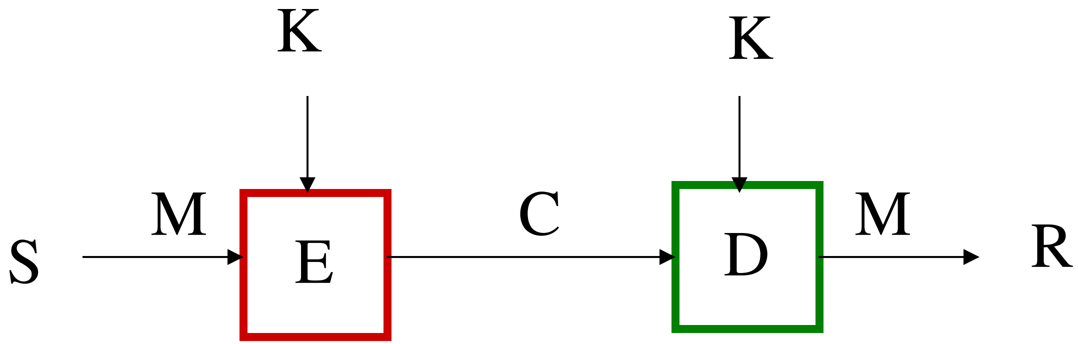
Symmetric Case: *both keys are the same or derivable from each other.*

Asymmetric Case: *keys are different and not derivable from each other.*

Symmetric Algorithms

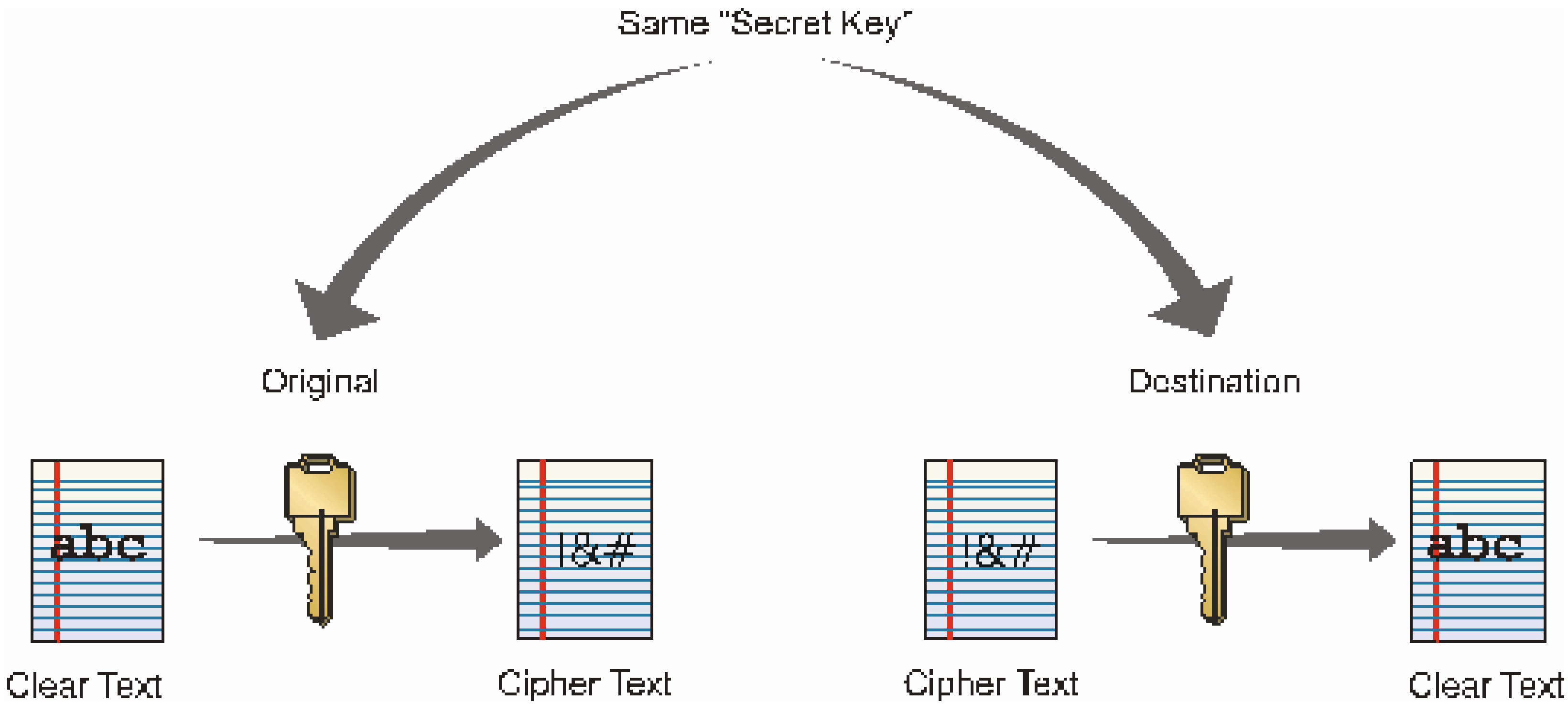
- *Symmetric algorithms* require both ends of an encrypted message to have the same key and processing algorithms.
- Symmetric algorithms generate a secret key that must be protected.
- The disclosure of a private key breaches the security of the encryption system.
- If a key is lost or stolen, the entire process is breached.

Secrete Key Cryptography



K is the secret key shared by both the sender (S) and receiver (R).

Private Key Cryptosystem (Symmetric)



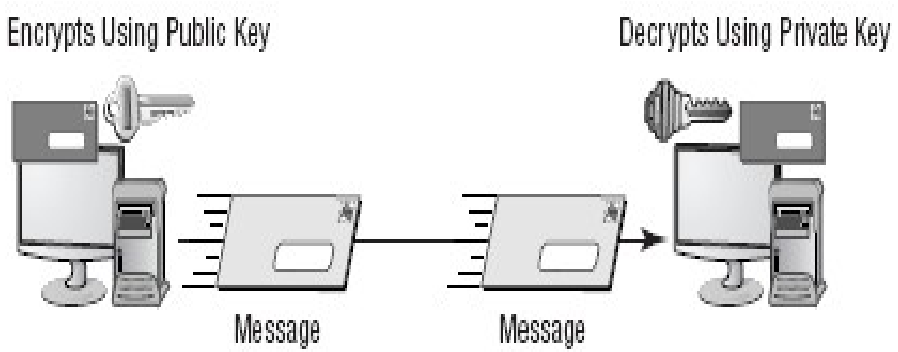
Symmetric Algorithms

- **DES** The *Data Encryption Standard (DES)* has been used since the mid-1970s.
  - It was the primary standard used in government and industry until it was replaced by AES.
  - It's a strong and efficient algorithm based on a 56-bit key.
- **AES** *Advanced Encryption Standard (AES)* has replaced DES as the current standard;
  - Uses the Rijndael algorithm.
  - It was developed by Joan Daemen and Vincent Rijmen.
  - It supports key sizes of 128, 192, and 256 bits, with 128 bits being the default.

Asymmetric Algorithms

- *Asymmetric algorithms* use two keys to encrypt and decrypt data.
- These keys are referred to as the *public key* and the *private key*.
- The public key can be used by the sender to encrypt a message
- The private key can be used by the receiver to decrypt the message.
- The algorithms used in this two-key process are complicated.

Asymmetric Algorithms



Asymmetric Algorithms

- **RSA** is named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman.
  - The RSA algorithm is an early public-key encryption system that uses large integer numbers as the basis of the process.
- **Diffie-Hellman** Dr. W. Diffie and Dr. M. E. Hellman conceptualized the Diffie-Hellman key exchange.
  - They are considered the founders of the public/private key concept;
  - their original work envisioned splitting the key into two parts.
  - This algorithm is used primarily to send keys across public networks

Cryptographic Systems

- A cryptographic system is a system, method, or process that is used to provide encryption and decryption.
- These systems may be hardware, software, or manually performed processes.
- Cryptographic systems exist for the same reasons that security exists: to provide confidentiality, integrity, authentication, non-repudiation, and access control.

Cryptographic Systems

- **Confidentiality**
  - One of the major reasons to implement a cryptographic system is to ensure the confidentiality of the information being used.
  - This confidentiality may be intended to prevent the unauthorized disclosure of information in a local network.
  - A cryptographic system must do this effectively in order to be of value.

Cryptographic Systems

- **Integrity**
  - providing assurance that a message wasn’t modified during transmission
  - Integrity can be accomplished by adding information such as checksums or redundant data that can be used as part of the decryption process.
  - These two additions to the message provide a two-way check on the integrity of the message.
  - A common method of verifying integrity involves adding a *message authentication code (MAC)* to the message.
  - The MAC is derived from the message and a key.

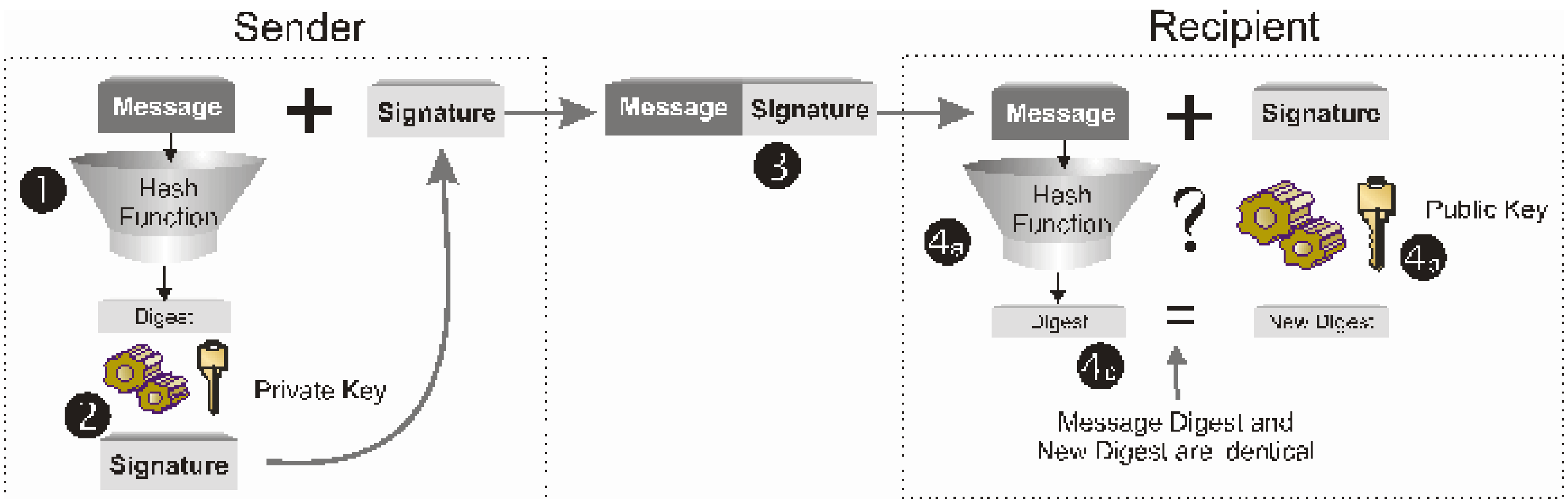
Cryptographic Systems

- **Using Digital Signatures**
  - A *digital signature* is similar in function to a standard signature on a document.
  - This signature validates the integrity of the message and the sender.
  - The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message
  - The digital signature is derived from a hash process known only by the originator

Digital Signatures

- A digital signature is a protocol the produces the same effect as a real signature.
  - It is a mark that only sender can make
  - Other people can easily recognize it as belonging to the sender.
- Digital signatures must be:
  - Unforgeable: If P signs message M with signature S(P,M), it is impossible for someone else to produce the pair [M, S(P,M)].
  - Authentic: R receiving the pair [M, S(P,M)] can check that the signature is really from P.

Digital Signature Process



Cryptographic Systems

- Authentication
- Non-Repudiation
- Access Control

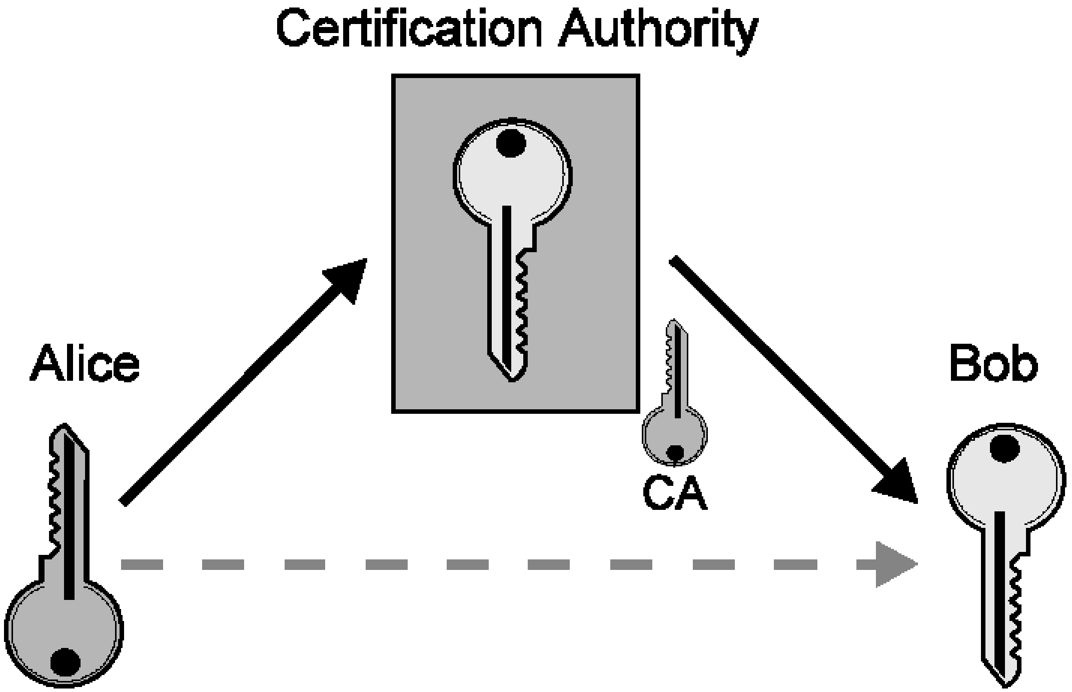
Public Key Infrastructure

- The *Public Key Infrastructure (PKI)* is a first attempt to provide all the aspects of security to
- messages and transactions that have been previously discussed.
- The need for universal systems to support e-commerce, secure transactions, and information privacy is one aspect of the issues being addressed with PKI.
- PKI is a two-key—asymmetric—system.

Public Key Infrastructure

- As defined by Netscape:
  - *“Public-key infrastructure (PKI) is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet.”*
  - Integrates digital certificates, public key cryptography, and certification authorities
- Two major frameworks
  - X.509
  - PGP (Pretty Good Privacy)

Certification Authorities (CAs)



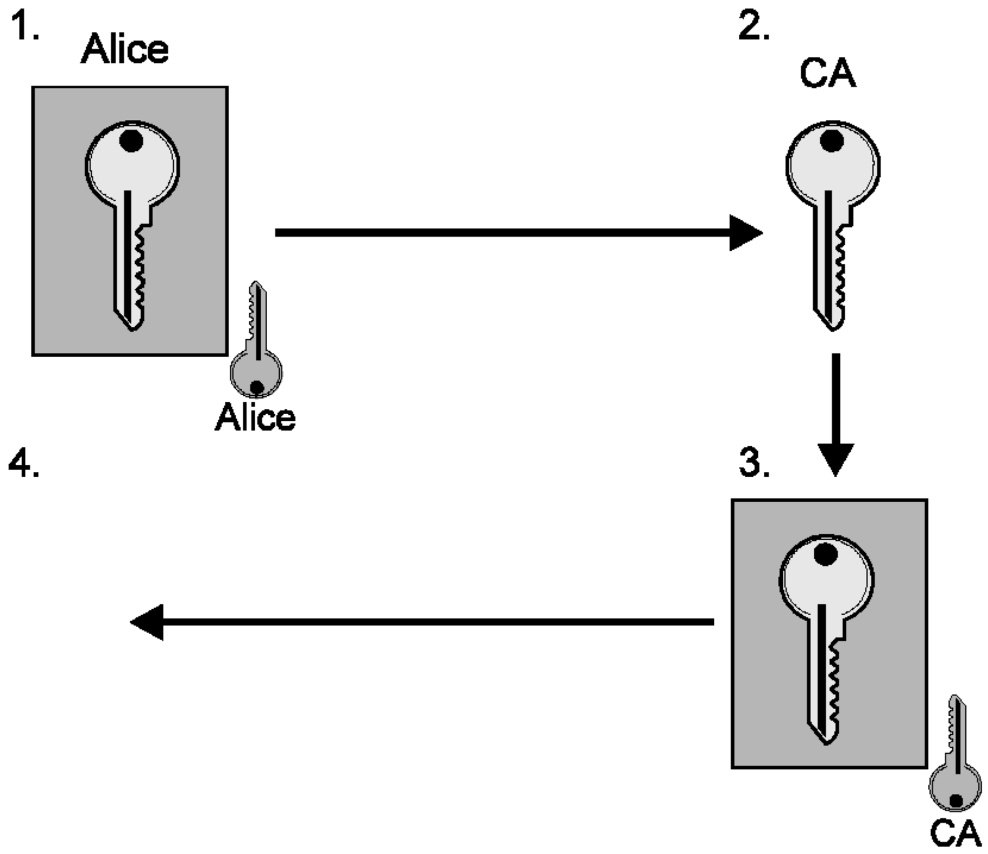
Certification Authorities (cont.)

- Guarantee connection between public key and end entity
  - Man-In-Middle no longer works undetected
  - Guarantee authentication and non-repudiation
  - Privacy/confidentiality not an issue here
    - Only concerned with linking key to owner
- Distribute responsibility
  - Hierarchical structure

Digital Certificates

- Introduced by IEEE-X.509 standard (1988)
- Originally intended for accessing IEEE-X.500 directories
  - Concerns over misuse and privacy violation gave rise to need for access control mechanisms
  - X.509 certificates addressed this need
- From X.500 comes the Distinguished Name (DN) standard
  - Common Name (CN)
  - Organizational Unit (OU)
  - Organization (O)
  - Country (C)
- Supposedly enough to give every entity on Earth a unique name

Obtaining Certificates



Obtaining Certificates

- 1. Alice generates A_{priv}, A_{pub} and A_{ID}; Signs $\{A_{pub}, A_{ID}\}$ with A_{priv}
  - Proves Alice holds corresponding A_{priv}
  - Protects $\{A_{pub}, A_{ID}\}$ en route to CA
- 2. CA verifies signature on $\{A_{pub}, A_{ID}\}$
  - Verifies A_{ID} offline (optional)
- 3. CA signs $\{A_{pub}, A_{ID}\}$ with CA_{priv}
  - Creates certificate
  - Certifies binding between A_{pub} and A_{ID}
  - Protects $\{A_{pub}, A_{ID}\}$ en route to Alice
- 4. Alice verifies $\{A_{pub}, A_{ID}\}$ and CA signature
  - Ensures CA didn't alter $\{A_{pub}, A_{ID}\}$
- 5. Alice and/or CA publishes certificate

PKI: Benefits

- Provides authentication
- Verifies integrity
- Ensures privacy
- Authorizes access
- Authorizes transactions
- Supports non-repudiation

PKI: Risks

- Certificates only as trustworthy as their CAs
  - Root CA is a single point of failure
- PKI only as secure as private signing keys
- DNS not necessarily unique
- Server certificates authenticate DNS addresses, not site contents
- CA may not be authority on certificate contents
  - i.e., DNS name in server certificates
- ...

Implementing Trust Models

- Four main types of trust models are used with PKI:
  - Hierarchical
  - Bridge
  - Mesh
  - Hybrid

Preparing for Cryptographic Attacks

- **Attacking the Key** Key attacks are typically launched to discover the value of a key by attacking the key directly.
- These keys can be passwords, encrypted messages, or other key-based encryption information.
- An attacker might try to apply a series of words, commonly used passwords, and other randomly selected combinations to crack a password.
- A key attack tries to crack a key by repeatedly guessing the key value to break a password.

Preparing for Cryptographic Attacks

- **Attacking the Algorithm** The programming instructions and algorithms used to encrypt information are as much at risk as the keys.
- If an error isn't discovered and corrected by a program's developers, an algorithm might not be able to secure the program.
- Many algorithms have wellpublicized back doors

Preparing for Cryptographic Attacks

- **Intercepting the Transmission** The process of intercepting a transmission may, over time, allow attackers to inadvertently gain information about the encryption systems used by an organization.
- The more data attackers can gain, the more likely they are to be able to use frequency analysis to break an algorithm.