

---

# Enterprise Encryption

---

Bayly Eley

---

# C I A

- Confidentiality
  - Integrity
  - Availability
-

---

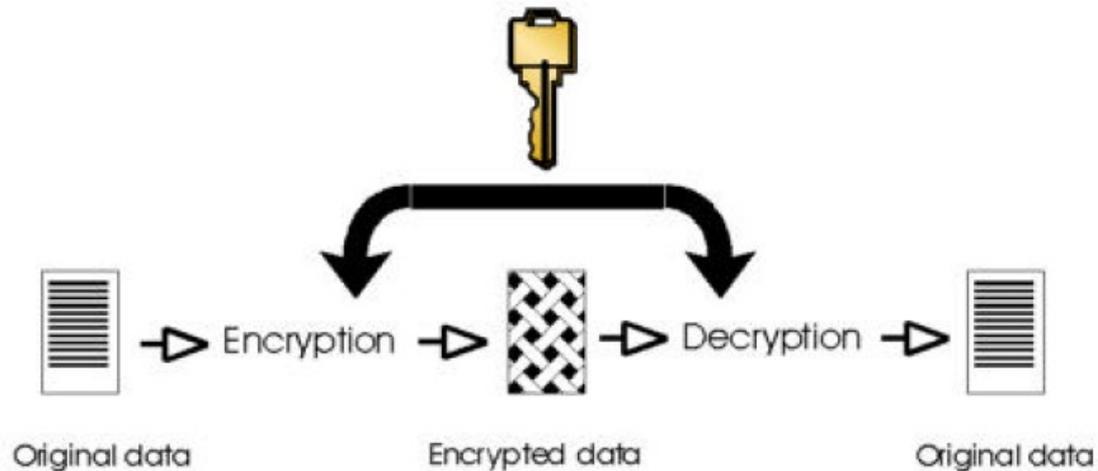
# Encryption 101

- Symmetric (Private Key) Encryption
  - Asymmetric (Public Key) Encryption
  - Hash
-

# Symmetric Encryption

## Symmetric key algorithms

*Symmetric-key* encryption is an encryption method that uses the **same** key for encryption and decryption, as shown below. This type of encryption is **quick** and well suited when the data does not need to be shared (hard disk encryption, or file encryption of sensitive data on a PC).



---

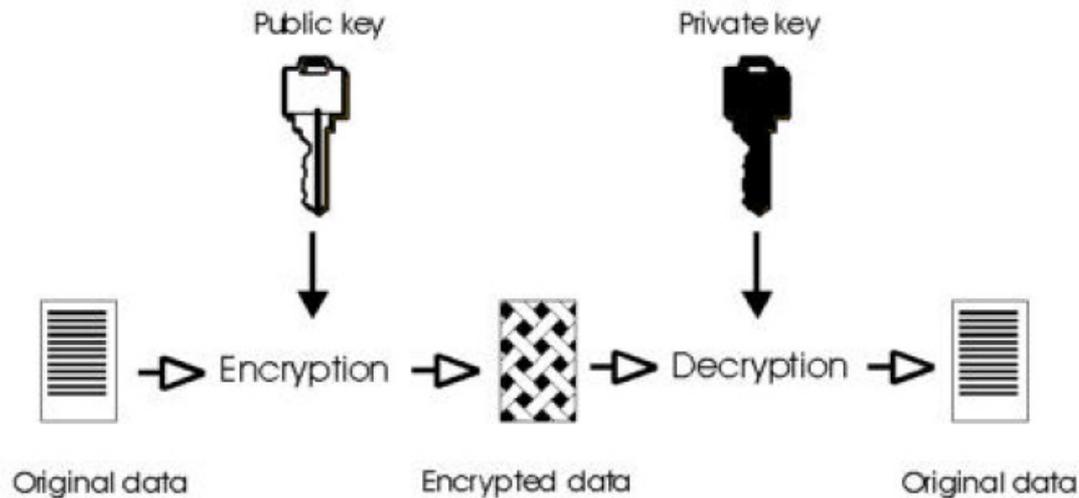
# Symmetric Encryption Examples

- ❑ DES
    - Not secure
    - 56-bit key
  - ❑ Triple-DES
    - Has not been cracked yet
    - Do DES 3 times...
  - ❑ AES
    - Replaces Triple-DES
    - Very secure
-

# Asymmetric Encryption

## Public key algorithms

A *public-key* algorithm (also called an *asymmetric* algorithm) uses a key pair. As shown below, the key used for decryption is **different** from the key used for encryption.



---

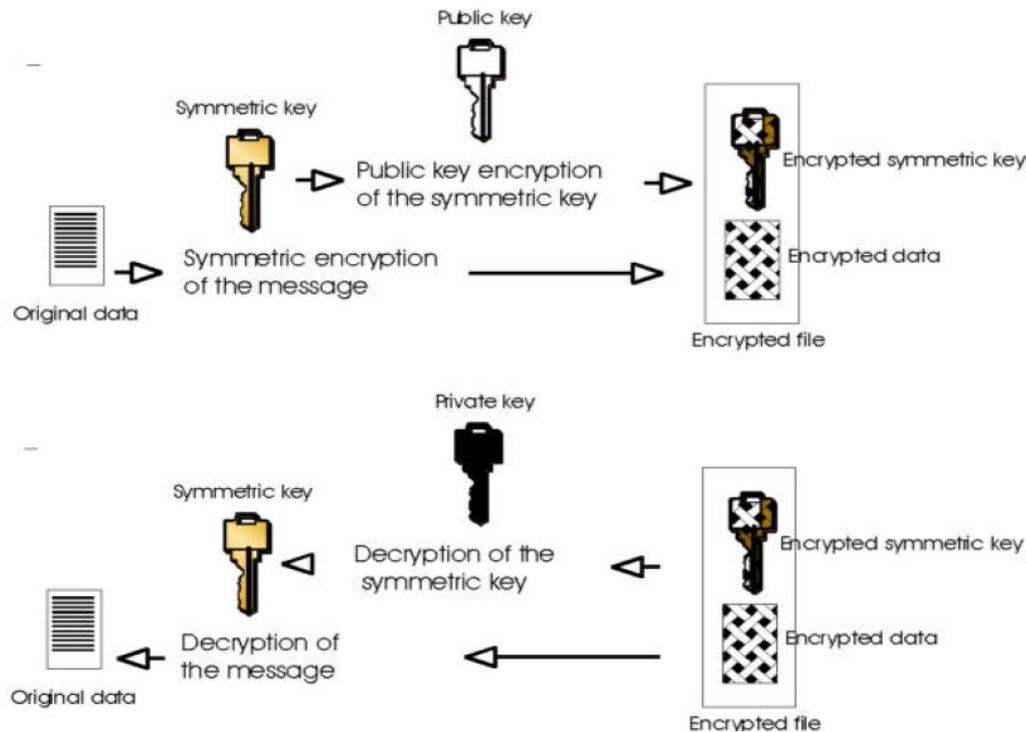
# Symmetric Encryption Examples

- Diffie-Helman
    - Mechanism to share a private key over a public connection
  - DSS (Digital Signature Standard)
    - Used in DSA – US Gov
    - Developed by NIST in 1991
  - RSA (PKCS)
    - First algorithm used for symmetric encryption
    - Widely-used, but limited lifetime
-

# Using Asymmetric & Symmetric Together

## A mixture of both

The drawback of the public key system is the slowness of the encryption/decryption process. It makes it almost useless when processing big files. (In software, DES is about 100 times faster than RSA; in hardware 1000 times faster). To avoid this, a combination of public and symmetric keys can be used, as shown below:



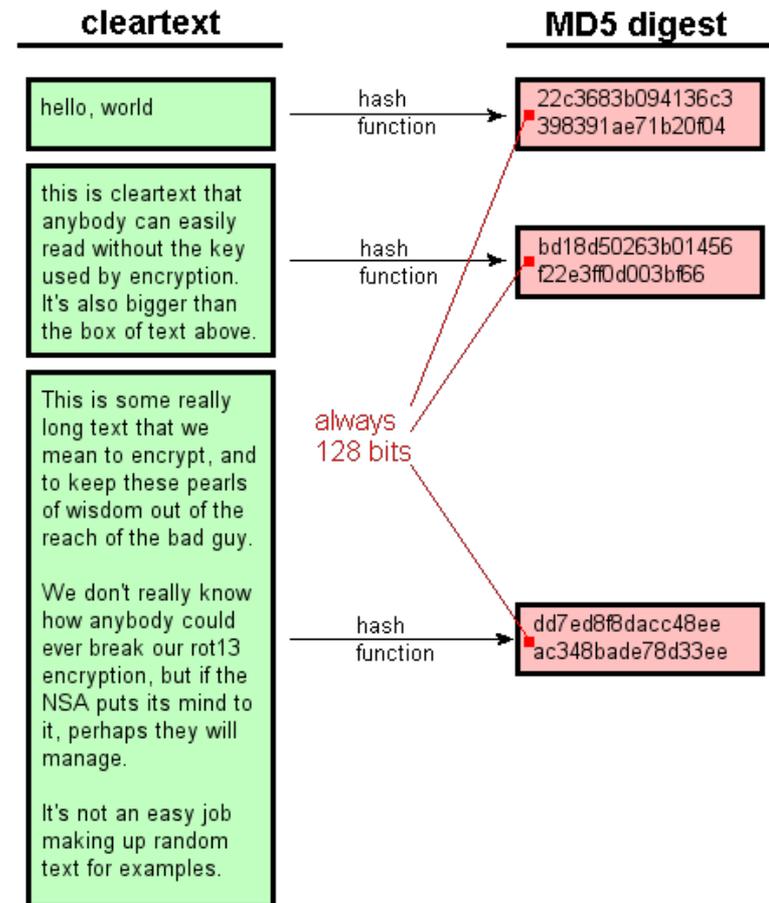
---

# Mixture Examples

- PGP / GPG
    - Email / File Encryption
  - SSH
    - Authentication & Encryption
  - SSL
    - Certificates (PKI)
    - Authentication & Encryption
-

# Hashing

- ❑ One-way
- ❑ No Keys
- ❑ Message Integrity
- ❑ Not Encryption



---

# Hashing Examples

- Passwords
    - Windows – NTLM & NTLMv2
    - UNIX / Linux – Crypt, MD5, Blowfish
  - Digital Signatures
    - Email Integrity
    - File Integrity
-

---

# Implementation & Operational Issues

- Key Management
    - Distribution
    - Loss
    - Protection
  - Integration
    - Applications
    - OS
    - Network
    - Users (Process)
  - Speed / Scalability
    - System Capacity
    - Transaction Delay
-

---

# Applications

- Email

- [www.hushmail.com](http://www.hushmail.com)
- Microsoft Outlook / Exchange
- PGP / GPG

- Whole Disk

- PointSec
  - Dekart
  - PGP / GPG
  - CryptFS
-

---

# Applications (cont.)

- File

- Microsoft EFS
- PGP / GPG
- Password – MS Office, Winzip, etc.

- Application Development

- RSA
  - Microsoft .NET
-

---

# Applications (cont.)

- Database
    - Oracle 10g
    - MS SQL 2005
  - Network
    - VPN - Cisco, Checkpoint, MS-RAS, etc.
    - SSH
    - HTTPS (SSL)
  - Authentication
    - Microsoft AD
    - Sun Identity Manager
    - Physical / Badge Access
-

---

# Wrap Up...

---

## Questions?

[Bayly.Eley@alltel.com](mailto:Bayly.Eley@alltel.com)