# Cryptography

- Cryptography is a collection of mathematical techniques to ensure confidentiality of information
- Encryption and Decryption
  - The process of scrambling a message with the help of a key is called Encryption
  - The process of unscrambling a message using an appropriate key is called decryption
- Keys are numbers or characters that are randomly generated
- Symmetric and Asymmetric cryptography
  - Symmetric - same keys are used for encryption and decryption
  - Asymmetric or Public Key Cryptography – a pair of public key and private key is used for encryption and decryption
- Pretty Good Privacy (PGP) – a popular cryptographic system

# Digital/Electronic Signatures

- An electronic signature means any letters numbers, symbols, images, characters or any combination thereof in electronic form applied to an electronic document
- Uses public key cryptography
- Ensures authenticity, integrity and non- repudiation
  - Authenticity means the message is from a particular source/individual
  - Integrity means the message has not been altered
  - Non-repudiation means that the execution of the digital signature cannot be denied
- Electronic signature vs. hand written signature

# Digital Certificates

- Establish whether or not a public key belongs to the purported owner
- Comprises of a public key, certification information (name, ID etc.) and electronic signatures of a certification authority
- x.509 standard format

Name:Jonathan Marshall
Public Key:023917918729087395045273927
Date Issue:January 15, 2003
Date Expiry: January 15, 2005
Serial Number:2345872364

We certify that the above information is true.
**Dues Certification Authority Inc.**

# Certification Authority (CA)

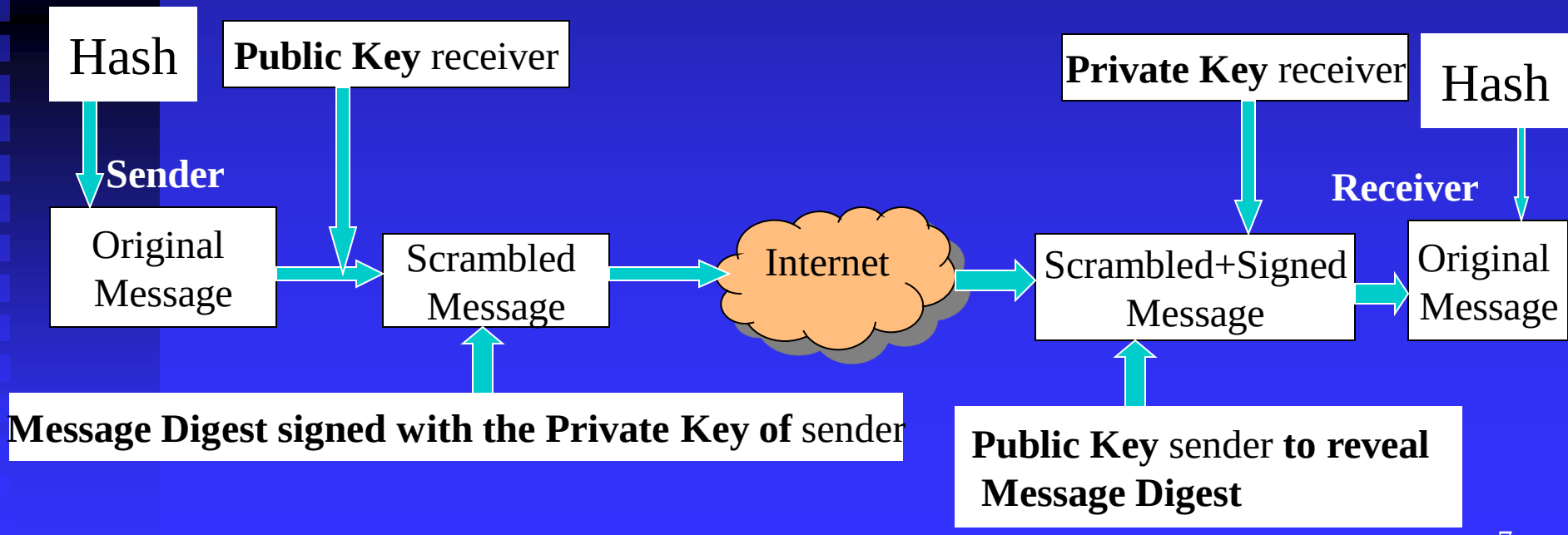
- A trusted public/private body that attests the association of a particular individual with his/her corresponding public key
- Signs digital certificates with its private key
- Hierarchy of CA's
- Can issue different types of digital certificates attaching different levels of trust

# Hash Function & Message Digest

- Hash function is a one-way mathematical function applied to a message
- Result of the hash function is unique to each message called Message Digest
- A message digest is a single large number typically between 128 and 256 bits in length

# How Digital Signature Technology Works?

The Process of Sending Messages Using Public Key Cryptography



# Steps Involved in Digital Signature Process

1. Hash function is applied to the original message in order to find the message digest
2. Public Key of the receiver is used to encrypt the message
3. A digital signature is attached to the scrambled message by signing the message digest with Private Key of the sender
4. The encrypted message, the digital signature and the hash function are sent to the receiver
5. Public Key of the sender is used by the receiver to reveal the message digest and, thus, to confirm identity/authenticity of the sender
6. Receiver uses his/her Private Key to decrypt the message
7. Receiver applies hash function to the received original message and computes the message digest – if this message digest matches with the one received from the sender, it confirms that the message has not been altered during transmission

# Public Key Infrastructure (PKI)

- A structured system that provides key management facilities, storage and management facilities of digital certificates and involves a certification authority
- Application of PKI
  - Online contracts
  - E-Banking – electronic payment systems such as electronic checks, credit card based systems, electronic cash, micro payment systems

# Key Length

- A cryptographic key is represented as a string of binary digits – 0's & 1's inside a computer
- If a key is 1 bit in length it means two possible keys, that is, 0 and 1. If a key is 2 bits in length it means four possible key values, 00,01,10 and 11
- Key having 3 bits length can have values - 000,001,010,011,100,101,110,111
- Number of keys = $2^{(\text{number f bits})}$

# Symmetric Key Algorithms

- DES (Data Encryption Standard) – 56 bits
- IDEA (International Data Encryption Algorithm (IDEA) – 128 bits
- RC2 – (block cipher) 1-2048 bits
- RC4 (stream cipher) – 1-2048 bits
- Rinjdael – 128-256 bits

# Attacks on Symmetric Key Algorithms

- Key Search Attacks
- Cryptanalysis
- System-based Attacks

# Attacks on Symmetric Key Algorithms…

- Key Search (Brute Force) Attacks – attempt to decrypt the message with every possible key
  - The greater the key length, the more difficult it is to identify the key
  - If there were a computer that could search a billion keys per second, and if you had a billion of these computers, it would still take 10783 billion years to search all possible 128 bit keys

# Attacks on Symmetric Key Algorithms…

- Cryptanalysis – encryption algorithms can be defeated by using a combination of sophisticated mathematics and computing power so that many encrypted messages can be deciphered without knowing the key
- System-Based Attacks – attack the cryptographic system that uses the cryptographic algorithm without actually attacking the algorithm itself

# Public Key Algorithms

- DSS – Digital Signature Standard based on DSA (Digital Standard Algorithm) – key length is between 512-1024 bits
- RSA
  - developed in 1977 by three professors at MIT
  - provides basis of existing digital signature technology
  - key may be of any length depending on the system
- Elliptic Curves

# Attacks on Public Key Algorithms

- Key Search Attacks – these attacks attempt to derive a private key from its corresponding public key with the use of a large factoring number
- Analytical Attacks – uses some fundamental flaw in the mathematical problem on which the encryption system is based

Global Chartered Accountants

www.gcaofficial.org