



Introduction to Public Key Infrastructure (PKI)

by
Jim Fisher

Presentation Overview

- **Information Assurance Needs**
- **Symmetric and Asymmetric Encryption**
- **Digital Signature**
- **Public Key Infrastructure**
- **Security Benefits of Public Key Infrastructure**
- **A Word About Standards...**

Information Assurance Needs

- **Assurance that:**

- Information and information systems are not accessed by unauthorized persons or systems
- Information stored on computer media or that is in transit is not altered without authorization
- The information originator is whom she or he claims to be
- The information originator cannot deny the data content

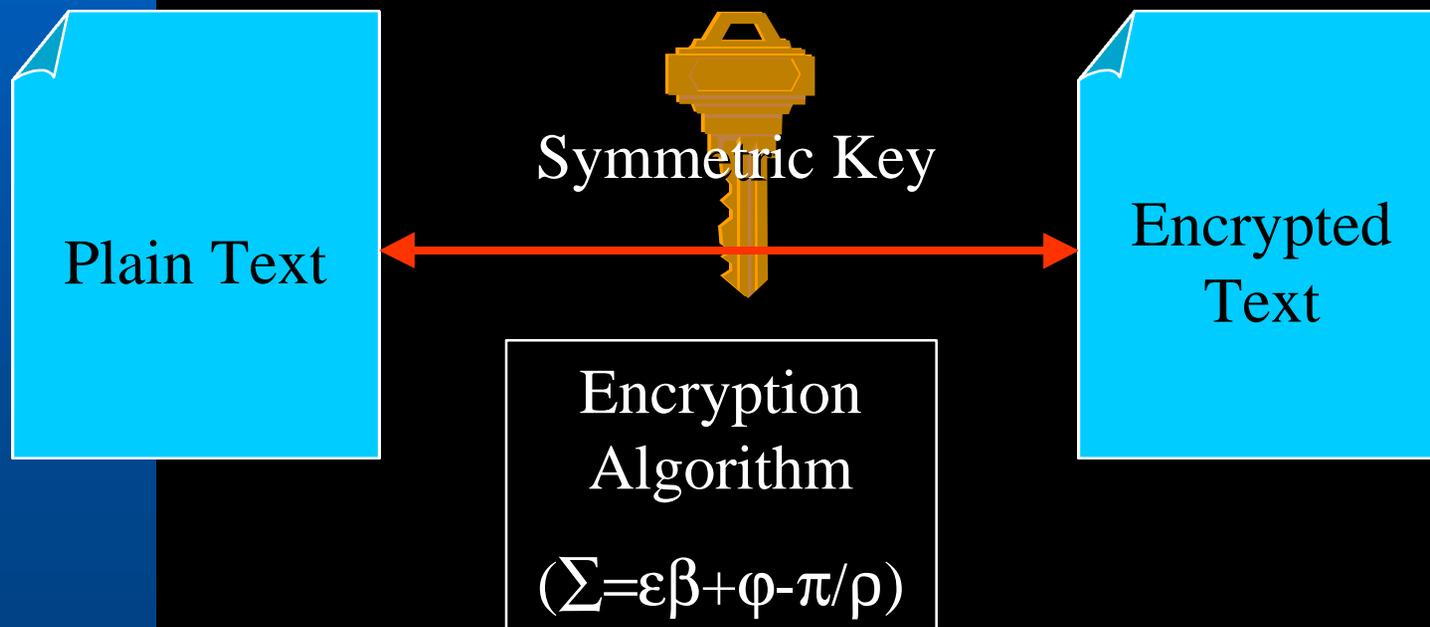
Security Benefits of Public Key Infrastructure

- **Identification and Authentication**
- **Confidentiality**
- **Digital Signature**
- **Data Integrity**
- **Non-Repudiation**

Encryption

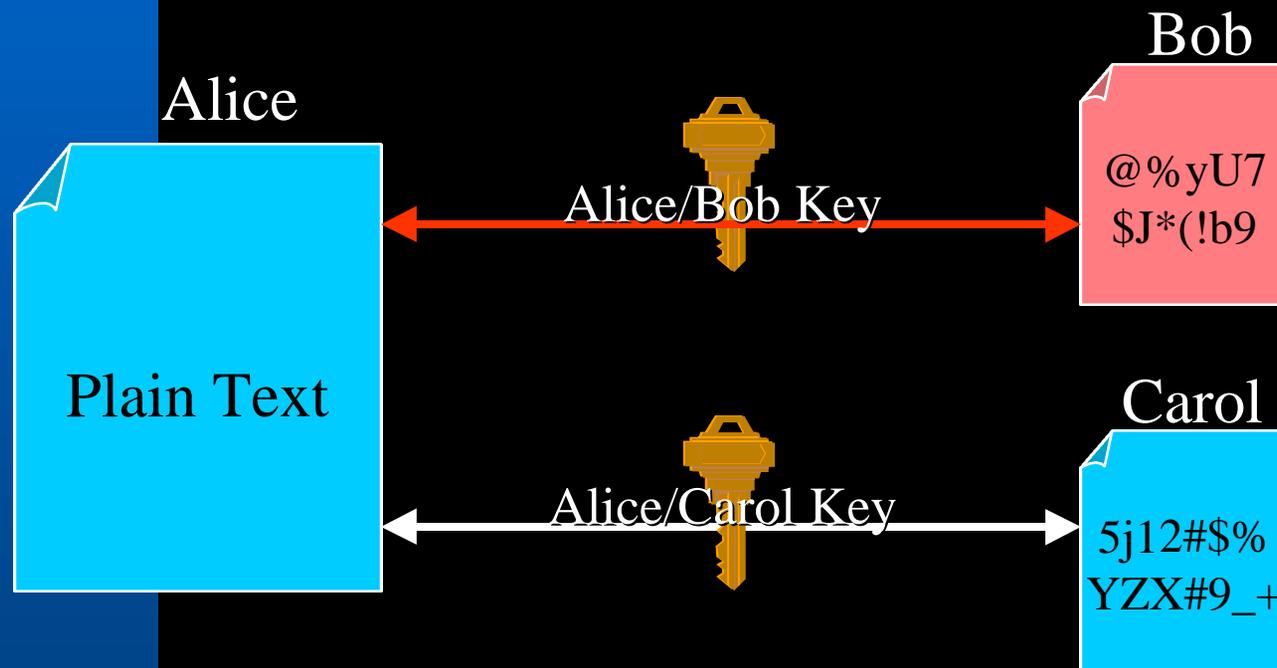
- **Symmetric (single) Key Encryption**
- **Asymmetric Key Encryption (called public key encryption)**

Symmetric (Single) Key Encryption



➡ Symmetric key encryption uses the same key to encrypt and decrypt.

Symmetric (Single) Key Encryption

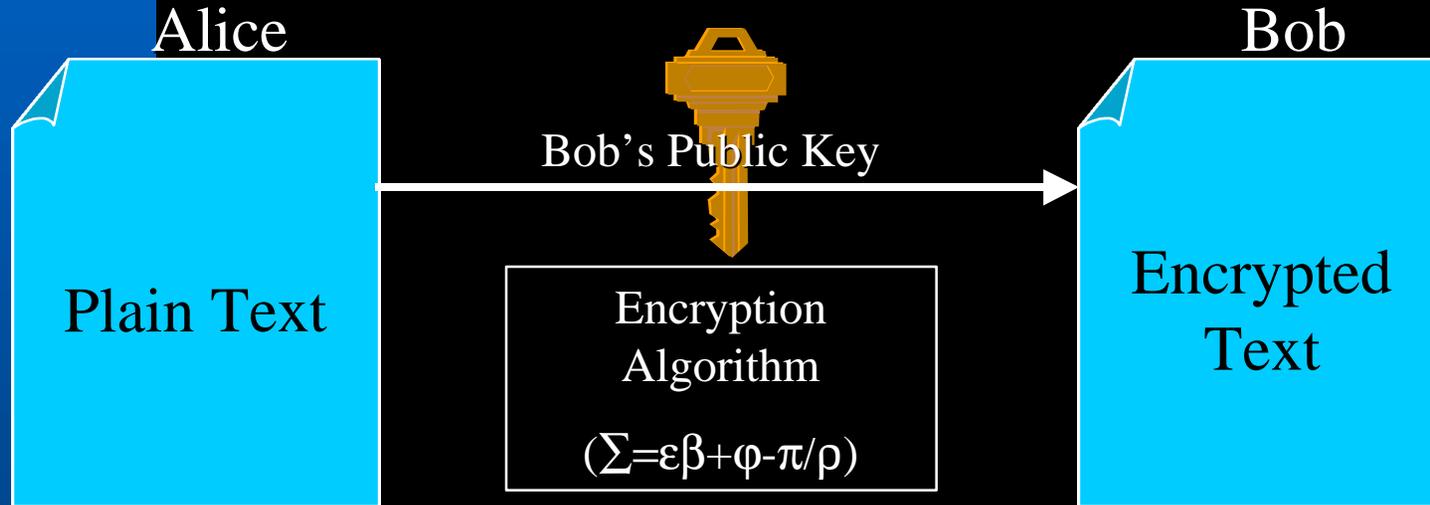


➡ Different symmetric keys result in different encrypted products.

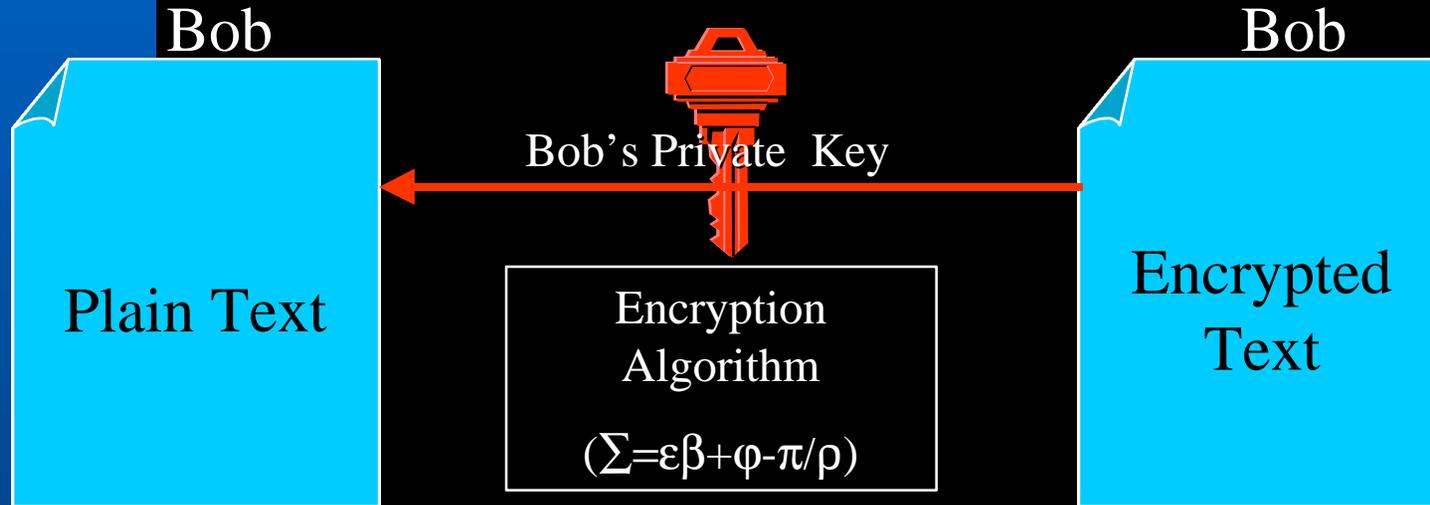
Asymmetric (Public) Key Encryption

- **Two mathematically related keys (called a key pair)**
- **Neither key can be easily calculated from the other**
- **Either key may be used to encrypt , but requires the other key to decrypt**
- **One key private (secret), the other public**

How Asymmetric (Public) Key Encryption Works

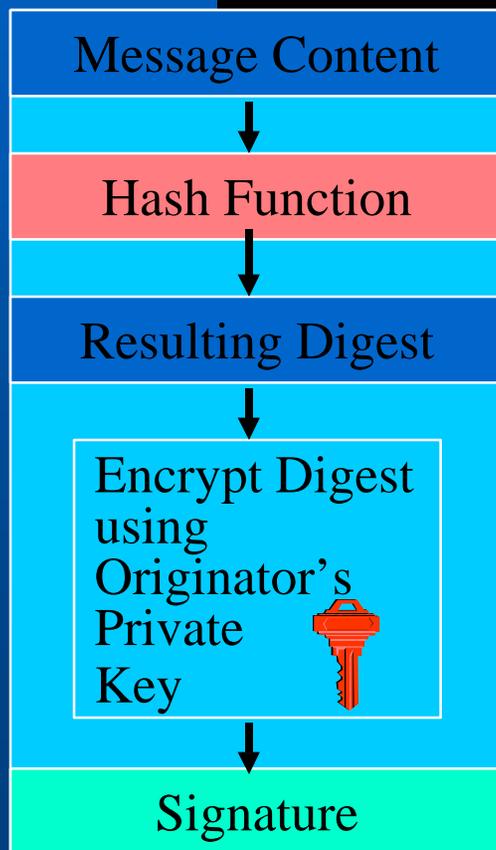


How Asymmetric (Public) Key Encryption Works



How Digital Signature Works

Originator



What A Digital Signature Looks Like

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

This is a sample message that demonstrates what a digital signature looks like.

Pretty Good Privacy, otherwise known as PGP, was used to create the digital signature.

Other digital signatures work similar to PGP.

Jim Fisher

-----BEGIN PGP SIGNATURE-----

Version: PGP for Personal Privacy 5.0

Charset: noconv

iQA/AwUBNk3v2QGEuyNapusp
EQKbfwCfZ1URAm dlSnaIp4Hqm8ItQzI6HC8
AoLThI39uSRq70+y7t1pKbQcaZr69
=v2CX

-----END PGP SIGNATURE-----

What A Digital Signature Looks Like

-----BEGIN PGP
Hash: SHA1

This is a sample
what a digital sig

Pretty Good Priv
was used to creat

Other digital sig

Jim Fisher

-----BEGIN PGP SIG

Version: PGP for Personal Pr
Charset: noconv

iQA/AwUBNk3v2QGEuyNapus
EQKbfwCfZ1URAmDlSnaIp4Hqm8ItQzI6HC8
AoLThI39uSRq70+y7t1pKbQcaZr69
=v2CX

-----END PGP SIGNATURE-----

-----BEGIN PGP SIGNATURE-----

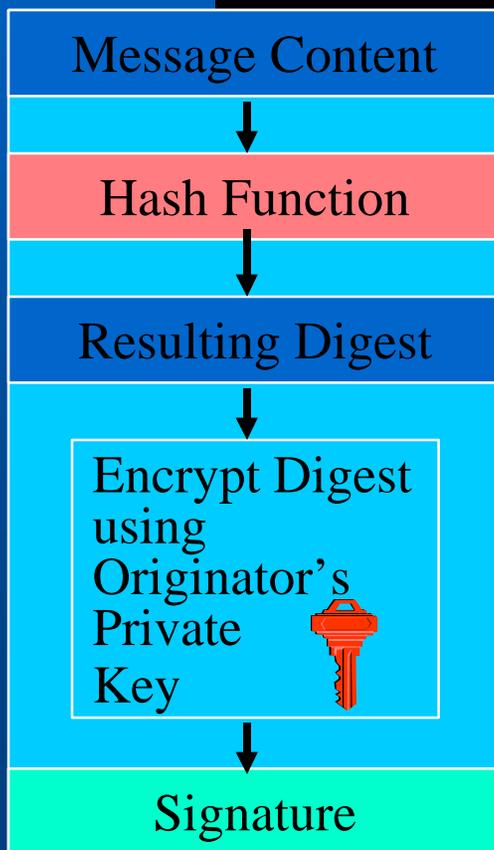
Version: PGP for Personal Privacy 5.0
Charset: noconv

iQA/AwUBNk3v2QGEuyNapus
EQKbfwCfZ1URAmDlSnaIp4Hqm8ItQzI6HC8
AoLThI39uSRq70+y7t1pKbQcaZr69
=v2CX

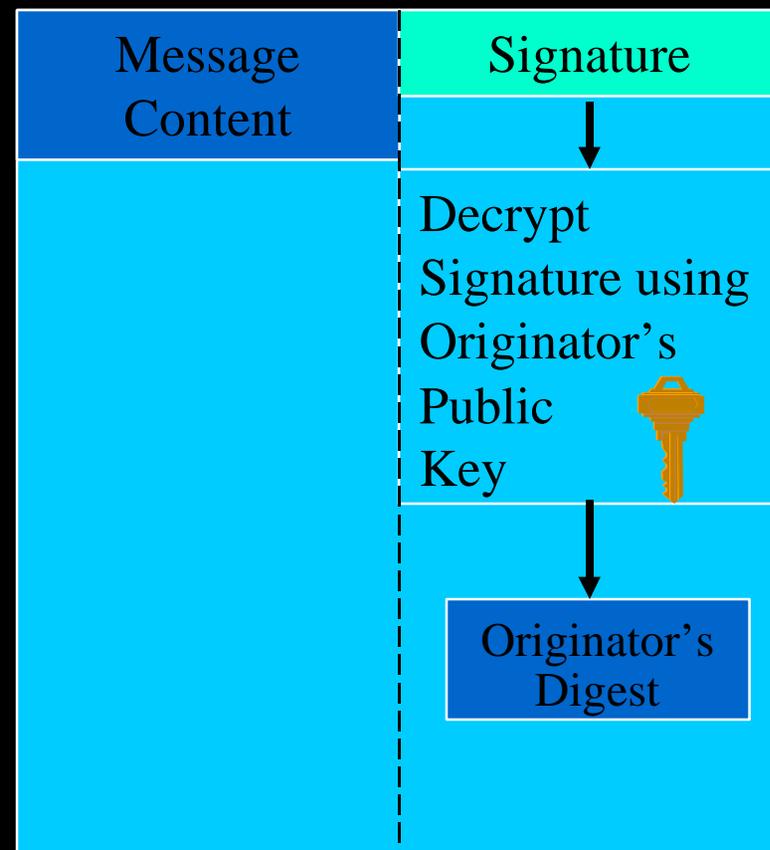
-----END PGP SIGNATURE-----

How Digital Signature Works

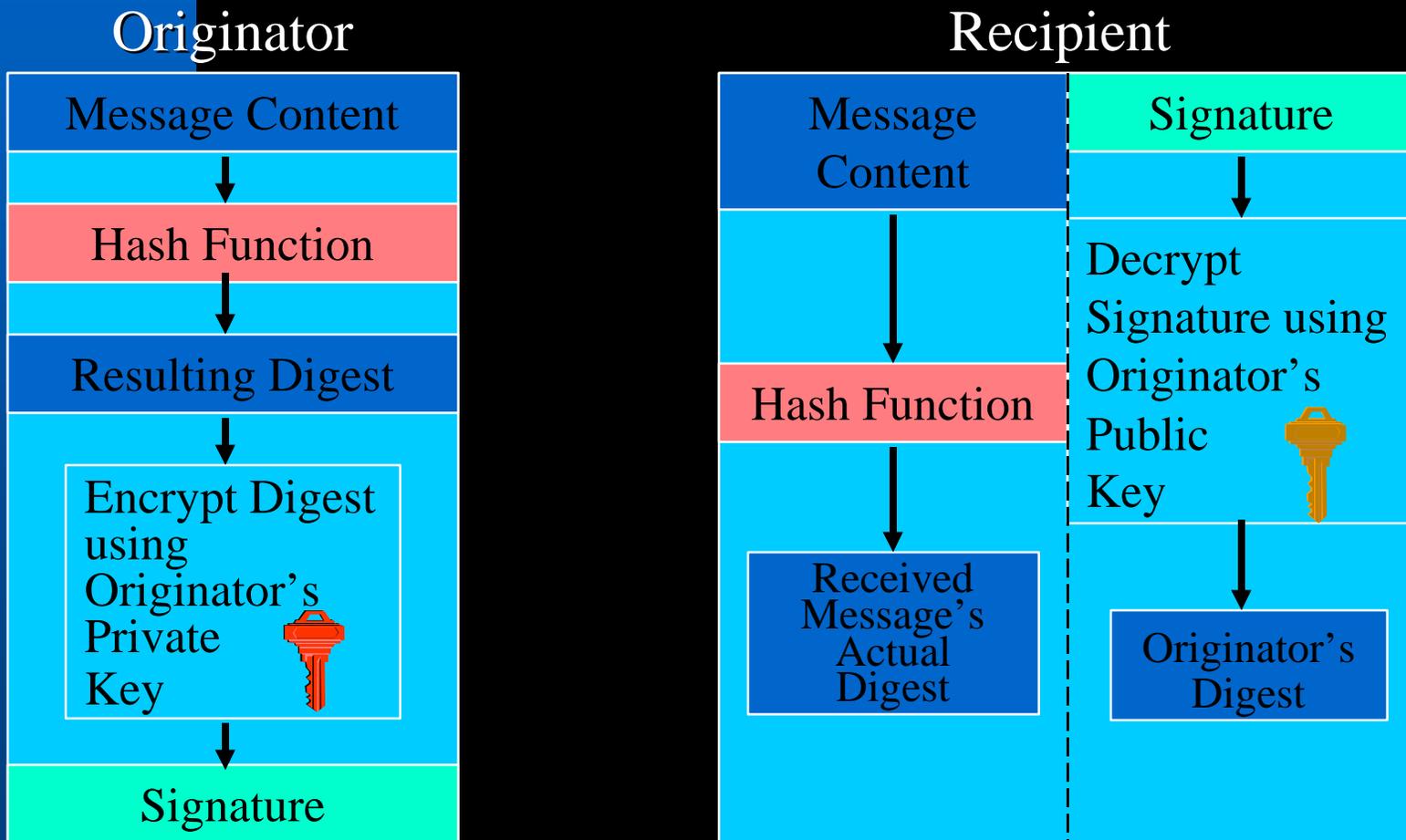
Originator



Recipient



How Digital Signature Works



How Digital Signature Works

Originator

Message Content

If digests are the same then,
the signature is verified
and
received message content is
the same as the
sent message content

Private
Key

Signature

Recipient

Message
Content

Signature

Hash Function

Received
Message's
Actual
Digest

Decrypt
Signature using
Originator's
Public
Key

Originator's
Digest



Benefits of Digital Signature

- **Signature can be validated as genuine**
- **Signature and data unalterable without detection**
- **Signature cannot be replicated**
- **Signature cannot be forged**

Digital vice Digitized Signature

- **Digital signature is the result of using a private key to encrypt a data file's digest, which can be validated by the signer's public key.**
- **Digitized signature is the bit map of a hand-written signature.**

Enhancing Security

Digital signature + Encryption

=

Enhanced security

A Note About Key Pairs

- **A single private/public key pair can be used for both encryption and digital signature (e.g., PGP)**
- **Current wisdom indicates the need for two key pairs:**
 - **One for encryption**
 - **One for digital signature**

Public Key Infrastructure Definition

- **A Public Key Infrastructure is the**
 - personnel,
 - policy,
 - procedures,
 - components, and
 - facilities
- **necessary to enable cryptographic functions**
- **so that applications can provide the desired security services.**

Three Primary Components of a Public Key Infrastructure

- **Certificate management**
- **Registration process**
- **Public key enabled applications**

Certificate Management

- **Certification Authority**
- **X.509 Certificate**
- **Certificate Repository (Directory)**

Certification Authority

- **Trusted third party**
- **Issues and publishes certificates**
 - for a population of public-key holders
 - in accordance with its published policy and practices statement
- **Issues certificate revocation lists (CRLs)**

X.509 Certificate

- **Purpose**

- Certifies that the information it contains is accurate and authentic.

- **Contains**

- Entity's Identification Information
- Entity's Public Key
- Certification Authority Name
- Certification Authority's Digital Signature

Kinds of Certificates

- **Identify**
 - Identification and authentication
 - Digital Signature
- **Encryption Certificate (sometimes called e-mail certificate)**
- **Server Certificate (SSL)**

Certificate Repository (Directory)

- **Certificate Authority publishes X.509 certificate in repository (generally a directory)**
- **Repository may be:**
 - **Public**
 - **Private**
 - **Combination public and private**

Registration Process

- **Registration Authority**
 - Identifies and authenticates subscriber
 - Issues user_ID and one-time password to subscriber
 - Securely relays user_ID and password to Certification Authority
 - May use a trusted agent for authentication

Public Key Enabled Applications

- Applications must be enabled for public key technology use
- Should be standards based (e.g., ISO, FIPS)
- Should be interoperable
- Should support multiple public key and hash algorithms

Security Benefits of Public Key Infrastructure

- **Confidentiality**
- **Enhanced Identification and Authentication**
- **Digital Signature**
- **Data Integrity**
- **Non-repudiation**

Confidentiality

- Provides a reliable solution for originator-to-recipient encryption, *independent* of point-to-point or inline encryption
- Public key encryption can be used in addition to inline encryption

Enhanced Identification and Authentication

- **Relying party uses entity's identity certificate for identification and authentication**
- **Relying party validates certificate , increasing assurance that entity is the actual claimant**
- **Uses — Log-on, IPSEC, VPNs**

Digital Signature

- **Signature can be validated as genuine**
- **Signature and data unalterable without detection**
- **Signature cannot be replicated**
- **Signature cannot be forged**

Data Integrity

- **Digital signature ensures that data cannot be altered from the time the data was signed without detection**
- **Encryption ensures that data cannot be modified without authorization**

Non-Repudiation

- **Digital signature makes it difficult for:**
 - **The signing party to deny:**
 - That he or she was not the originator
 - **The signing party or the recipient to claim:**
 - That the contents of the data received is different from the data that was sent

A Word About Standards and Government Information

- **Federal Information Processing Standards (FIPS) published by NIST**
- **International Telecommunication Union - Telecommunication (ITU-T) for X.509v3 standards**
- **Public-Key Cryptography Standards (PKCS) from RSA, Inc.**
- **International Standards Organization (ISO)**
- **Internet Engineering Task Force (IETF)**

Algorithms

- **Data Encryption Standard (DES)**
- **Digital Signature Algorithm**
- **RSA, Elliptical Curve and others**
- **Secure Hash Algorithm - 1 (SHA-1)**
- **Proprietary**

Federal Information Processing Standards (FIPS)

- **FIPS 46-2, 74, & 81—Data Encryption Standard**
- **FIPS 140-1—Security Requirements for Cryptographic Modules**
- **FIPS 180-1—Secure Hash Standard**
- **FIPS 186—Digital Signature Standard**
- **FIPS 196—Entity Authentication Using Public Key Cryptography**

Good Book...

- ***Secure Electronic Commerce: Building the Infrastructure for Digital Signatures & Encryption*, by Warwick Ford & Michael S. Baum, Pub: Prentice Hall, © 1997, ISBN: 0-13-476342-4, Cost ~\$50**

For More Information...

- **Army PKI -**
www.army.mil/doim/pkiweb/default.cfm
- **DISA PKI -** www.disa.mil/infosec/index.html
- **Government Information Technology Services**
 - gits-sec.treas.gov/
- **NIST PKI -** csrc.nist.gov/pki/
- **Miscellaneous**
 - www.tbq.com/samples/netsvcs/pkiarcc.htm
 - www.iword.com/iword32/istory32.html

PKI Point of Contact

Jim Fisher (PKI Support Contractor)

Voice: (703) 604-7583

DSN 664-7582

Fax: (703) 601-0742

E-mail: fisherj2@hqda.army.mil



Questions?