TITLE:

Practical Cryptography: Privacy for Business and E-commerce

INSTRUCTOR:

Frederick M. Avolio, independent security consultant

SUMMARY OF TOPICS:

Up Front—

- Defining Terms
- Basics of Cryptography—types and methods, Applications—
- Private Messaging (E-mail)
- Files and Directories
- Strong User Authentication
- Virtual Private Networks
- Web Sites
- Electronic Commerce
- Next Steps

Practical Cryptography: An Overview

Frederick M. Avolio

<fred@avolio.com>

Shameless (but brief) Marketing

Avolio Consulting, http://www.avolio.com/

- Network and computer security
  - Training
  - Policy and Procedure development
  - Product Review and Analysis
- Product Marketing, technical assistance
- E-mail system design, configuration, and training
- Writing: white papers, tutorials, product reviews

Syllabus

- Defining Terms
- Basics of Cryptography
- Private Messaging (E-mail)
- Files and Directories
- Strong User Authentication
- Virtual Private Networks
- Web Sites
- Electronic Commerce

Defining Terms

Concern

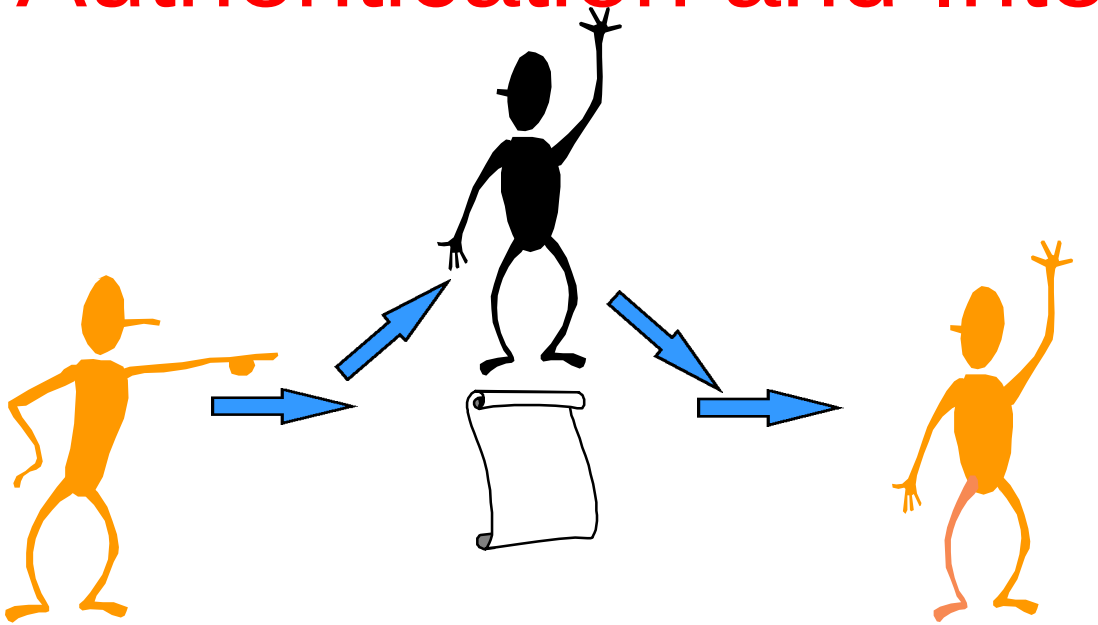
- Fraud
- Unauthorized access
- Snooping
- Message Alteration
- Disavowal

Requirement

- Authentication
- Authorization
- Privacy
- Data Integrity
- Non-Repudiation

From Understanding Digital Signatures by Gail Grant, McGraw-Hill, 1997

Authentication and Integrity

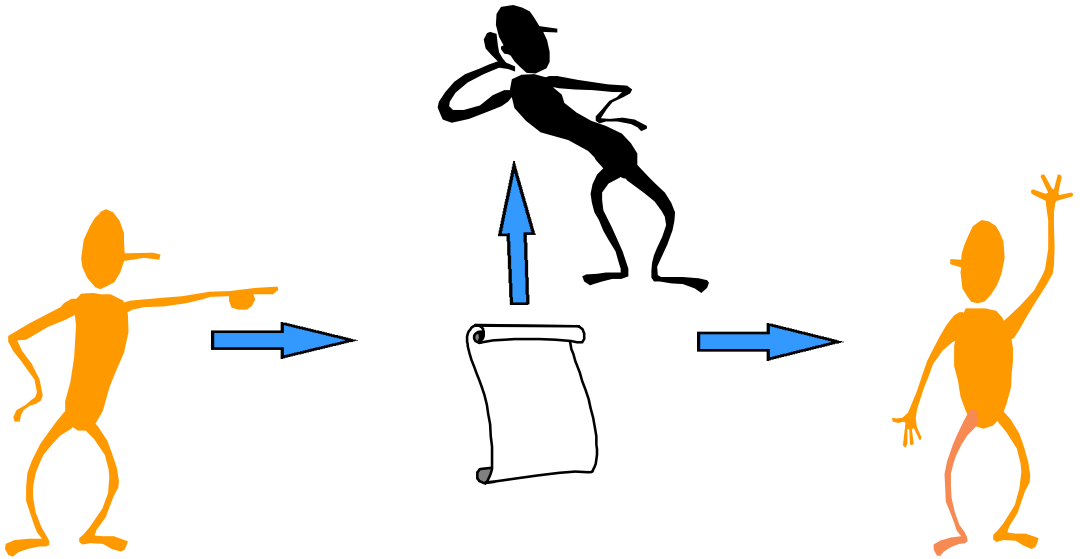


Guarantee to Receiver

- Knows identity of sender
- Message not altered
- Not unduly delayed

From *Internet Security* presentation at WICS by Whit Diffie

Privacy or Confidentiality



Guarantee to Sender

- Authorized receivers only

From *Internet Security* presentation at WICS by Whit Diffie

Business Needs for Crypto

Privacy

- Most businesses (and governments) don't need long-term security
- Mailing lists, business plans, negotiations, product R&D
- Commerce privacy needs are moderate
- Financial information might need to be secure for a decade
- Exceptions are embarrassments: personal, political, business

From *Internet Security* presentation at WICS by Bruce Schneier

Business Needs for Crypto

Authentication

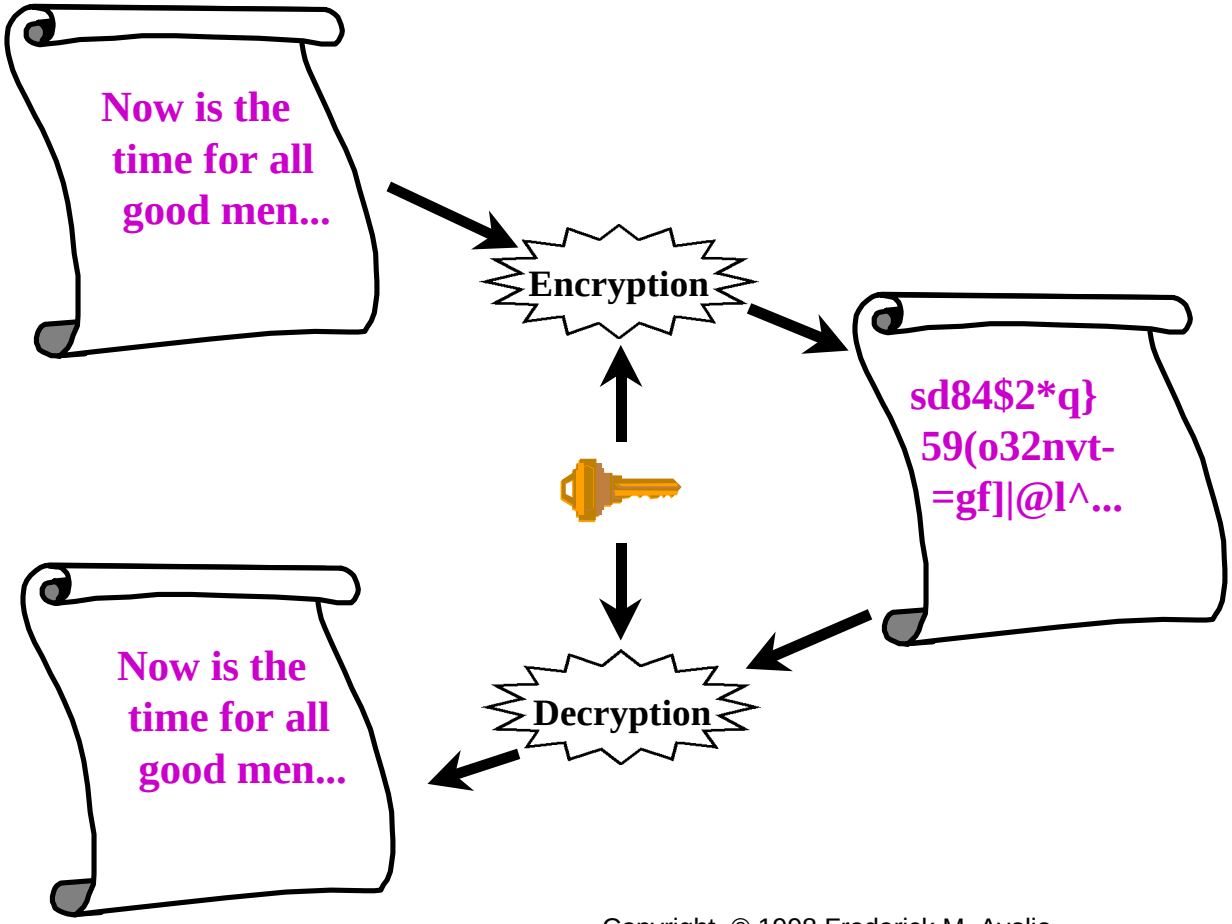
- Authenticating sessions versus transactions
- Need for audit trail depends on application
- Audit trail must be usable in court while not compromising the future security of the system

From *Internet Security* presentation at WICS by Bruce Schneier

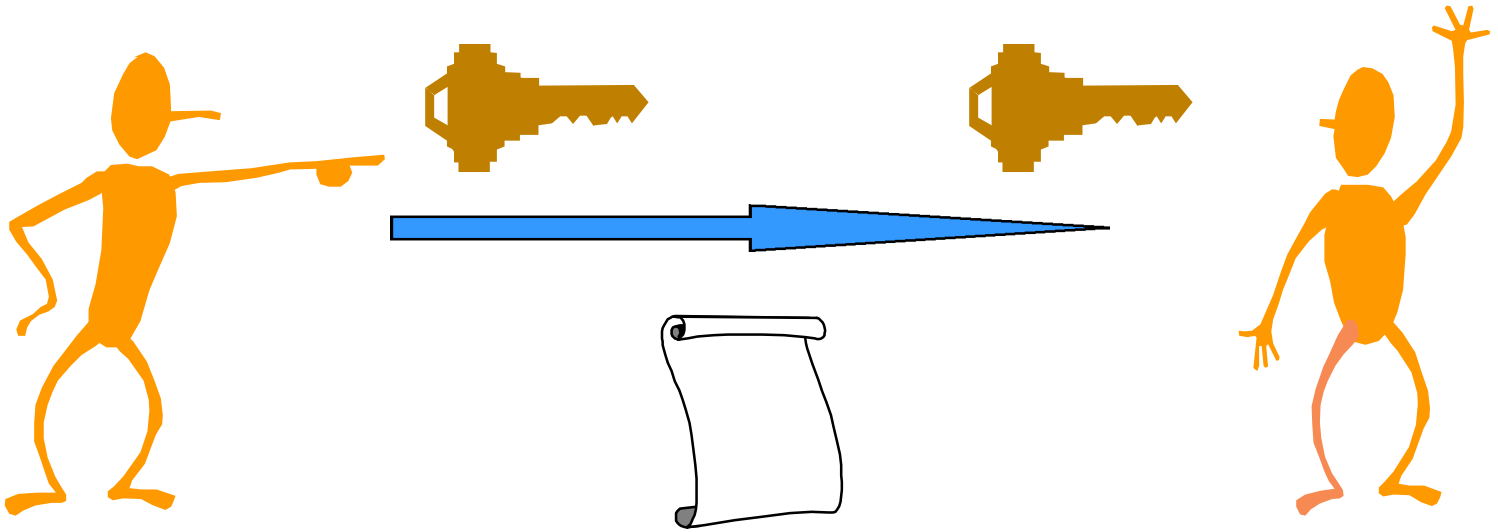
Basic Cryptography

- Secret key or symmetric encryption
- Public key or assymmetric encryption
- One-way hash functions

Encryption
Secret-Key (Symmetric)



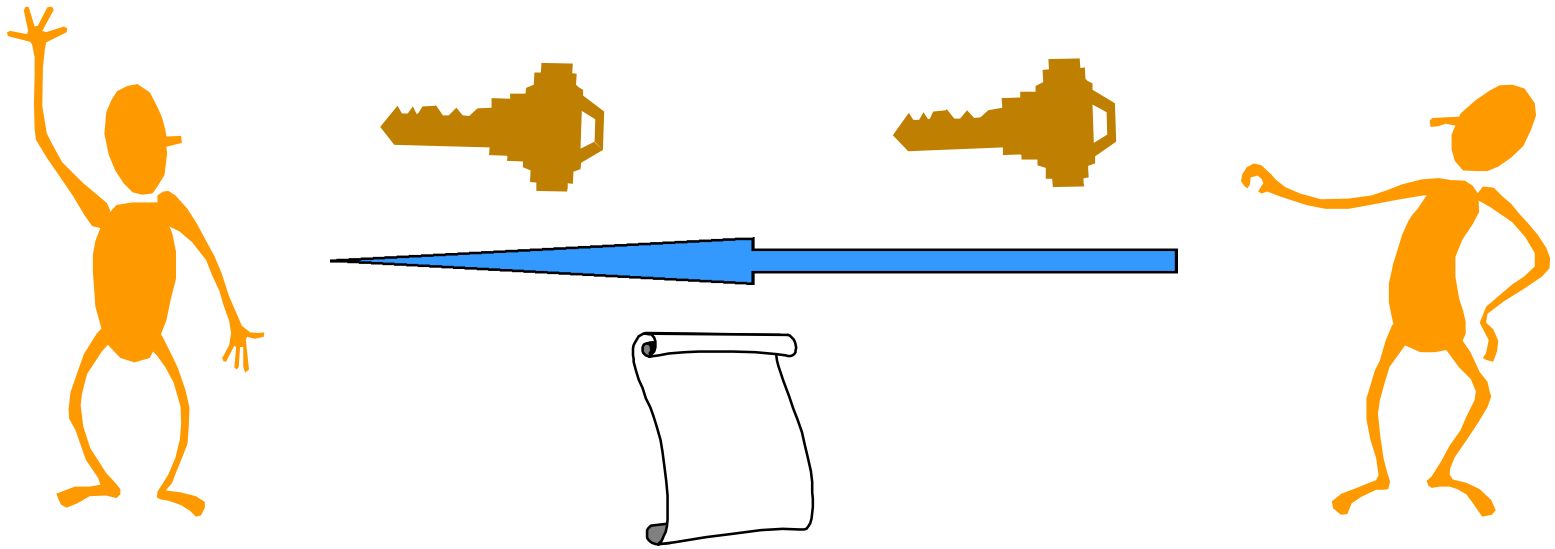
Encryption
Secret-Key (Symmetric)



Bob encrypts his messages to Ted with their shared secret key

Ted decrypts messages from Bob with the same secret key.

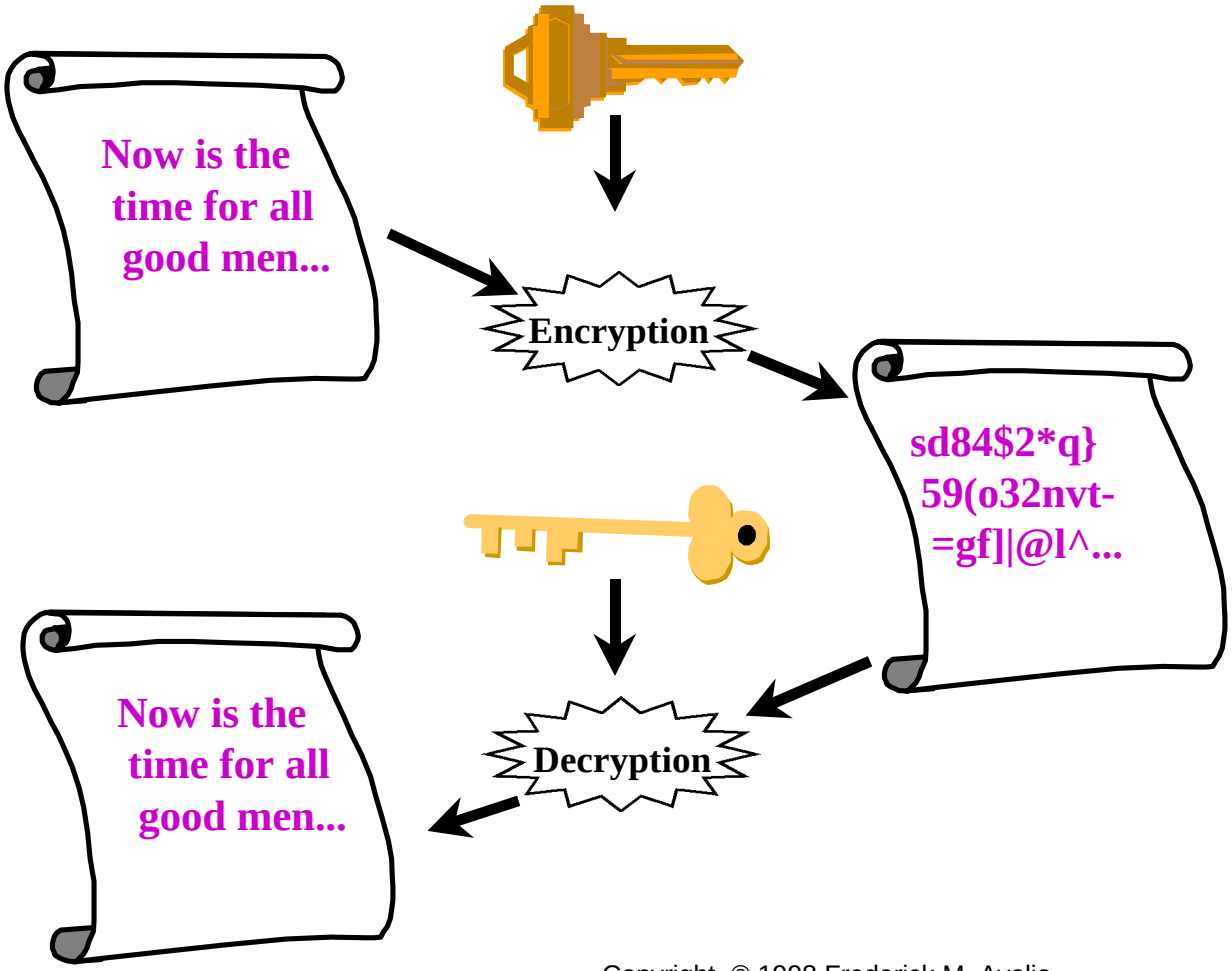
Encryption
Secret-Key (Symmetric)



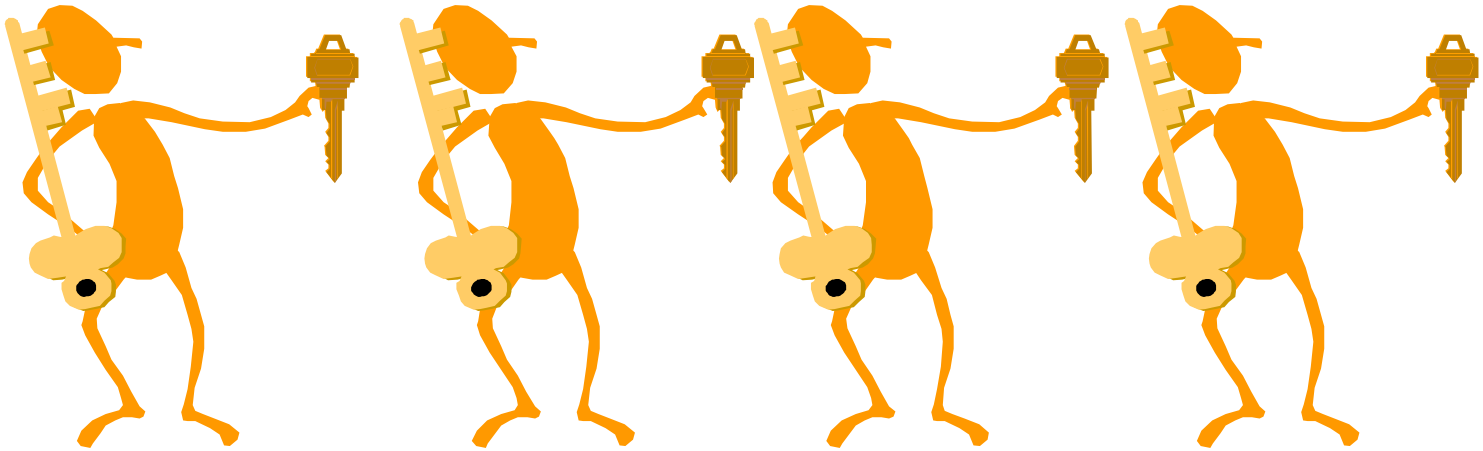
Bob decrypts Ted's messages using their secret key.

Ted sends messages back to Bob with the same secret key.

Encryption
Public-Key (Asymmetric)

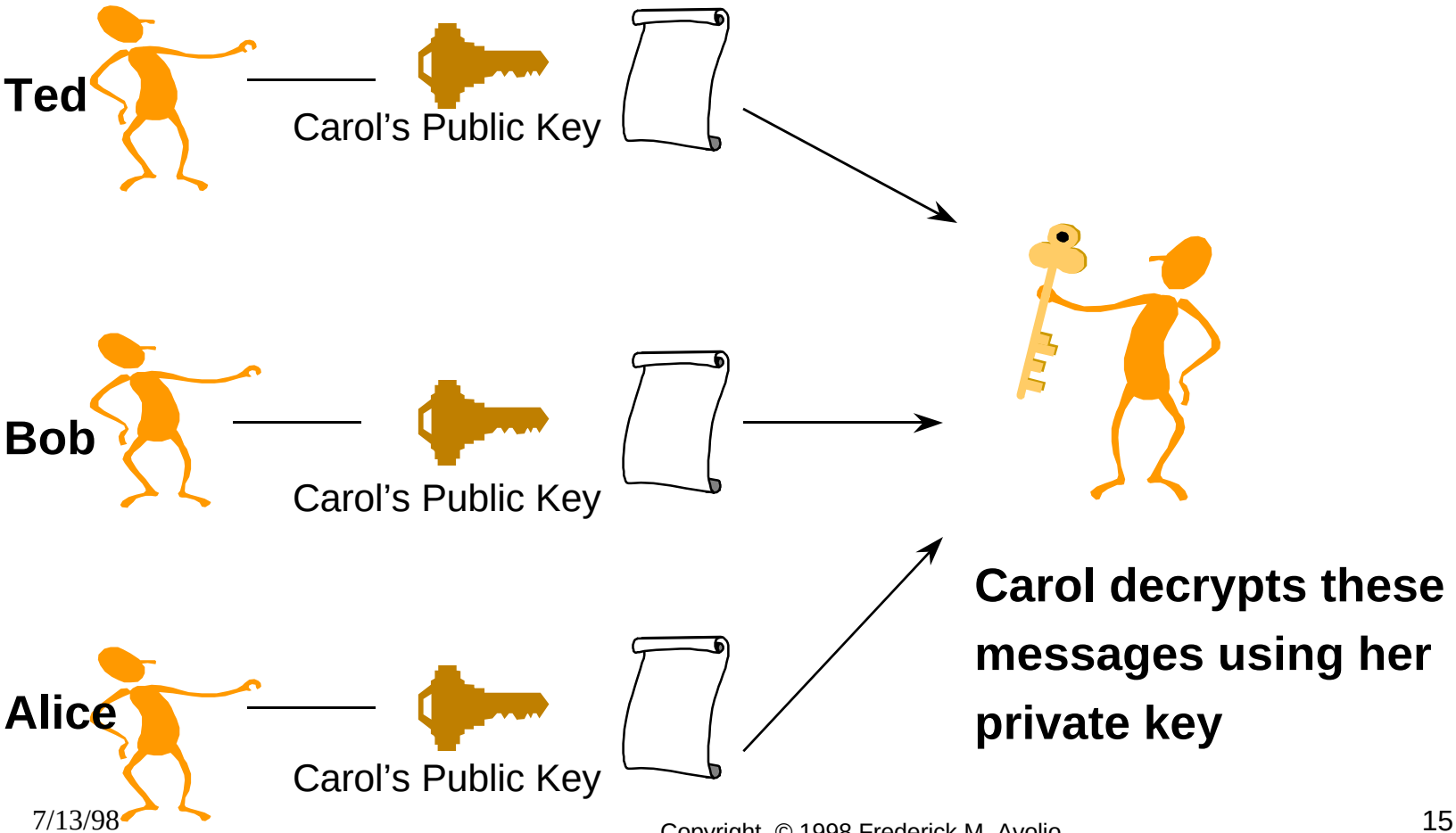


Encryption
Public-Key (Asymmetric)

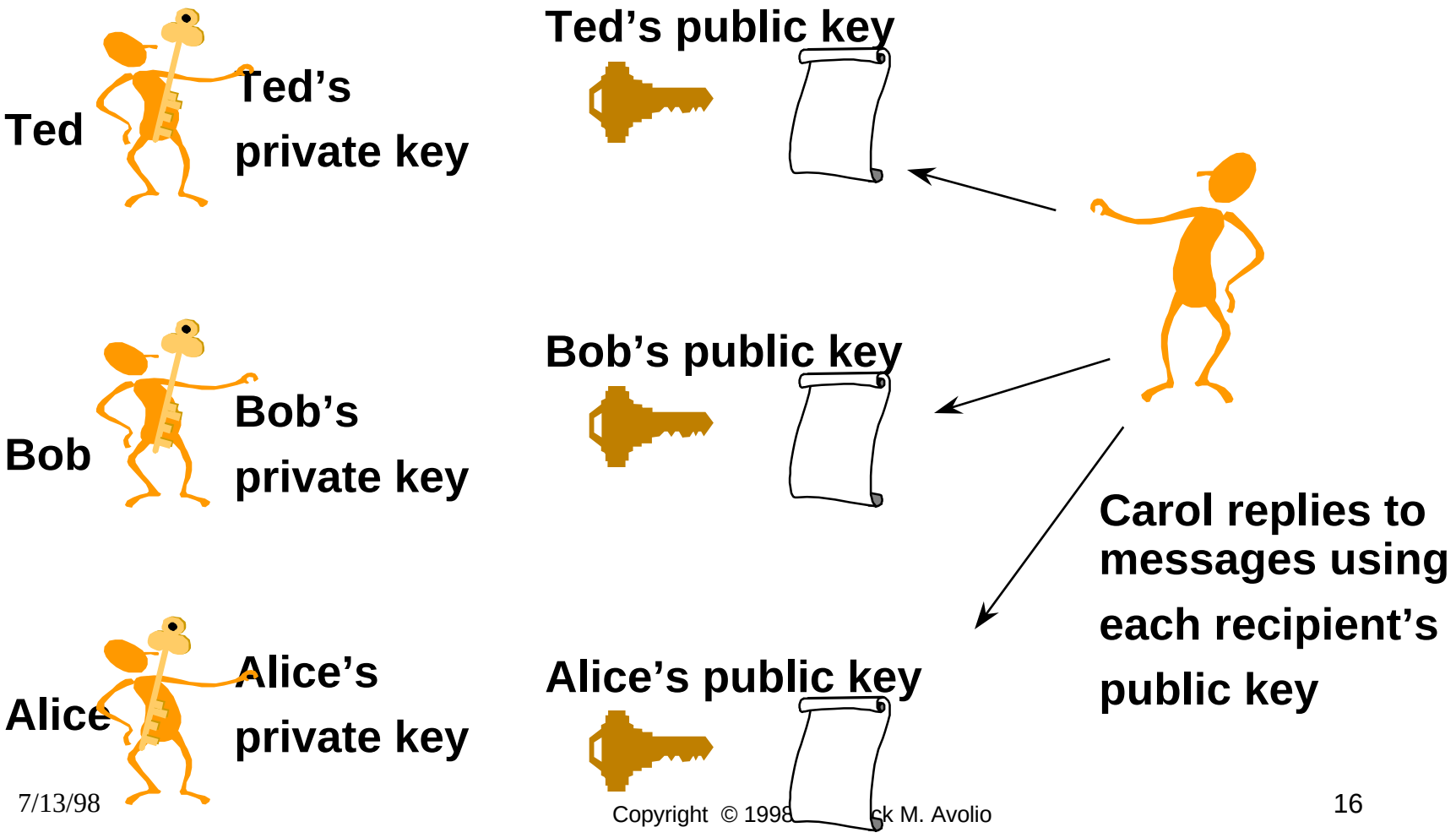


Carol, Ted, Bob, and Alice post their public keys and keep their private keys secret

Encryption
Public-Key (Asymmetric)



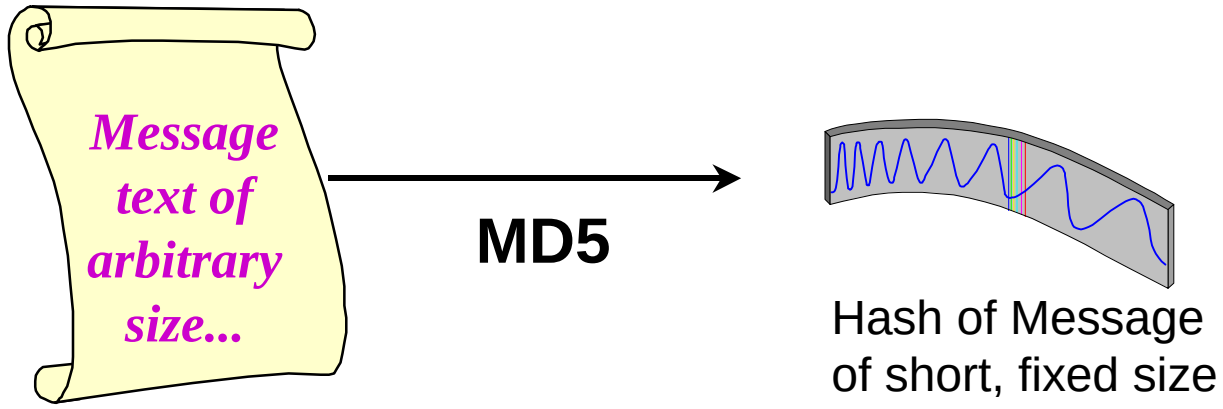
Encryption
Public-Key (Asymmetric)



Hash Functions

- Converts a string of data of any size into a fixed-length hash
- No way to go backwards
- E.g., a fingerprint
- Chances of any two strings of data hashing to the same value very, very small. This is very important!

Hash Functions



Security Problems Solved by Cryptography

- Privacy of stored data, messages, and conversations
- Secure electronic commerce
- Transaction non-repudiation
- User and data authentication
- E-mail security
- Multi-party control
- Secure audit logs

From *Internet Security* presentation at WICS by Bruce Schneier

Application Examples

- E-mail
- User Authentication
- Privacy for Files and Directories
- Virtual Private Networks
- Web Site Security

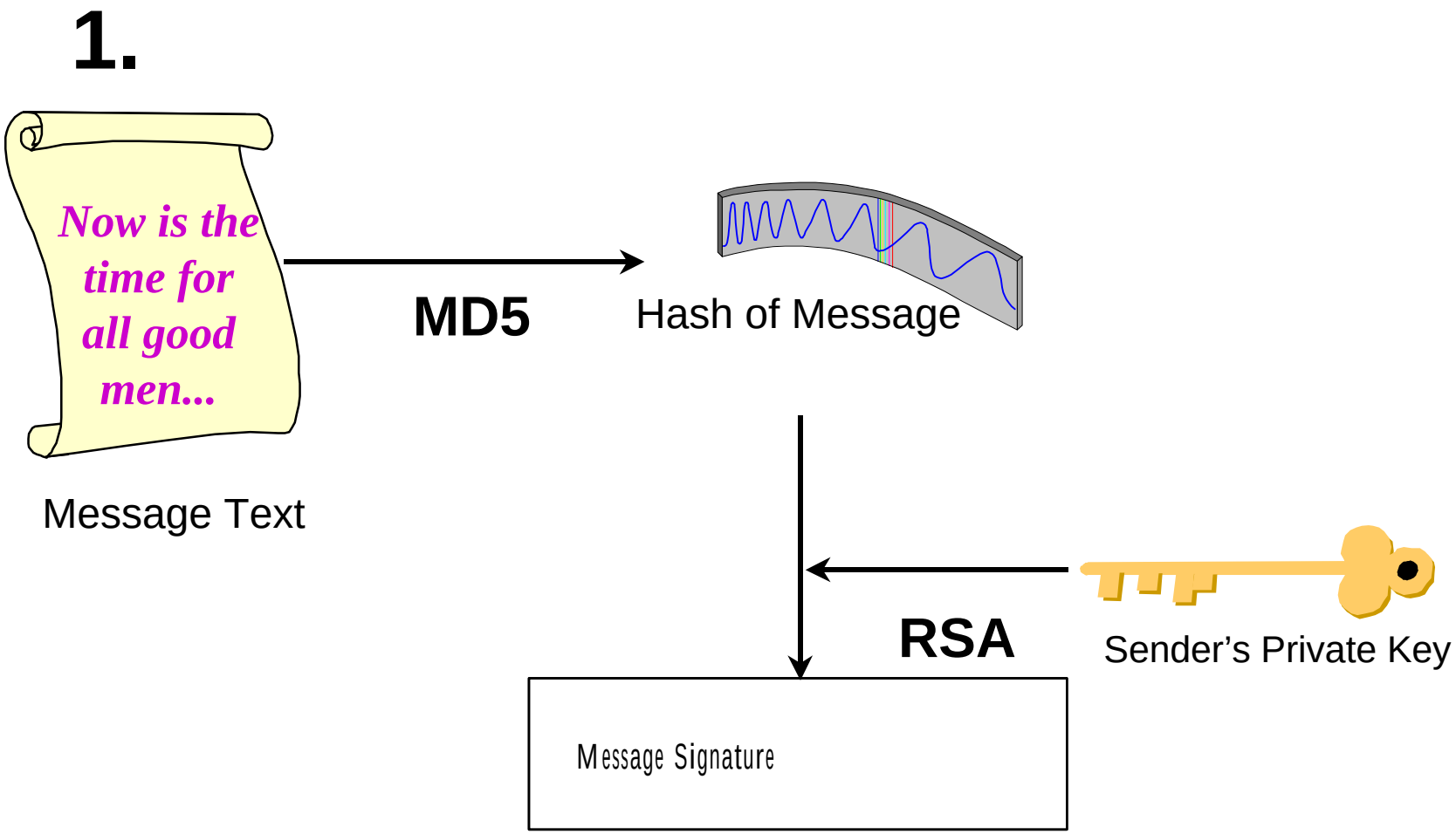
Private E-mail

The Goals

- Confidentiality
- Authentication
- Non-repudiation

Securing E-mail as well or better than postal mail!

Integrity and Authentication



Integrity and Authentication

2.

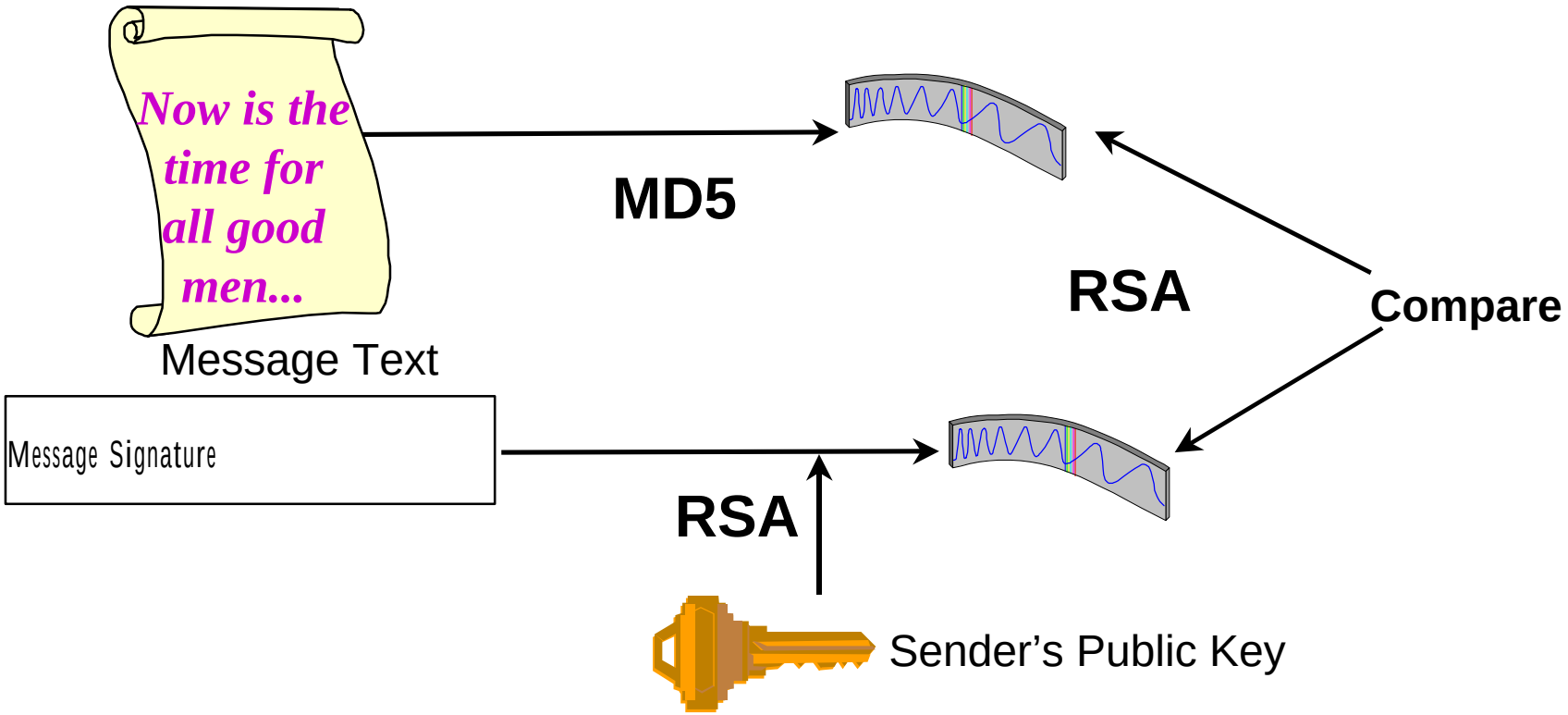
Data to Send

Digitally Signed Message

```
TO:     sysadmin
From:   avolio@tis.com

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

Please complete the deployment of the PGP software to all employees.

Fred,CSO

-----BEGIN PGP SIGNATURE-----
Version: 4.5

iQCVAgUBM+ZICTGr72+Les/dAQHmhwP/WorAeL6LzTJJre6lU77oPkNxYS+izmnM
1ozOHxVD6pDlEu7pgsju0g3yRO6tKxN4uJRW5ZeOUtVEgBw+dgFptuOSD9cmDAgS
w3SAEFwp9C6cPO0L9MMbc+eps3w8GKLlZkYRZPuANom0ggbmRpqDkjMIU25yEUr5
Vj/P54ZuaRY=
=zu3P
-----END PGP SIGNATURE--—
```

Integrity and Authentication

How can *anyone* validate integrity and authenticate sender?



Checking a Signed Message

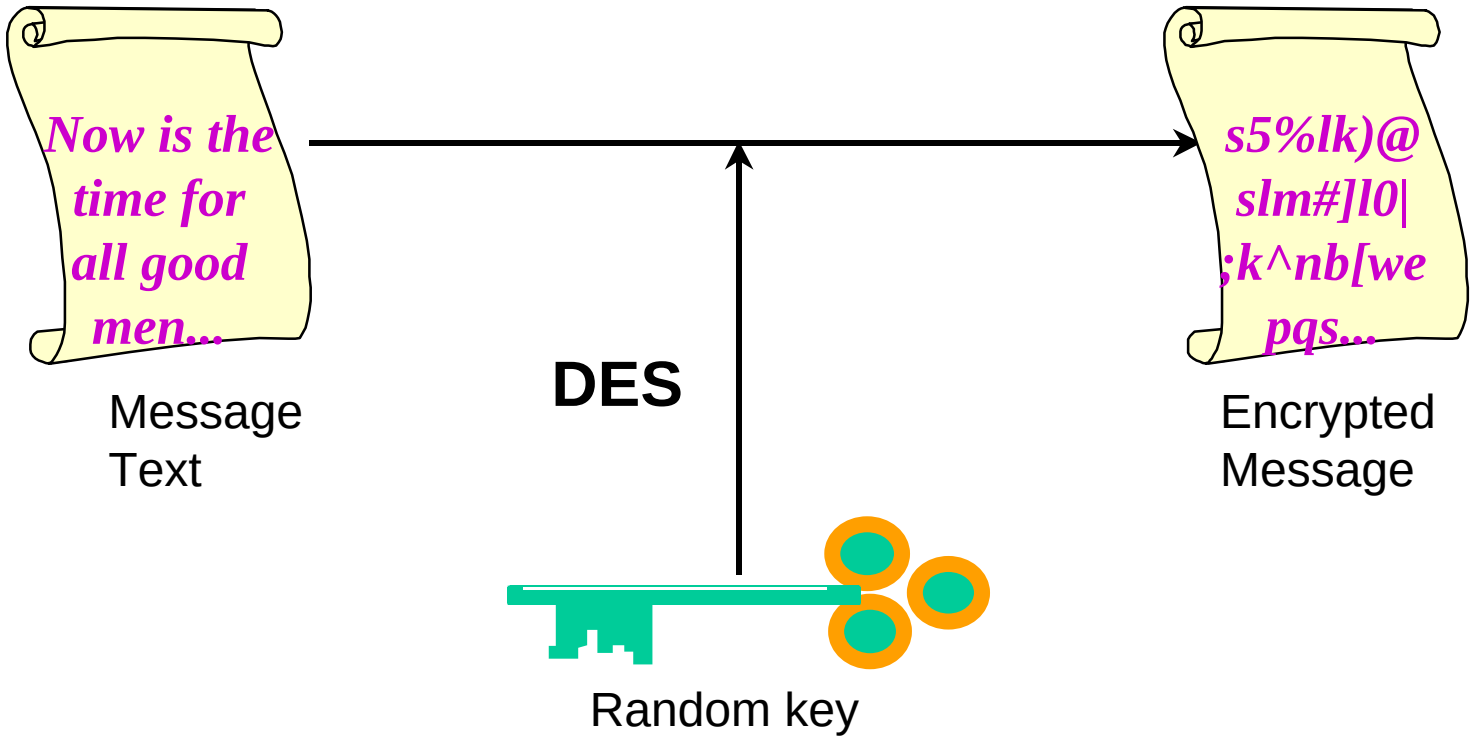
```
TO:     sysadmin
From:   avolio@tis.com

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

Plea

Frec

----
Vers

iQCVAgUBM+ZICTGr72+Les7dAQHmhwP7worAeL6LZTJJre6tU77oPkNXYS+IzmhM
1ozOHxVD6pDlEu7pgsju0g3yRO6tKxN4uJRW5ZeOUtVEgBw+dgFptuOSD9cmDAgS
w3SAEFwp9C6cPO0L9MMbc+eps3w8GKLlZkYRZPuANom0ggbmRpqDkjMIU25yEUr5
Vj/P54ZuaRY=
=zu3P
-----END PGP SIGNATURE--—
```

Encryption
Hybrid Systems

- Symmetric key is fast for encryption, but distributing keys is difficult
- Public key is good for key distribution, but slow at encryption
- Solution: use public key crypto as a secure means of distributing the keys for symmetric encryption

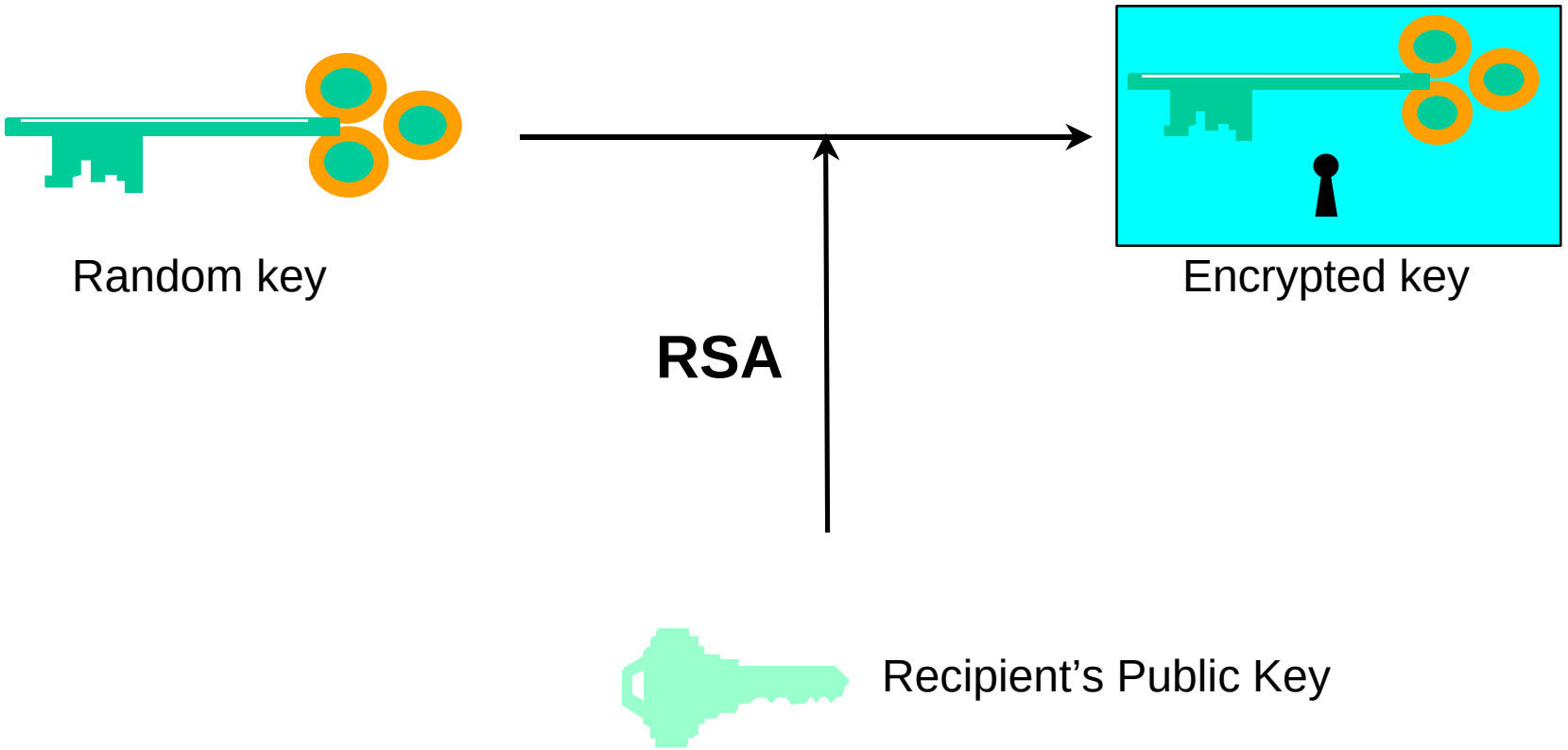
Adding Privacy

1.



Adding Privacy

2.

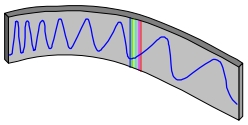


Adding Privacy

3.

Message Text

MD5



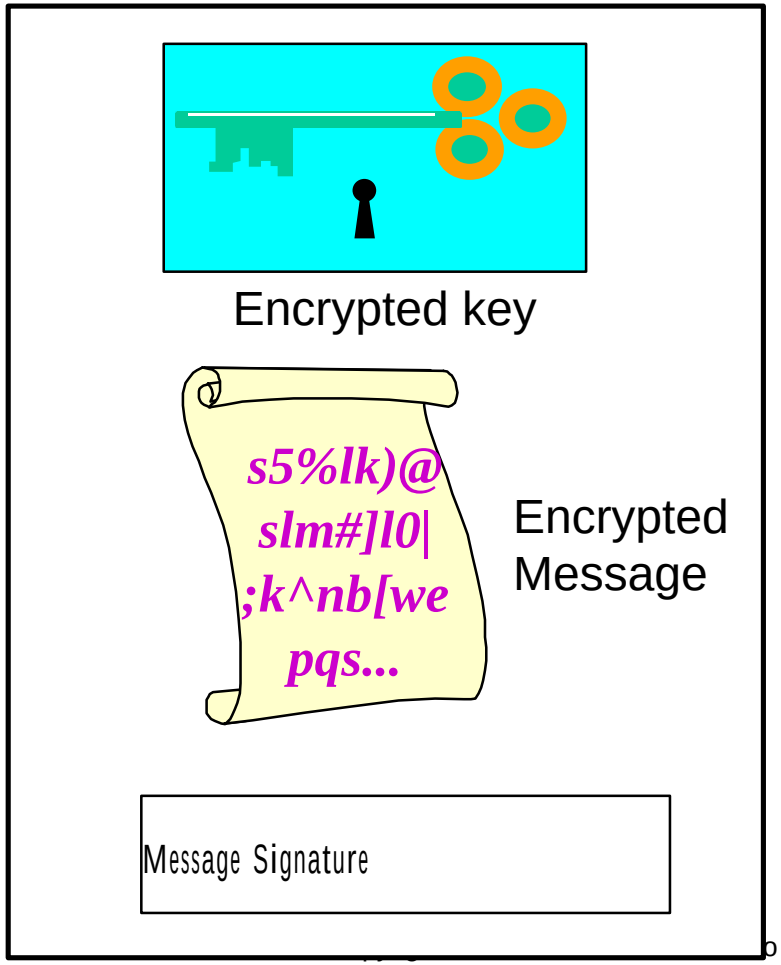
RSA

Sender's Private Key

Message Signature

Adding Privacy

4.



Data to Send

Adding Privacy

How can the recipient (and only the recipient) decrypt?

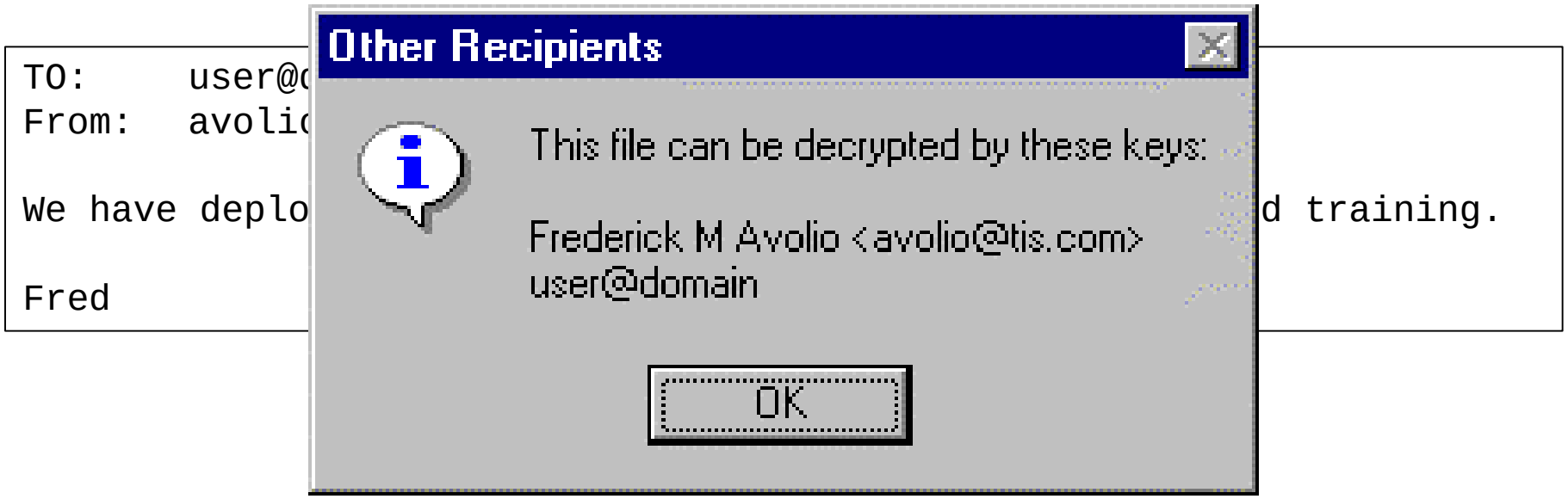
- DES key is encrypted with recipients public key
- Recipient decrypts with private key (only recipient has this)
- DES key is applied to encrypted message
- The result is the clear-text message

Sample Encrypted Message

```
Date: Tue, 08 Jul 1997 16:39:25 -0400
To: user@domain
From: Frederick M Avolio <avolio@tis.com>

-----BEGIN PGP MESSAGE-----
hIwCMavvb4t6z90BA/42UOAdWvnzfhRG2xXyYe203CISLsn2O39vM/y640hNbSl7
U29aNGZFfLMRGn7eLZG43SWwBz4cHjphG6iAzeLftRgHkLggxXA9VpGki5PyNID9
B0rk4TpRVE3qzgTbdio69aMlK6BdAQ4zWkyxSCi0oR3Vpnh+VVZyOVyaX8etlYRM
AvUTsuDYCkr1AQH+OlA4ntqhxoPP/SJpKm5ugMLYiiij8ak8V90a8IYMkYB0CzMr
liOJ6ZZxQm1x8orgjL/6Bm5EoSvN4eCCeA/xXKYAAAHXLhG47kVhJkjlPrI/U/sr
2aQEm6r+aU1s0ziU1LxF2c5DAW6cD5b4xH+EbvYrnQQJClNMh9y03SjviXvnqFDC
O4M70u3iLC50+em4PouqM1DZdoW8O5pb
=vhFx
-----END PGP MESSAGE-----
```

Sample Encrypted Message

Sample Encrypted Message



Sample Encrypted Message

```
TO:     user@domain
From:   avolio@tis.com

We have deployed the PGP mail software and have completed training.

Fred
```

Files and Directories

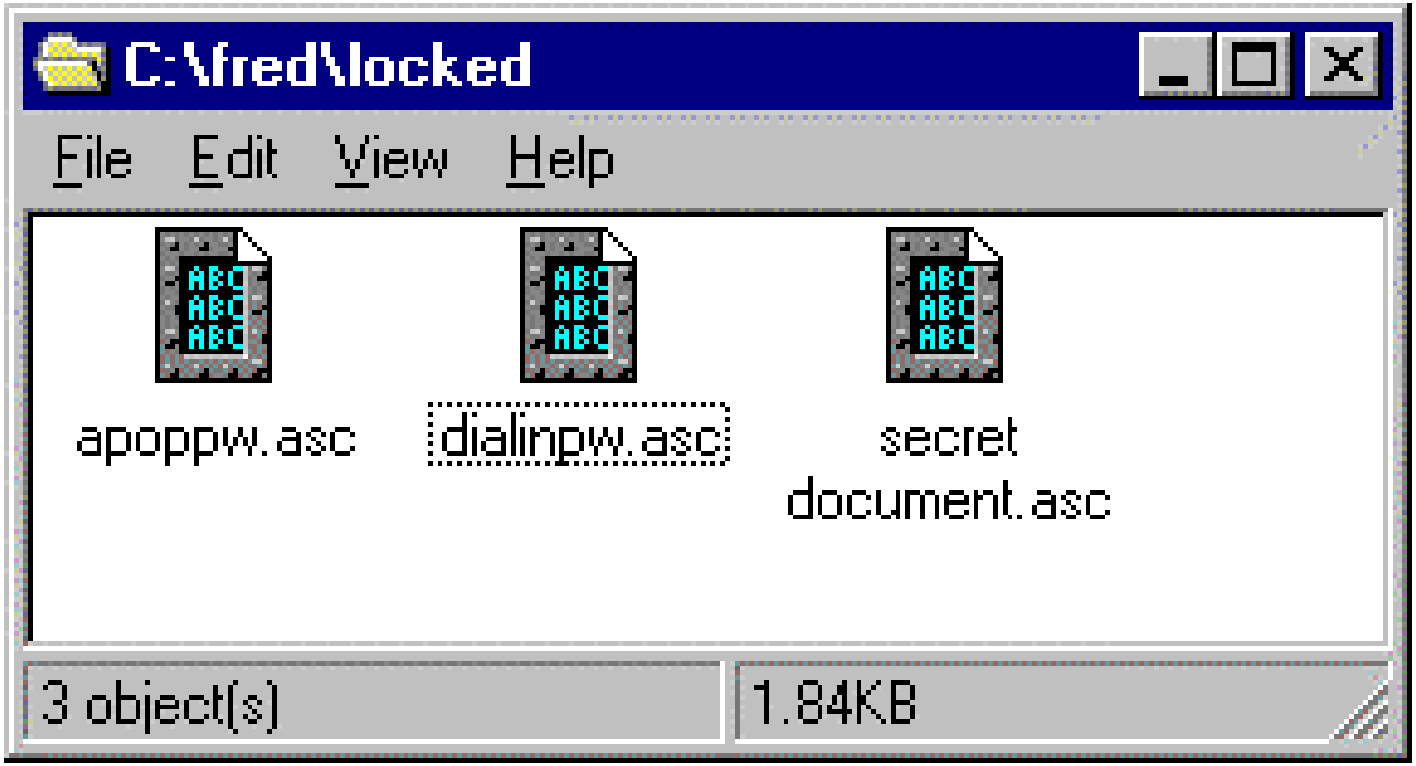
The Goals

- Seal data files from unauthorized access or alteration (reading, writing, etc.)

Files and Directories

- Similar to E-mail concerns and solutions
- Encrypt a file with a symmetric key
- Encrypt a file with YOUR public key
- Like locking drawers in a desk of file cabinet
- Desert Storm …

Files and Directories



Files and Directories

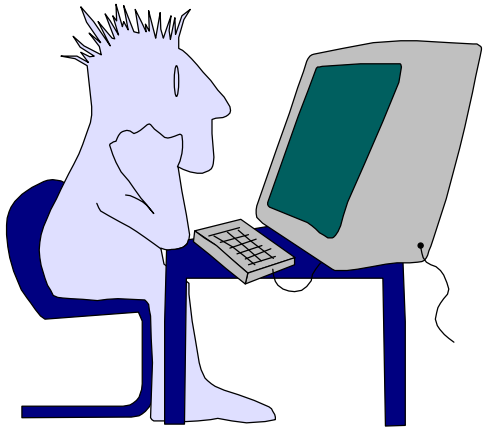
- Need to be built into file system
- Need to be built into applications
- Open — automatically decrypt if encrypted
- Close — automatically encrypt if was encrypted (and delete cleartext)
- Close with encrypt

Strong User Authentication

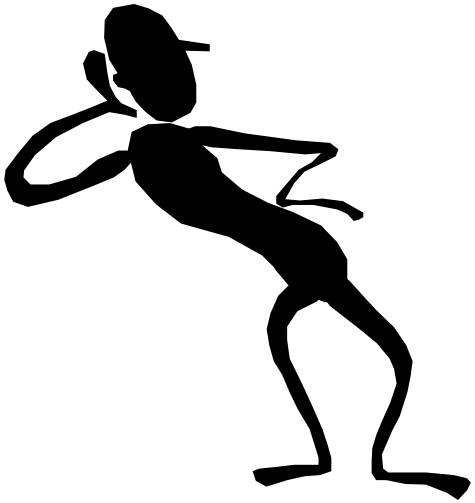
The goals

- “To establish the validity of a claimed identity or to provide protection against fraudulent transactions by establishing the validity of ... [the] individual ...” — NCSC “Red Book”
- To identify in a way that is not vulnerable to a replay attack

Replay Attack



```
Username: fred
Password: lisa
%
```



Authentication Techniques

- Strong user authentication
  - Smart cards or tokens
    - Software (server) and smartcard based
    - PIN-protected smartcard private key
    - System issues challenge based on user
    - User uses password to unlock smartcard, which reads challenge, calculates cryptographic response
    - Response is used as response to challenge

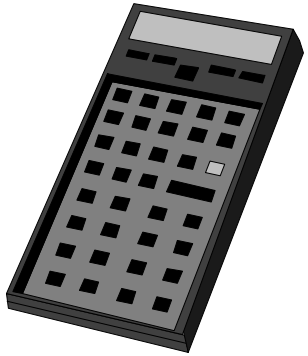
Authentication Techniques

Server sends Challenge: "876261"

User "unlocks" authentication token by keying in Personal Identification Number

(Server and token share a secret encryption key that user never has access to)

"1105"



User enters challenge into authentication token

"876261"

(Secret key: "0x8A5F42")

Token returns an encrypted response to the challenge

"722512"

Server compares response

User responds to server with unique response

"722512"

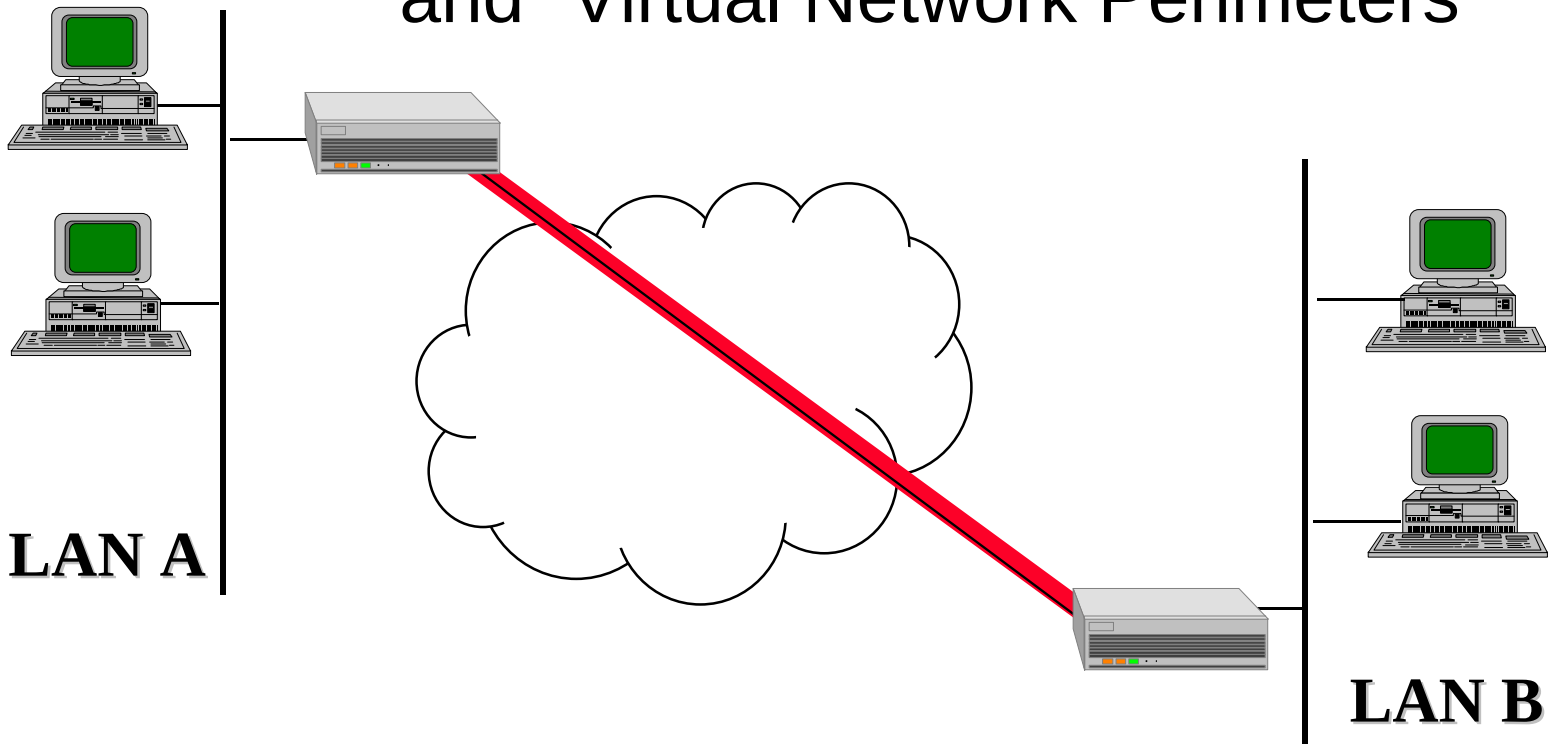
Virtual Private Networks

The goals

- Privacy of communication between secure enclaves over an untrusted network
- Privacy and access for remote employees
- Privacy and controlled access for remote clients

Privacy

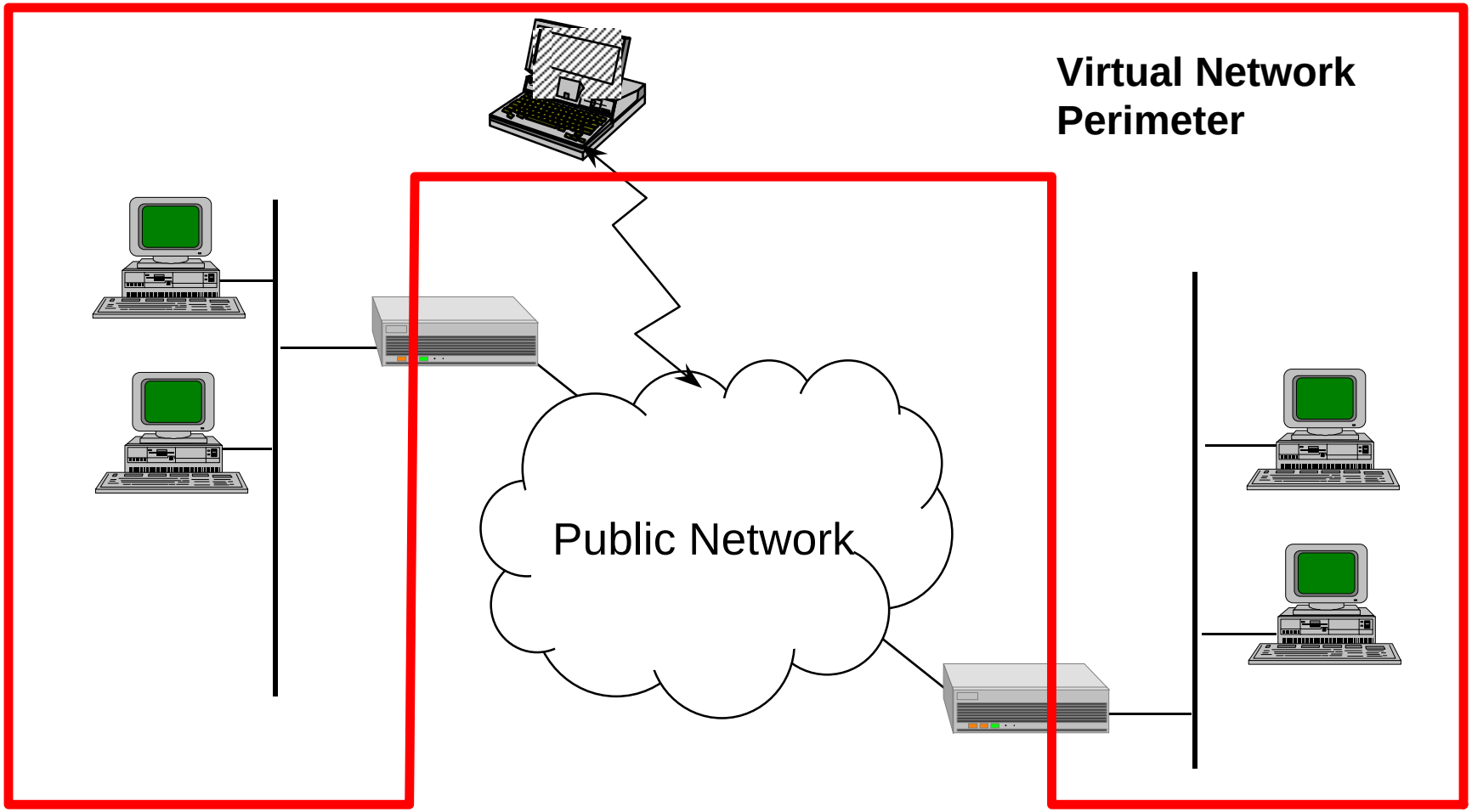
Encryption — “Virtual Private Networks”
and “Virtual Network Perimeters”



Virtual Private Networks

- Firewall-to-firewall connections over the Internet.
- Using encrypted “tunnels” over the Internet to connect LANs and WANs can reduce costs 23-50% (US Computer March 1996).
- Secure Wide Area Networking (S/WAN).
- IPv6, end-to-end encryption, IPSEC

Extending the Perimeter



Global VPNs

- Key Issues
  - The Internet is a worldwide network
  - Companies cross international boundries
  - Partnerships cross international boundries
  - Privacy in business transactions is critical to success
  - Network communications privacy means employing encryption

Global VPNs

Encryption Requirements

- Strong (56 bit or better key length)
- Exportable
- Platform independent

Web Site Security

The goals

- Deployment of web sites for internal and external use
- Protection from modification
- Assurance data has not been modified
- Control of access

Web Site Security

Web site attacks

- CIA
- DOJ
- NASA
- USAF
- Singapore Government
- Nation of Islam
- MGM Studios

Web Site Security

- Message hash of all files on web site kept
  - Periodic checking of stored hash against hash of pages — integrity checking
- Digitally sign pages, documents, software
  - Assurance for users that data has not been modified

Web Site Security

- Controlled access
  - Strong user authentication
  - User name and password over protected channel

Web Site Security

ftp://info.cert.org/pub/cert_advisories/CA-97.20.javascript:

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

===========================================================================
CERT* Advisory CA-97.20
Original issue date: July 8, 1997

Last revised: July 28, 1997, Appendix A - added information for
                        Hewlett-Packard and IBM.
                        Section III.A - slight wording change.

                A complete revision history is at the end of this file.

Topic: JavaScript Vulnerability
          …
-----BEGIN PGP SIGNATURE-----
Version: 2.6.2

iQCVAwUBM9yyN3VP+x0t4w7BAQFLAgP/Z1moGK6SI2Q3OBbV/fpCOcW2J9TdXE3/
UHuZ7vHCjKDWxelHr5551JQ9i19s6sVBNDOX1W031IrlS36nIblp3vX4rVuAaufw
VOxqxYg44i3gxsC8NgC/HW5j7KHsOiGzoRmU5a+vWyLmmged+Y2wBDrxGeqbHacE
4S6FPph4/w8=
=5MP2
-----END PGP SIGNATURE-----
```

E-Commerce

- Transaction security
  - Privacy of a sale
  - Integrity of a sale
- Electronic payment
  - Privacy
  - Integrity
  - Provenance of an agreement to transfer funds

From Web Security Sourcebook by Rubin, at al, John Wiley & Sons, 1997

Transaction Security

- Virtual Private Network approach
  - Encryption and authentication done as part of the network communication
  - Network software must be modified
  - Users need not modify behavior or application software

From Web Security Sourcebook by Rubin, at al, John Wiley & Sons, 1997

Transaction Security

- Application-level encryption
  - OS and platform independent
  - No data is exposed between client and server software
  - Most web browsers are using this type of security
    - SSL, SHTTP

From Web Security Sourcebook by Rubin, at al, John Wiley & Sons, 1997

Transaction Security

- Application-level encryption
  - Browser and server shake hands and decide on encryption scheme and key
  - Data is transmitted encrypted with the key
  - They shake hands at the end.

This is the meaning of the filled in key on the Netscape browsers.

From Web Security Sourcebook by Rubin, at al, John Wiley & Sons, 1997

Transaction Security

- Most e-commerce today uses application-level transaction security
- Most transaction security today protects privacy of the data sent from the client
  - Order blanks or questionnaires
  - Credit Card numbers
- Most e-commerce on the Internet today is like telephone catalog ordering without the catalog or telephone

Netscape - [Online Catalog]

File Edit View Go Bookmarks Options Directory Window Help

Back Forward Home Reload Images Open Print Find Stop

Netsite: http://www.godiva.com/godiva-scripts/catalog/catalog-cpage?id=84

What's New? What's Cool? Destinations Net Search People Software

NOTE: Some items may be temporarily out of stock. Use the "Shop Search" to display only available items.

Summer Collection

5-Piece Summer Truffle Box

Almond Croquant Bar

Cigar Box

Summer Ballotins

1/4 lb. Summer Box

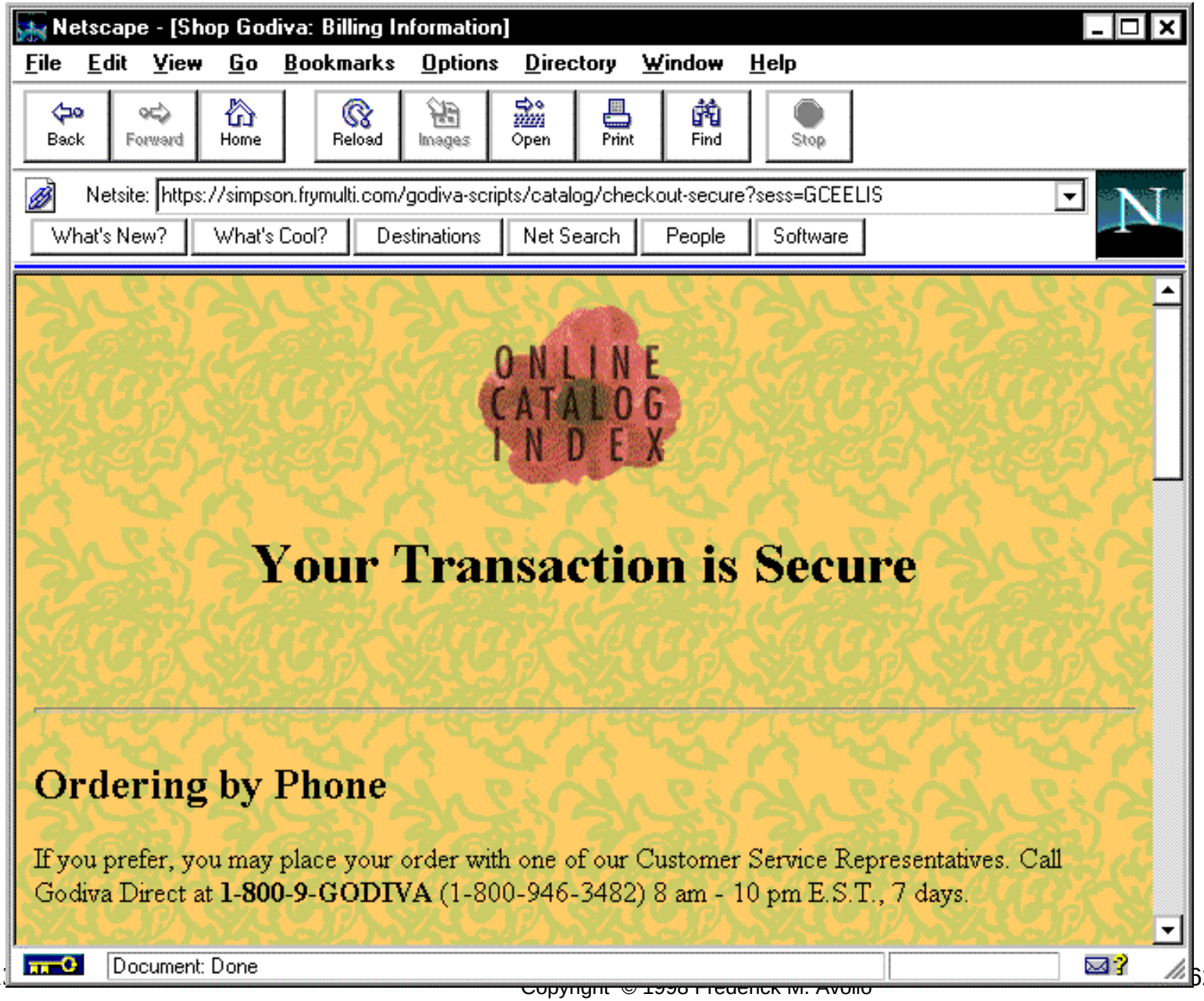
Almond Croquant Bar

Our super-sized 3 oz. bar is made of dark chocolate, croquant and loads of crunchy, decadent almonds. The combination...extraordinary! set of 2, 6 oz.

(752542) Almond Croquant Bar 6 oz. (set of 2) **$ 10.00**

Quantity: 3

Document: Done



Electronic Payment

- Secure payment protocols exist
- Most involve a trusted third entity acting as a gateway to financial networks or directly to a bank

Where do we go from here?

Or, what more is needed?

Infrastructure Needed

Public Key Infrastructure

- Key creation
- Key distribution
- Key certification
- Key lookup
- Key revocation
- Locally and Globally

Certificates

- A message
- Name, e-mail, public key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 4.5

mQCNAjPmUEIAAAEEAMj14c0xswae9XfbMVQeDFq8OVf29+N1745Hey5vkYw7UZUn
7K1ehDYK44W+f1Y/Ns4g3lFJNxuFRbPZXUPAc8dlPiBR1xq+wqcoOIm+gpQEd5Dl
1EgsUyE+3Si0WQ6zELRvKCWKww6/8egKDaMqQTgMqZFQEqjRFEvspjTJR9s3AAUR
tAt1c2VyQGRvbWFpbg==
=Cexv
-----END PGP PUBLIC KEY BLOCK-----
```

Certificate

- Signed by someone trustworthy

Summary and Review

Encryption
Uses

- Encryption is the encoding of information and can be used at many different points:
  - File encryption for storage (e.g.., for laptops)
  - Private E-mail
  - Digital signatures for Doctor Orders
  - Integrity checking for changes to patient records
  - Encrypted data in transit
    - Router to router encryption
    - Firewall to firewall encryption at the IP level

Encryption
Applications

- Access Control
  - Use cryptographic functions to distribute access control lists and privileges
- Authentication
  - Digital Signatures provide positive proof of identity
  - Digital certificates used to bind public key to physical identity

Encryption
Applications

- Non-repudiation
  - Cryptographic functions use to provide unforgeable proof of receipt or authorship
- Availability
  - Combination of applications used to reduce the chances of denial of service or malicious system outages

Basic Tools of Cryptography

- Symmetric encryption
  - Provides secrecy among parties who share a common key
- Message authentication codes
  - Provides integrity checking and authentication
- Public-key encryption
  - Allows someone to receive secret message from people he's never met
  - Allows method of exchanging secret keys
- Digital signature schemes
  - Establishes integrity, authenticity, and non-repudiation
- Secure hash functions
  - Used to reduce a message to a fixed size for signature

From *Internet Security* presentation at WICS by Bruce Schneier

Practical Cryptography: An Overview

Frederick M. Avolio

<fred@avolio.com>