PKI FUNDAMENTALS

Sarbari Gupta

sarbari@electrosoft-inc.com

3/23/12

OUTLINE OF PRESENTATION

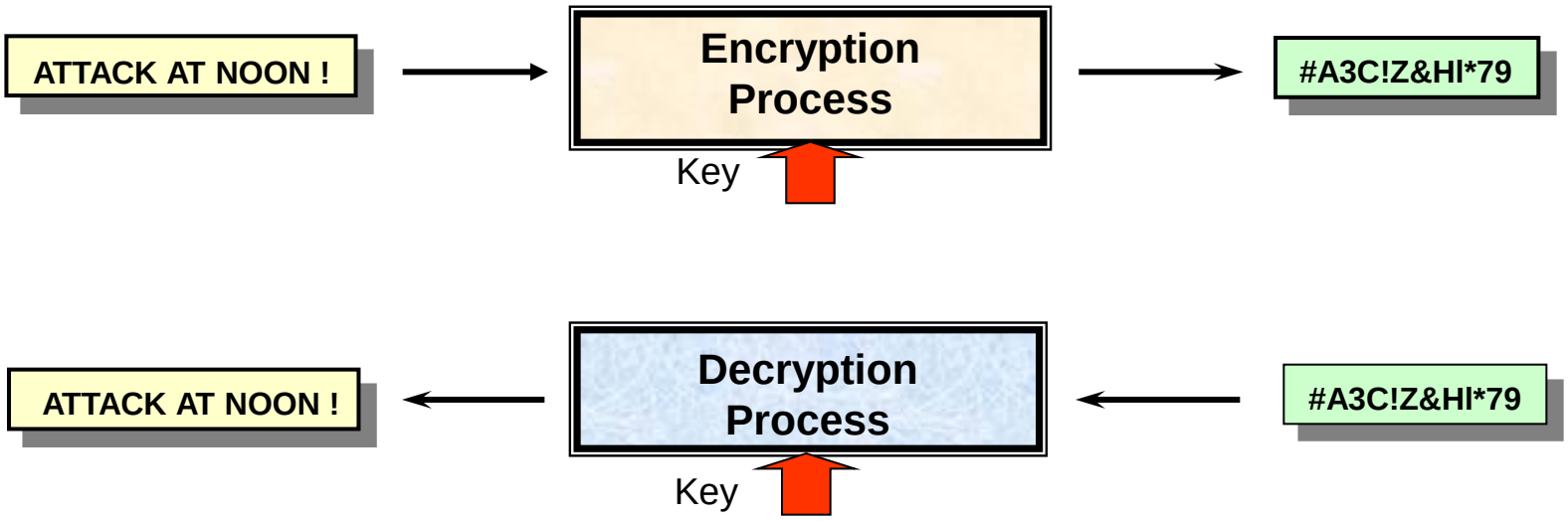
- **Cryptographic Algorithms**
  - **Symmetric Key**
  - **Public Key**
  - **Message Digest**

- **Public Key Functions**
  - **Data Encryption**
  - **Bulk Data Encryption**
  - **Digital Signature**

- **Public Key Infrastructure**
  - **Public Key Certificate**
  - **PKI Architectural Entities**
  - **CP/CPS**
  - **Path Processing**
  - **Revocation**

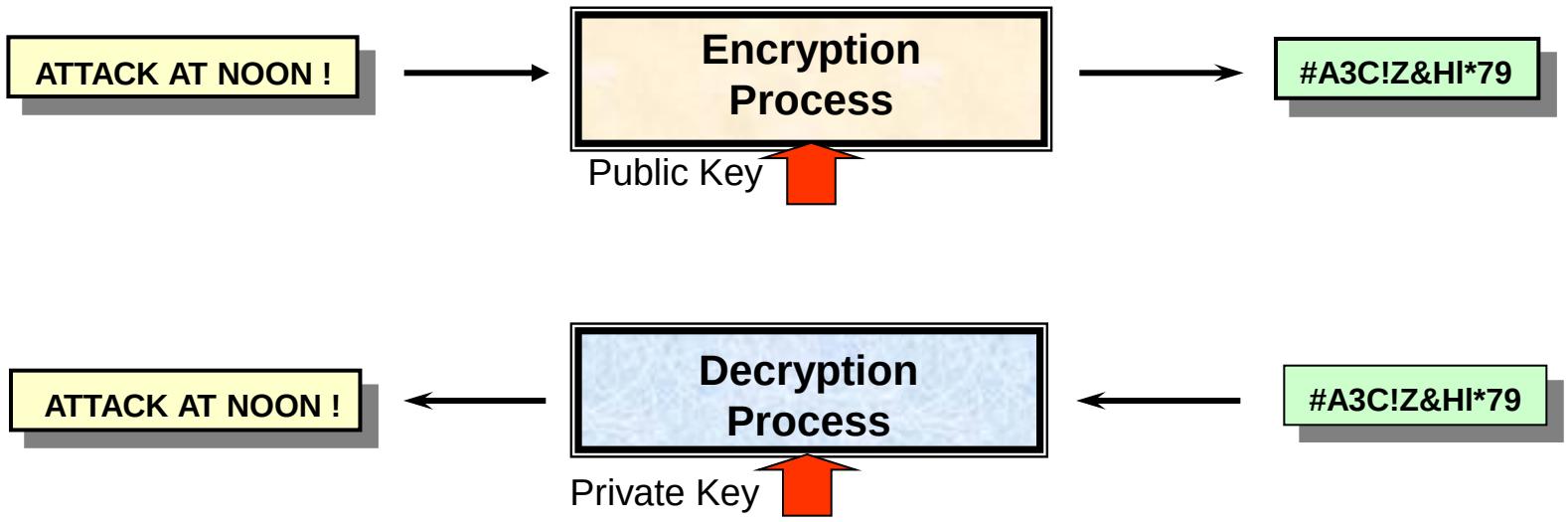
CRYPTOGRAPHIC ALGORITHMS - SYMMETRIC KEY

- **Same key is used for encryption and decryption**
- **Key needs to be kept secret from all except sender and receiver**



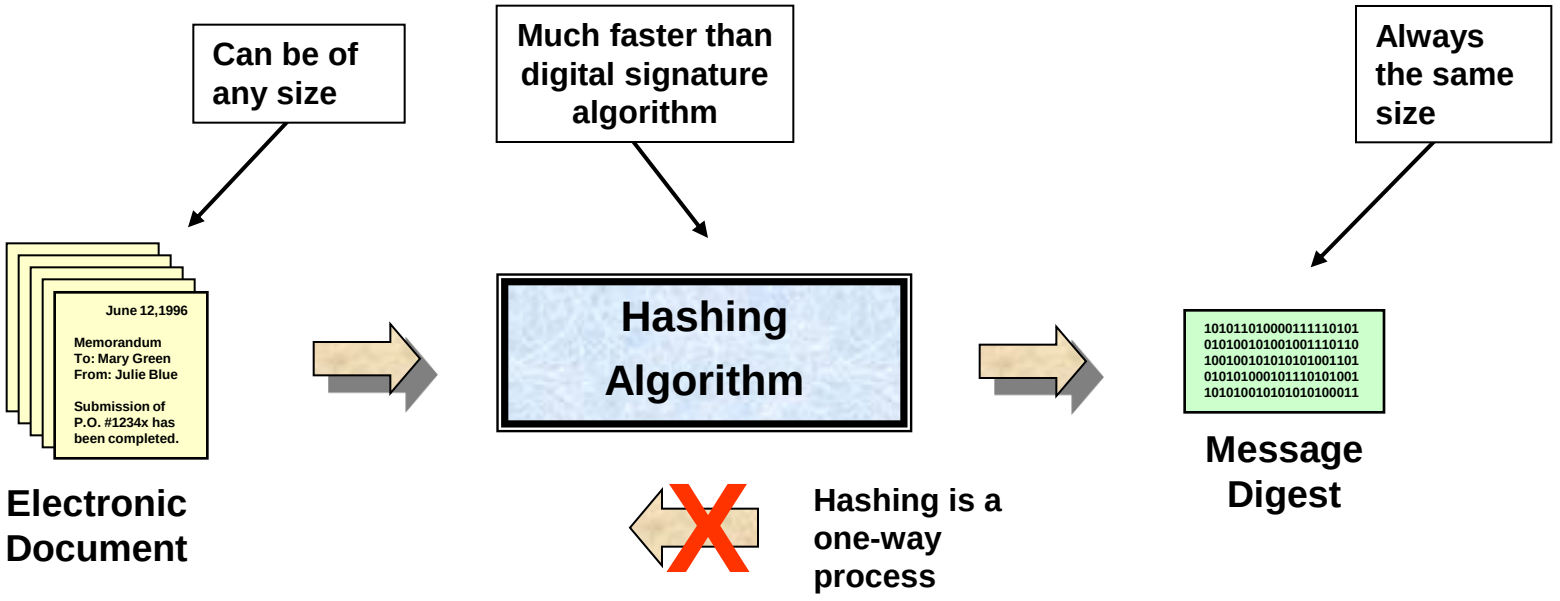
CRYPTOGRAPHIC ALGORITHMS - PUBLIC KEY

- Public key used for encryption
- Private key used for decryption
- Public key is widely distributed
- Private key held closely by key owner
- Private key cannot be calculated from public key

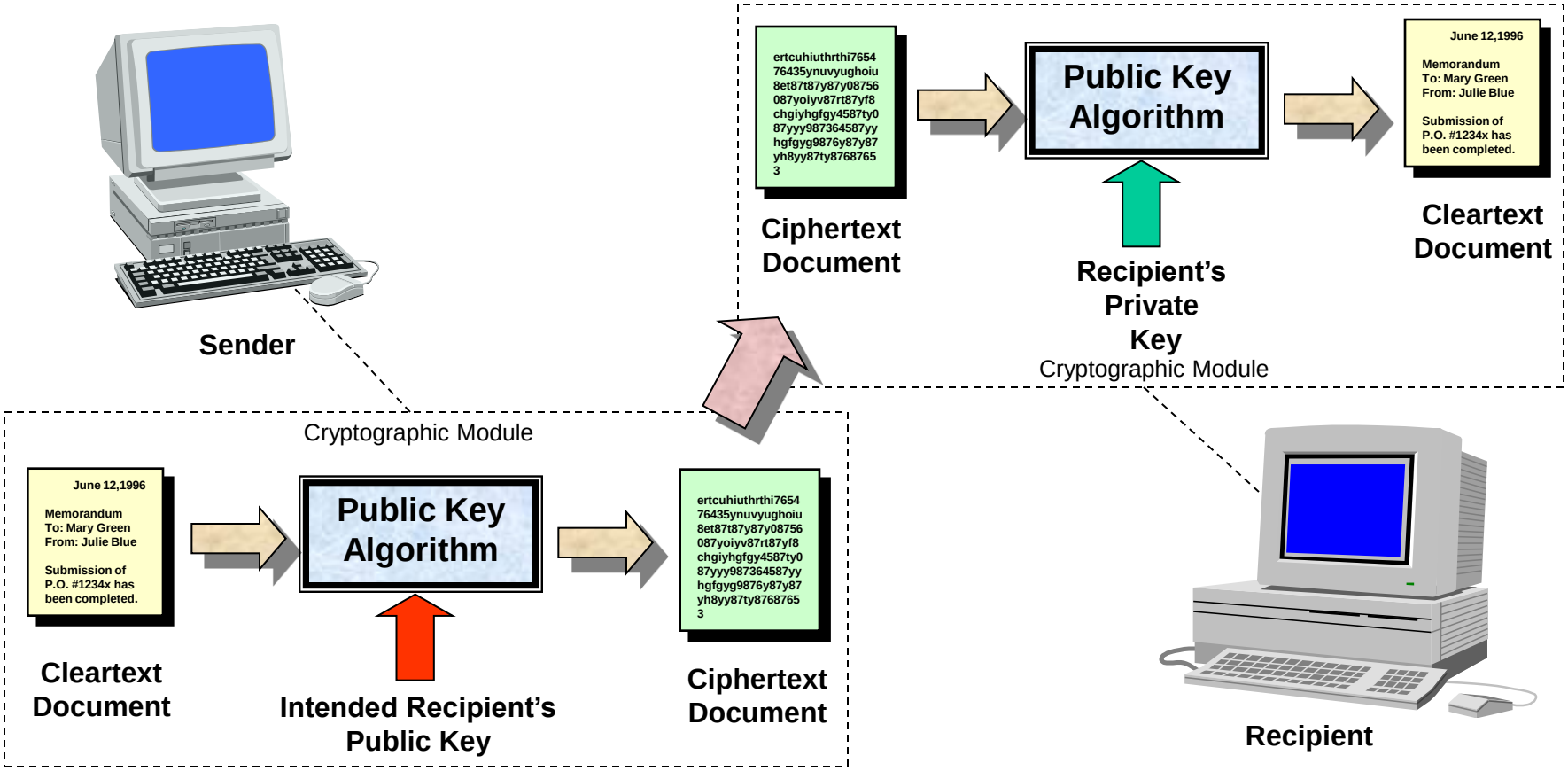


CRYPTOGRAPHIC ALGORITHMS
MESSAGE DIGEST

- **Each electronic document produces a unique message digest (non-collision property)**
- **The message digest cannot be used to calculate the original electronic document (one-way property)**

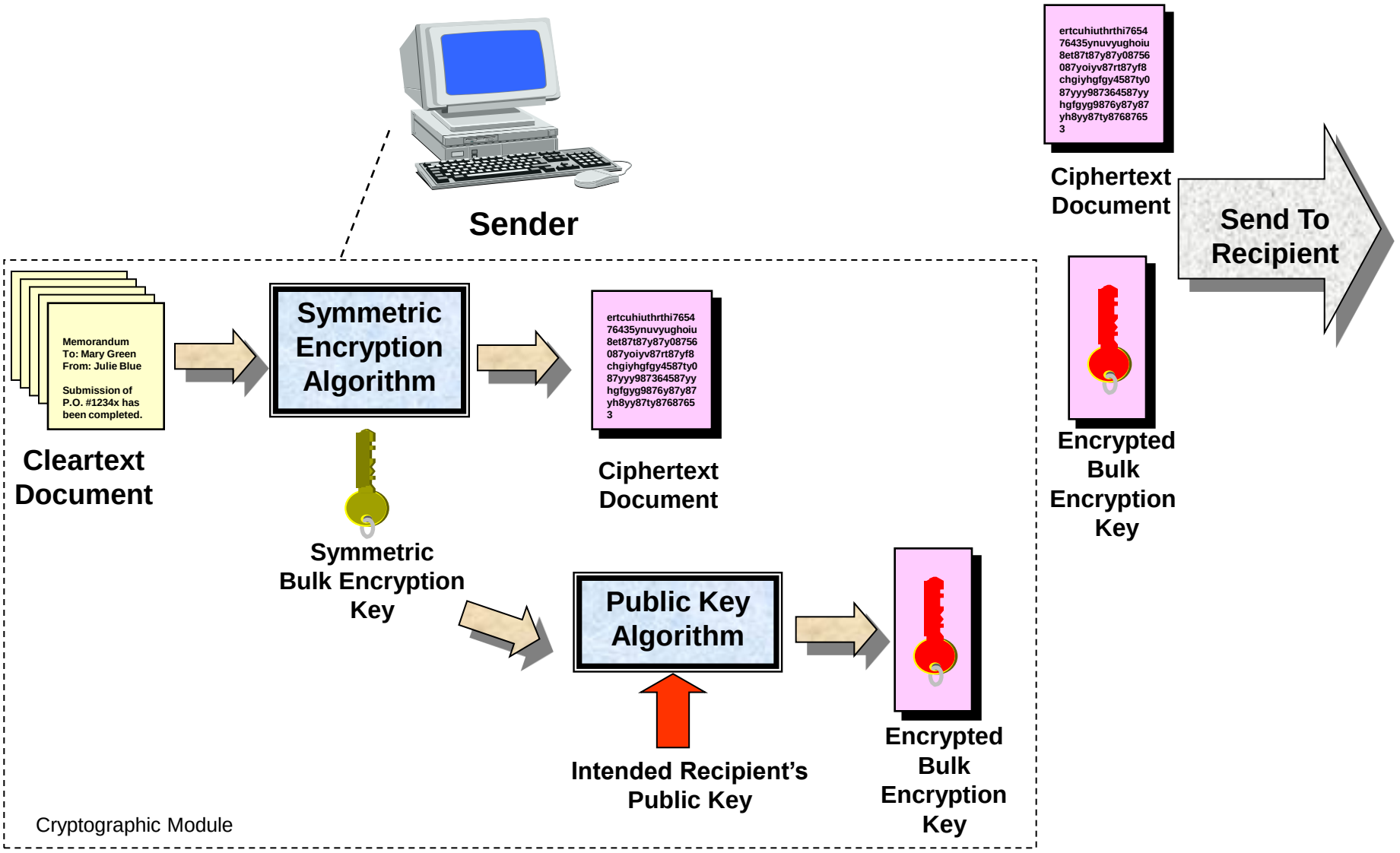


PUBLIC KEY - ENCRYPTION OF DATA

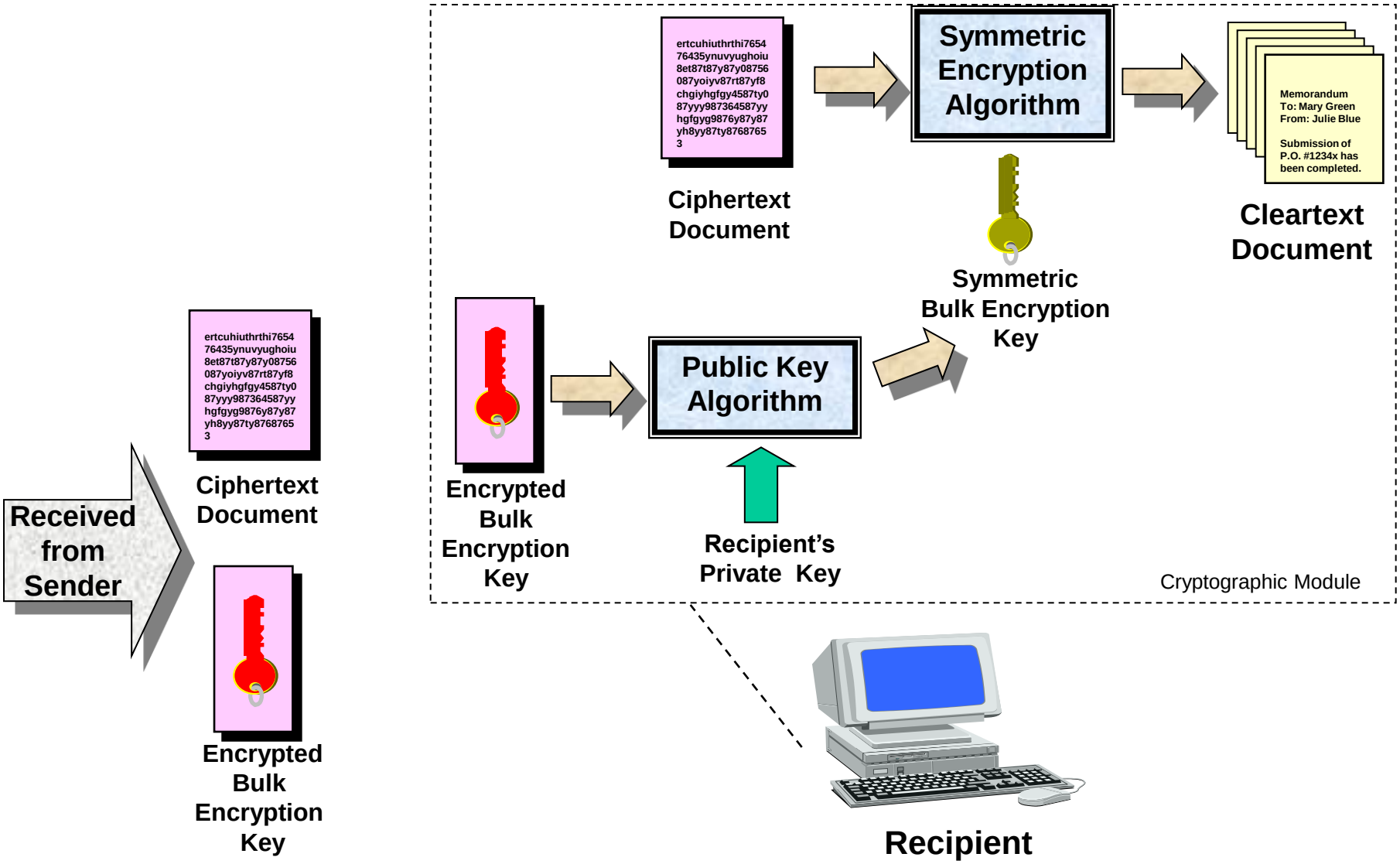


- **The sender uses the intended recipient's Public Key to encrypt the document.**
- **Only the intended recipient can decrypt the document, because only the intended recipient has the required Private Key.**
- **Public Key encryption can only handle small amounts of data**

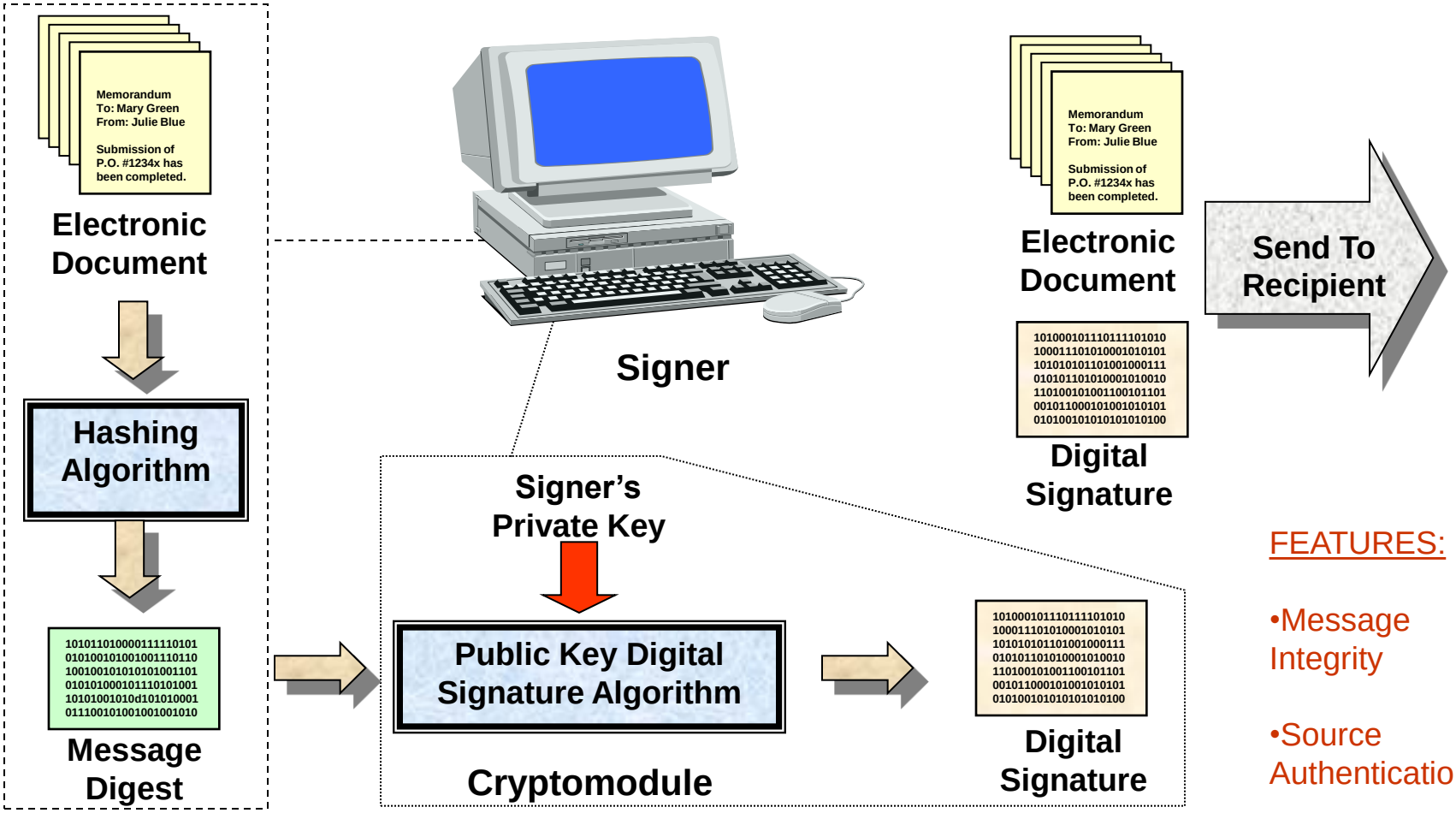
PUBLIC KEY – BULK DATA ENCRYPTION



PUBLIC KEY – BULK DATA DECRYPTION



DIGITAL SIGNATURE - GENERATION

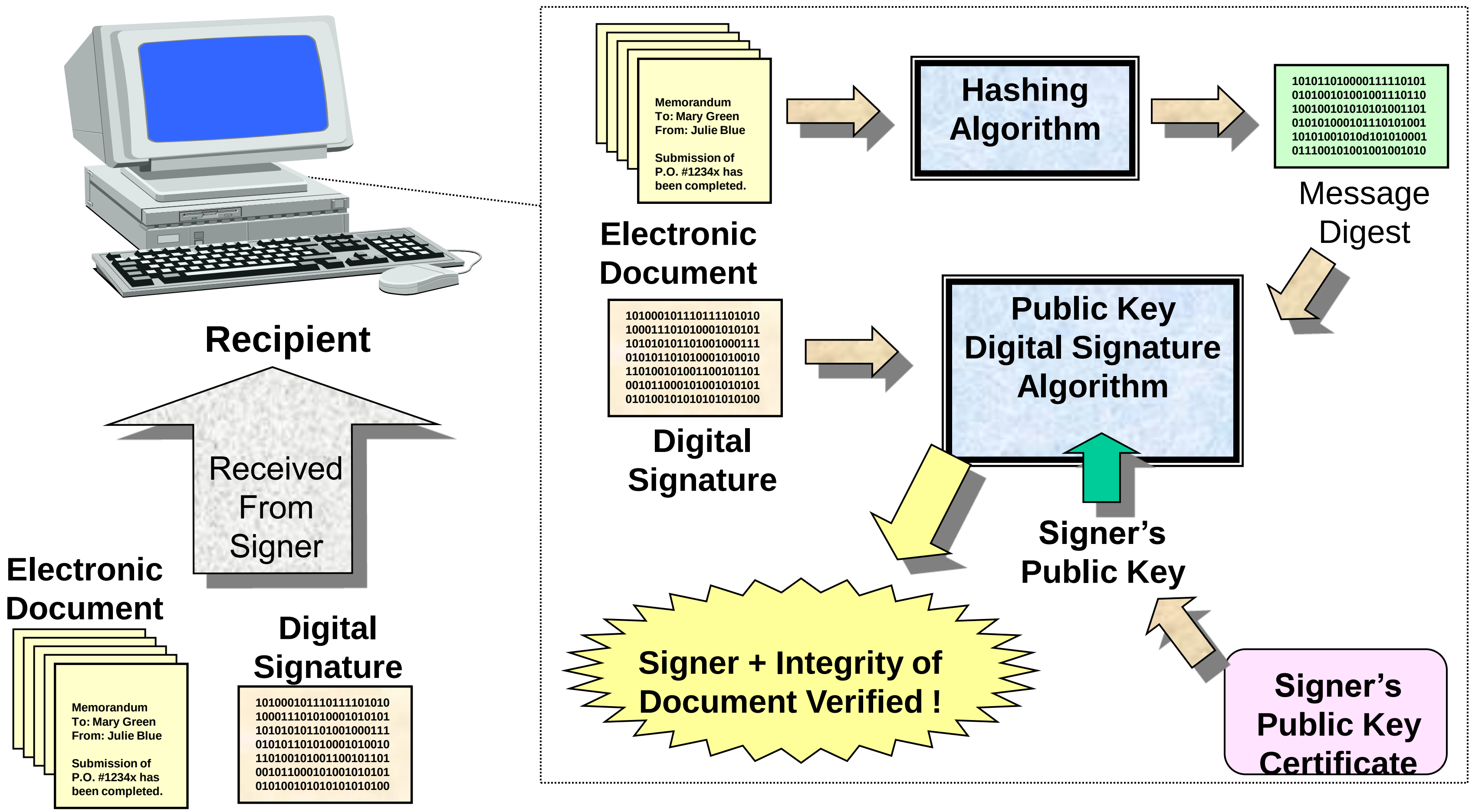


FEATURES:

- Message Integrity
- Source Authentication
- Sender Non-Repudiation

- The Hashing algorithm creates the message digest from the original document
- The Public Key Digital Signature Algorithm uses the message digest and the signer's private key to generate the digital signature

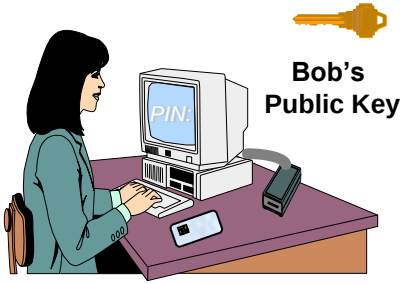
DIGITAL SIGNATURE - VERIFICATION



•The Public Key Digital Signature Algorithm requires the presence of the message digest, the digital signature as well as the signer's public key in order to verify the signer and integrity of the document

ESTABLISHING TRUST IN PUBLIC KEYS

- **How can Alice tell if she has the correct public key for Bob ?**
- **Need a mechanism to pair up public keys and their owners**
- **Need a mechanism to trust the pairing of public keys and their owners**

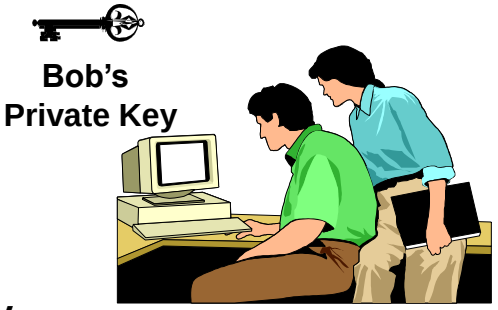


Alice

- Obtain Bob's public key
- **Establish trust in Bob's public key**
- Encrypt message using Bob's public key

#A3C!Z&Hl*79%*$YZ&@

Message Scrambled using Bob's public key



Bob

- Use (Bob's) private key to unscramble message

PUBLIC KEY CERTIFICATE

- Permanent vouching by trusted third party of someone's public key (certification of that key)
- Binds an entity (name, id) to a specific public key
- Everybody who accepts that certifier's authority can verify the binding between public key and identity
- Certification Authority

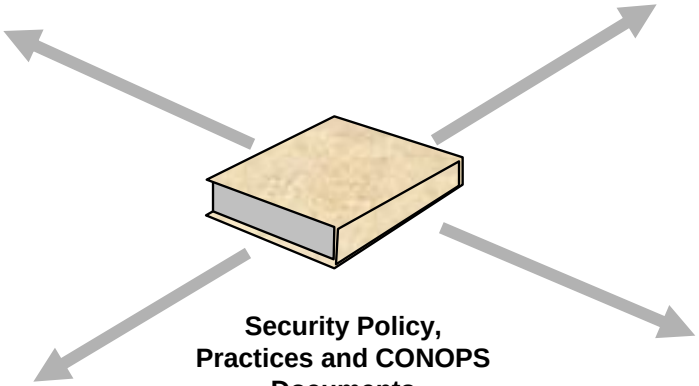
PKI ARCHITECTURAL ENTITIES

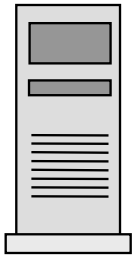
Certification Authority

A trusted entity that:

- Is centrally located
- Operated under control of Security Officer(s)
- Generates Public Key Certificates
- Revokes Public Key Certificates
- Publishes Public Key Certificates and Certificate Revocation Lists in Directory Servers
- Archives Public Key Certificates and Certificate Revocation Lists in Archive

Certificate Archive
Contains an archive of all Certificates and CRL's





Security Policy, Practices and CONOPS Documents

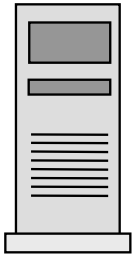
Directory Server
Contains valid Public Key Certificates and Certificate Revocation Lists

Organization Registration Authority

A trusted entity that:

- Is located at each geographical location of the organization
- Issues Token Cryptomodules to users
- Oversees key generation
- Verifies and vouches for the identity of users
- Generates and signs Requests for Issuance of a Public Key Certificate
- Sends Request to the Certification Authority

Trusted Time Stamp Server
Provides trusted time stamps for signatures and critical events



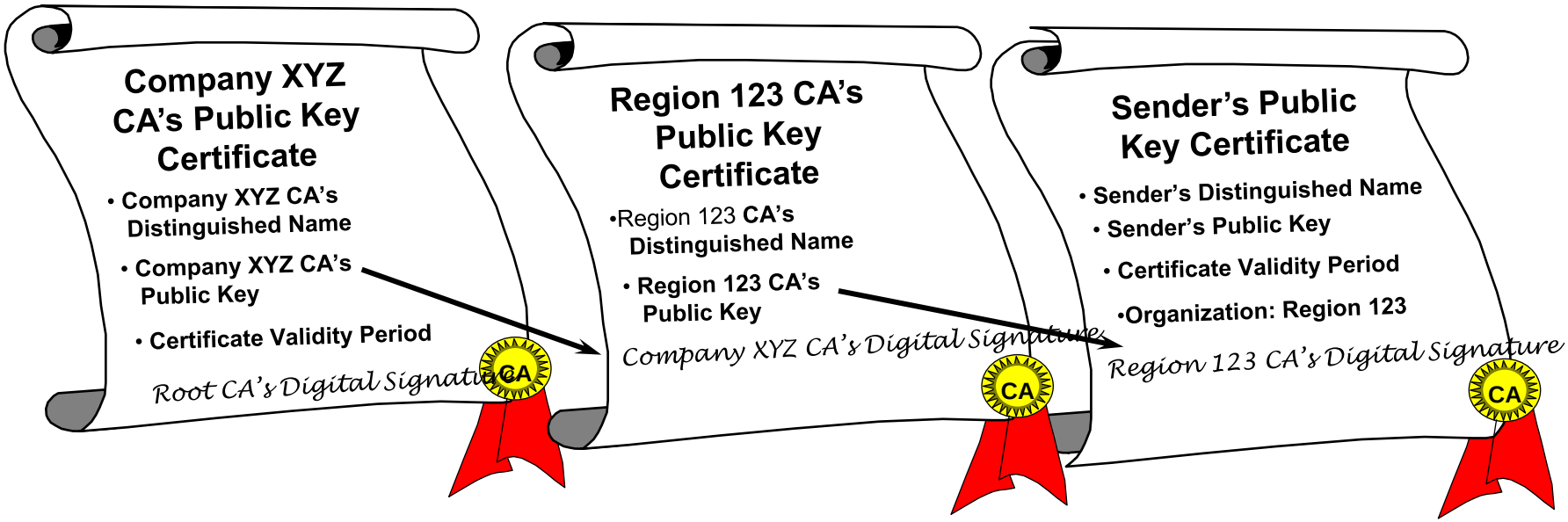
CERTIFICATE POLICY & CERTIFICATION PRACTICES STATEMENTS

- A **certificate policy** (CP) is defined as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements." [1]
- A **certification practices statement** (CPS) is "a statement of the practices which a certification authority employs in issuing certificates." [2]

1 "Information Technology - Open Systems Interconnection:The Directory: Authentication Framework," 1997 edition.

2 American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Electronic Commerce, 1995.

CERTIFICATION PATH PROCESSING



- Receiver knows the Root CA's Public Key
- Receiver has the Sender's Public Key certificate
- Receiver develops a chain of certificates beginning with a Root CA signed certificate and ending with the Sender's certificate

DISTRIBUTION OF PKI DATA OBJECTS

Public key infrastructure data objects need to be distributed to the subscribers and relying parties:

- Subscribers need their newly issued certificates
- Relying parties need certificates and CRLs for their peers

PUBLIC KEY TECHNOLOGY - THE REVOCATION LIST

- **QUESTION: Suppose Bob's Private Key is stolen, or suppose Bob is fired and becomes a disgruntled employee. How do we warn people not to trust anything encrypted or signed using Bob's key?**

- **ANSWER: The CA can revoke a Public Key Certificate by adding it to an unforgeable electronic Certificate Revocation List (CRL), which is made public and updated regularly.**

  - **A user reports a compromise of his public key to the CA, or an appropriate official instructs the CA to revoke a particular user's certificate.**

  - **The CA adds the user's public key certificate, with clarifying information, to the electronic Certificate Revocation List and signs it with the CA's digital signature.**

  - **The CA posts the updated CRL to the on-line public database or directory, where the CRL is maintained.**

  - **Anyone can obtain and verify the authenticity and integrity of the Certificate Revocation List using public key technology. Thus, the status of a Certificate can be obtained from the CRL and trusted.**