Enhanced Security through Authentication and Encryption

SSL and Certificates

Cryptography

- The process of using or the study of electronic security systems, methods, or schemes that protect data by altering it in some way so that only the intended recipient is able to extract the original information

Encryption

- Enables secure communications over any network
- Transforms data files (e-mail message, document, executable file) into a form that is unreadable and unusable by anyone except the intended recipient

Decryption

- Reverse process that returns data file to its original form
- Remember the process of encryption and decryption does not effect the actual data being transmitted

Basic Key Encryption

- Uses two primary tools, mathematical formulas or algorithms that are inverses of each other
  - Encryption key: Used by the sender to protect the data
  - Decryption key: Used by the recipient to extract the data
- Ciphertext: The encrypted data file

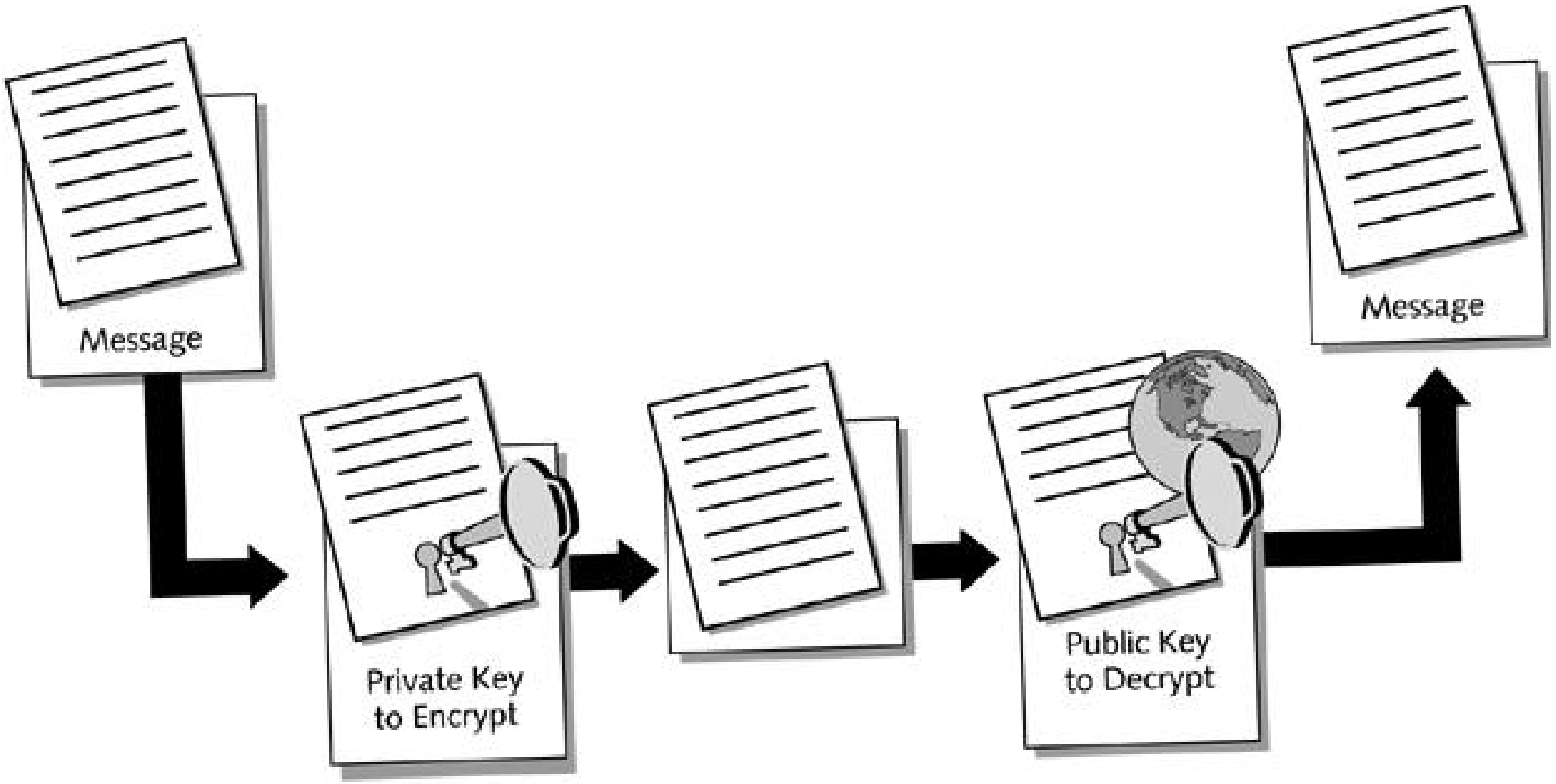

Figure 7.1 Basic key encryption.

Public Key Encryption

- Two-step encryption method that requires both the client and the server (sender and recipient) to have both a public key and a private key
- Although inverses of each other, it is impossible to derive or extract one key from the other

Private and Public Keys

- Private key
  - Applied by sender to protect message
  - Important to retain exclusive control
- Public key
  - Used by recipient to extract data
  - Freely distributed; often sent with encrypted message
  - Cannot be used to create a duplicate of private key

Digital Signatures and Secure Envelopes

- Variation of public key encryption system that adds a focus on identity verification
- Uses a dual-key system
  - Digital signature
  - Secure envelope

Digital Signatures and Secure Envelopes

- Digital signature
  - Private key of the sender
  - Proves to the recipient that the data is from the sender
- Secure envelope
  - Public key of the recipient
  - Assures the sender that the data file is deliverable only to the intended recipient

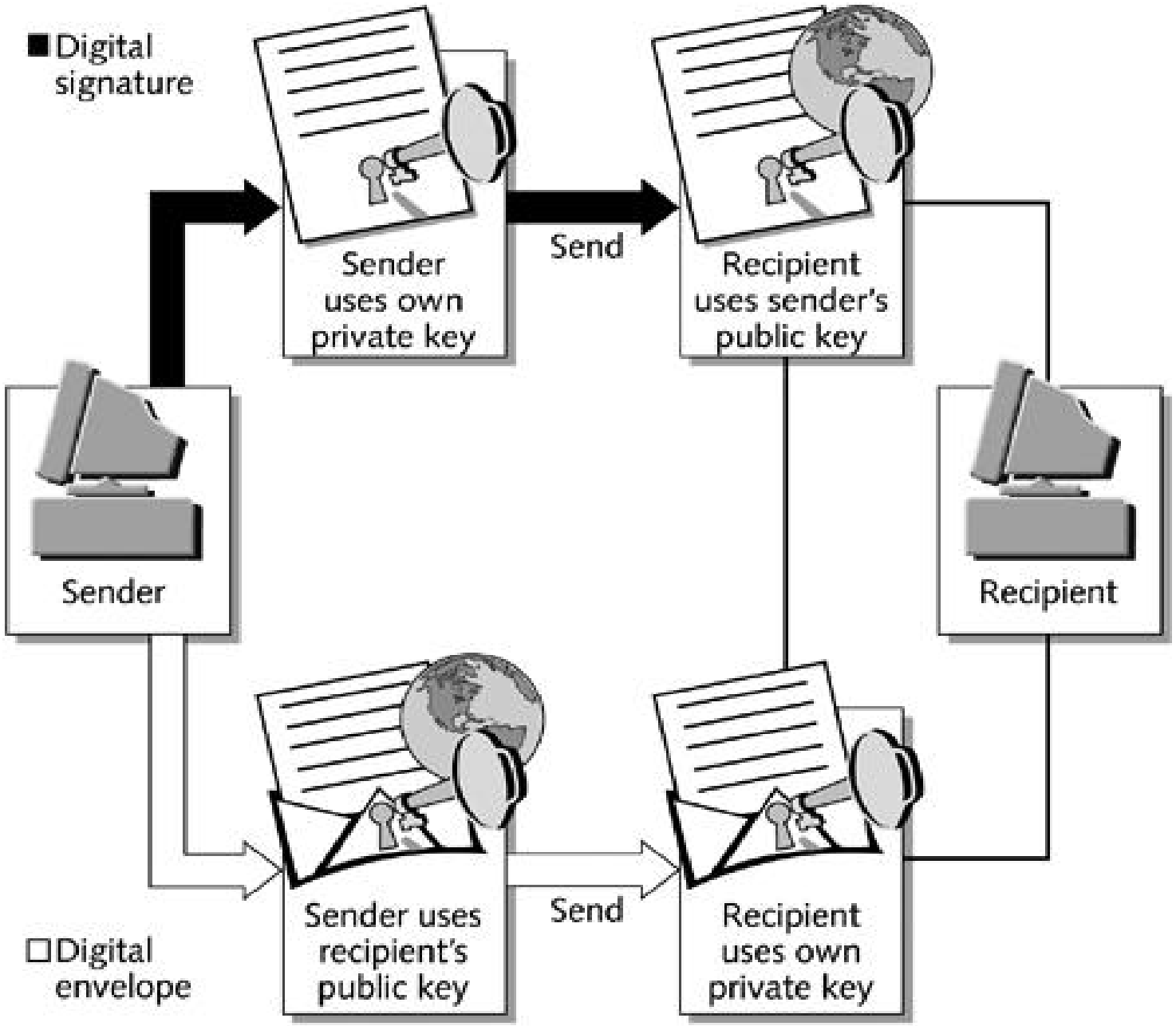

Figure 7.2 Digital signatures and secure envelopes.

Identity Verification: Certificates

- Security process that guarantees the sender of the recipient's identity or vice versa
- Performed through the use of digital certificates
  - Used to electronically prove identity of an entity (sender or recipient)
  - Issued by trusted third parties known as certificate authorities (CAs)

Identity Verification

- CAs verify identity of an entity (using the public key) and provide electronic proof of identity by issuing digital certificates
- Once identity is verified, select to:
  - *Always* accept transmissions from this entity
  - Accept transmission *only* from this session

Identity Verification

- Trust CA's verification of identity only as far as the CA itself can be trusted
- VeriSign and Thawte
  - Widely used and reliable CA's
  - Accepted by Microsoft and Netscape

Certificate Verification Failures

- Changes in site's configuration (such as IP address or domain name)
- Certificate expired
- Certificate revoked due to misconduct or site compromise

Certificate Revocation List (CRL)

- Maintained by the CA
- Lists all issued certificates that have been revoked due to expiration, misconduct, or site compromise
- Each time a new certificate is encountered, the CRL is consulted before verification is attempted

Secure Sockets Layer (SSL)

- An industry standard protocol
- Used by a webserver to establish secure communications between itself and client browsers
- A digital certificate system
- Establishes or proves identity of the server, possibly the client
- Allows server and client to agree upon a level of encryption for continued communication

SSL 3.0: Two-layered Protocol

- SSL Record Protocol
- SSL Handshake Protocol

SSL Record Protocol

- Lower layer protocol
- Operates just above TCP transport protocol
- Handles encapsulation of data communicated over TCP by the higher-level protocols
- Capability to encapsulate any data makes SSL a flexible, secure scheme that is application, service, and data type independent

SSL Handshake Protocol

- Higher-layer protocol
- Primarily used at beginning of communication between client and server to establish an encryption algorithm for ongoing secure communication

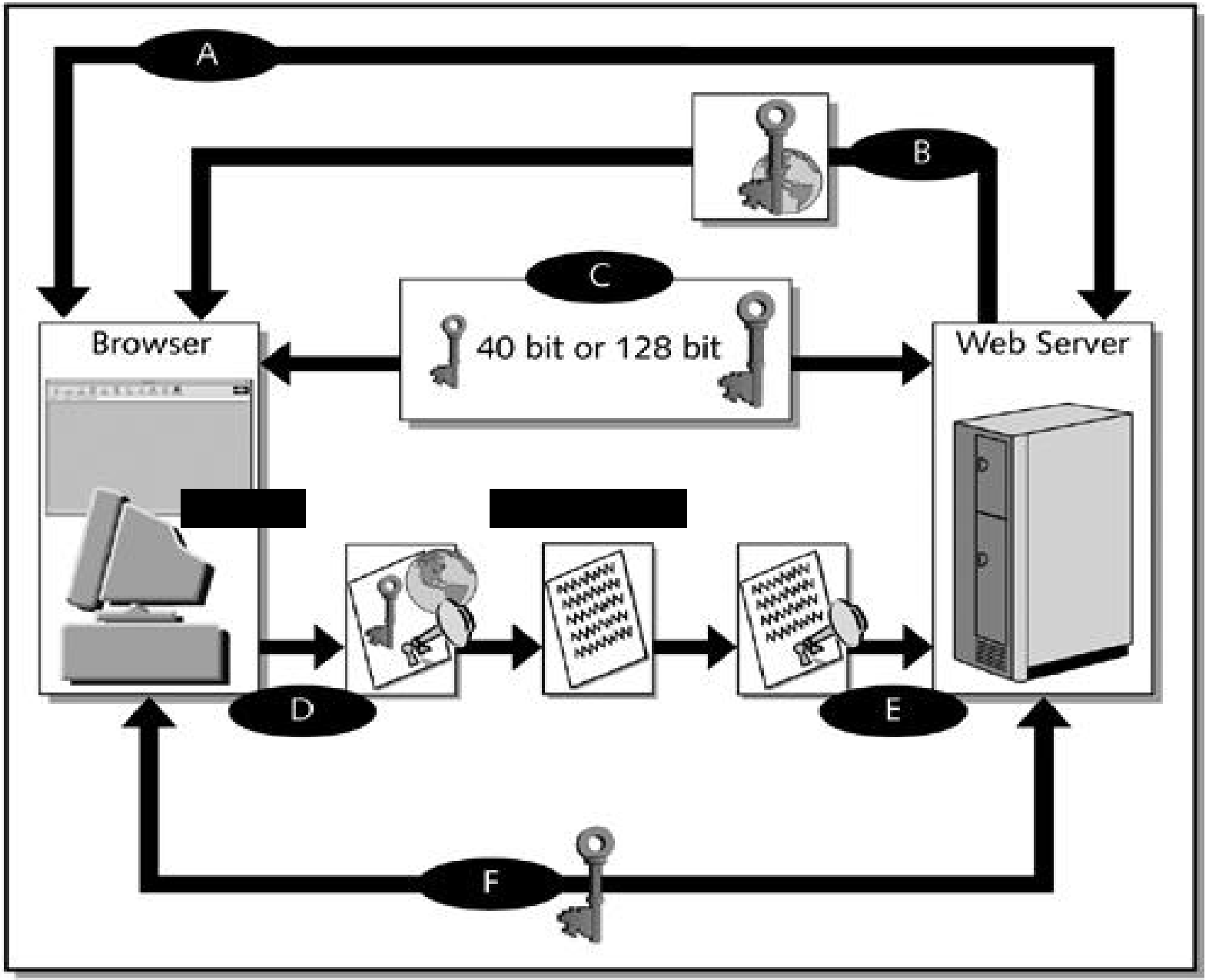

Figure 7.3 SSL in action.

Establishing SSL-secure Communications

- Multistep (A-E) process between client and server
- Provides strict framework within which to ensure security
- If either the client or the server fails to respond appropriately at each stage of the handshaking process, the SSL communication will fail

Establishing SSL-secured Communications

- Step A
  - Client initiates communication by requesting secured resource from a server “https:// …..”
- Step B
  - Server responds to indicate that it received the request for a secured resource
  - Server sends its certificate to client
  - Server requests client’s certificate (if required)
  - Server indicates that transmission is complete

continued

Establishing SSL-secured Communications

- Step C
  - Client sends its own certificate to server, if requested
  - Client attempts to verify server's certificate using the CA-distributed public key
  - Client sends encryption specification it needs to server (if certificate is verified)
  - Client indicates that its transmission is complete

continued

Establishing SSL-secured Communications

- Step D
  - Server verifies validity of client's certificate
  - Server receives session key, decrypts it using client's public key, and modifies server's encryption to match that requested by client
  - Server indicates end of normal transmissions
- Step E
  - Secure, encrypted communication begins between client and server

Session Key

- Determined once SSL identity verification is complete
- Defines the encryption strength for further communications
- Can be up to 128 bits if both server and client support the same encryption level
- 40-bit encryption is currently the highest level that can be used across U.S. borders

Encryption Levels

- Windows NT Server 4.0 supports only 40-bit encryption out of the box
- Higher level encryption requires a greater level of computing resources

Using SSL with Your Server

- Requires that a certificate be received from a CA
- If hosting internal private sites, you can be your own CA by using Certificate Server
- If hosting Internet-accessible sites, select a widely known and reputable CA such as VeriSign (www.verisign.com)