MSAck Hacklab

MSAck is prouds to announce:
“Metti al sicuro i tuoi dati: cifrali!”

Metti al sicuro i tuoi dati

- Perche':
  La privacy e' FONDAMENTALE

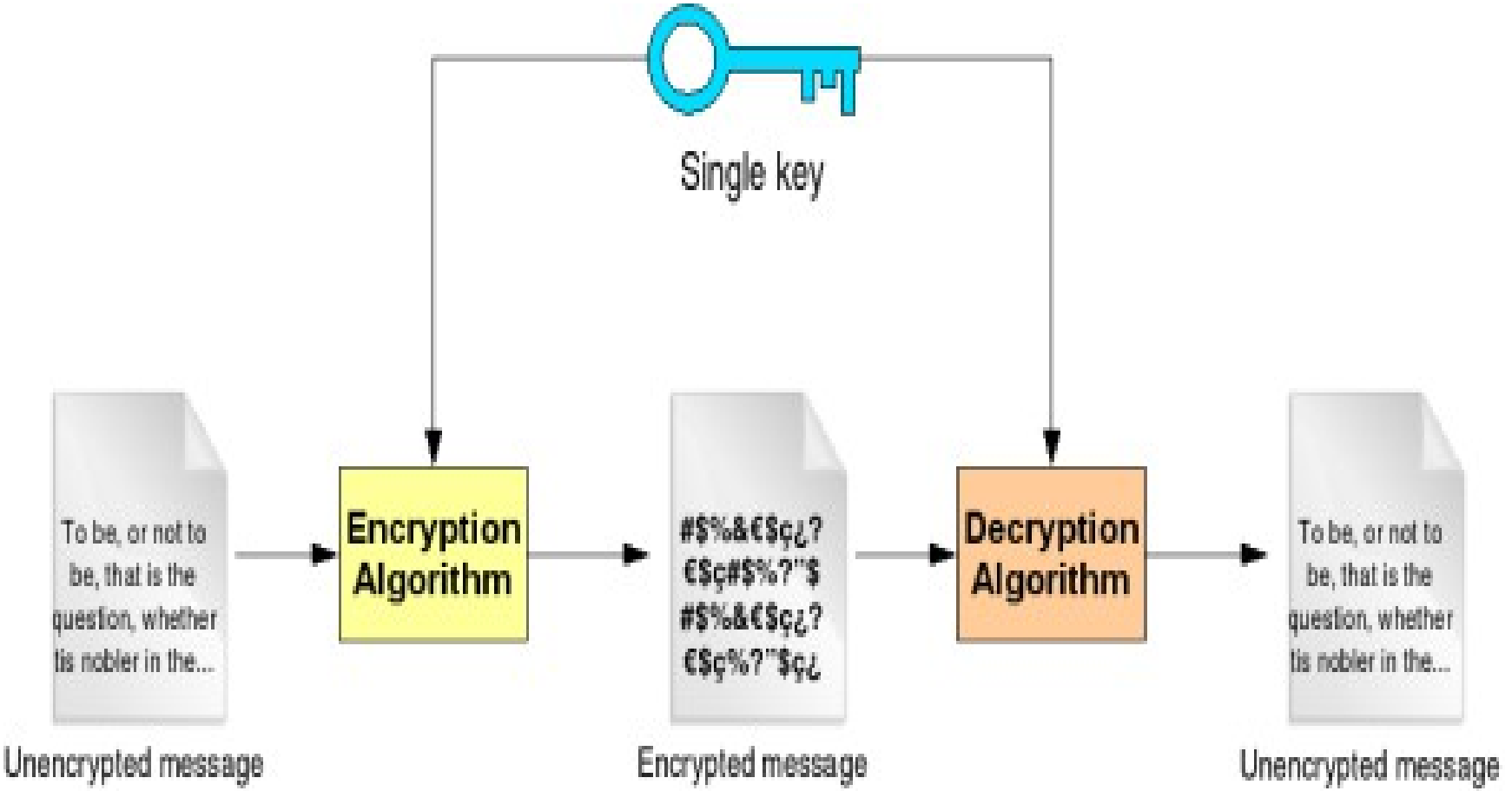
- Dove:
  Email, hard disk, file, swap/paging, etc.

- Come:
  Crittografia simmetrica/asimmetrica e relativi strumenti

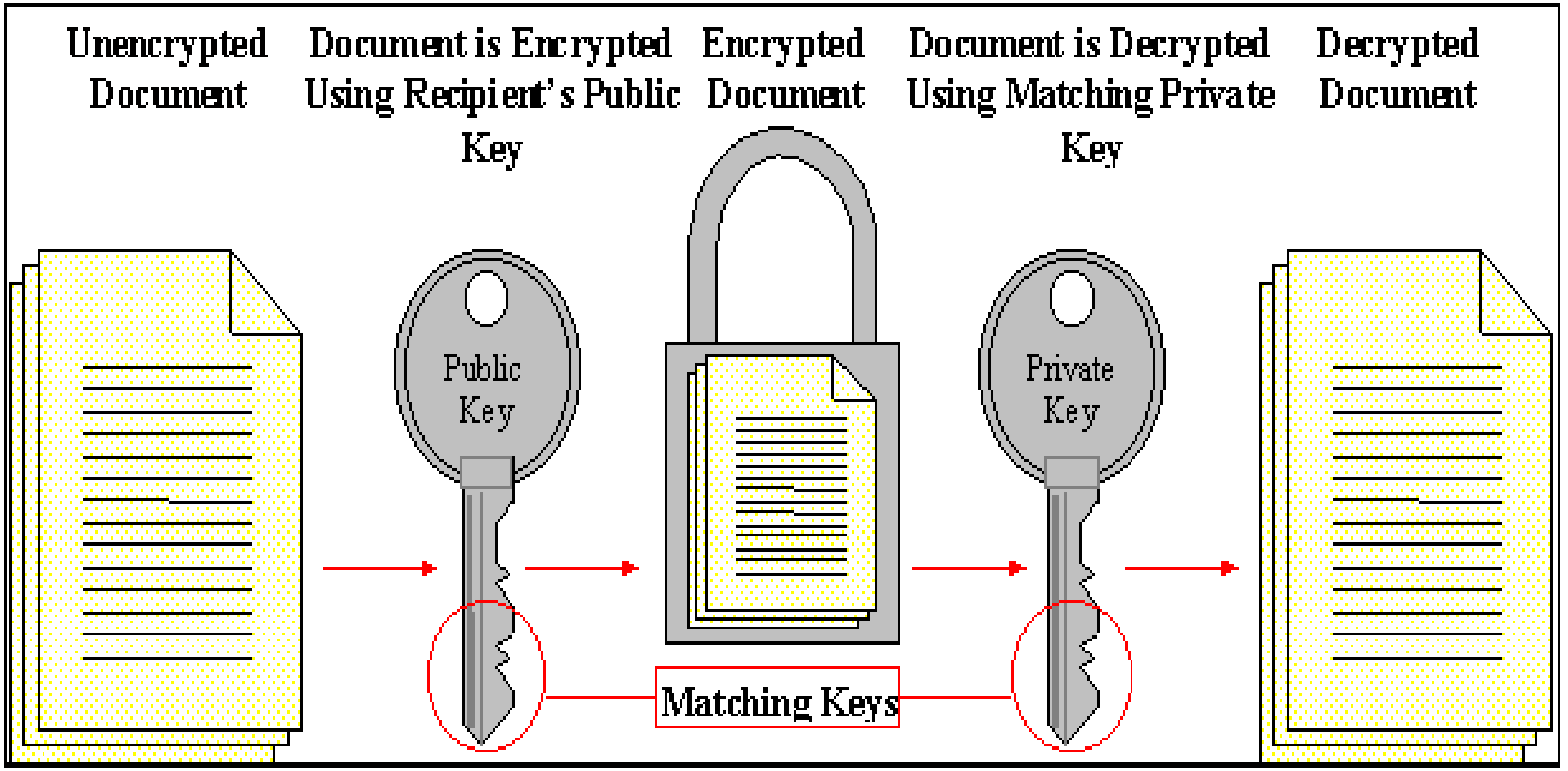
Crittografia

- Segretezza
- Integrita'
- Non ripudiabilita'

Crittografia simmetrica



Crittografia asimmetrica



Crittografia e firma digitale

- Crittografia
  Il mittente usa la chiave pubblica del destinatario per cifrare

- Firma Digitale
  Il mittente usa la propria chiave privata per cifrare il documento (o una parte)

Computer forensic: overview

- Recuperare dati rilevanti per un processo
- Data Recovery
- Data Carving

GPG: Gnu Privacy Guard

- Free software
- Crittografia asimmetrica/simmetrica
- Command line tool
- Gestione keyring
- Lanciato dalla Free Software Foundation
- Web of trust

GPG vs PGP

GnuPG:

- FLOSS
- Segue lo standard OpenPGP

PGP:

- Sviluppato da PGP Inc.
- Compatibile con lo standard OpenPGP
- Interagisce solo con determinati programmi Windows/MAC

Enigmail: GPG for Thunderbird

- Disponibile per (quasi) tutte le versioni di Thunderbird
- Crea nuove chiavi
- Importa chiavi gia' esistenti
- Cripta/decripta al volo

FireGPG: GPG for Firefox

- Estensione per Firefox 3
- Cripta/decripta al volo
- Supporta svariate webmail (non tutte)

OutlookGnuPG: GPG for Outlook

- Solo per Outlook 2007
- Necessita GnuPG (gpg.exe)
- Integra le stesse funzioni di Enigmail

Password manager

- Keepassx (Gnome) (Linux, Mac & Windows)
- Pwman (text/ncurses)
- PwManager (KDE)
- Firefox db (NON sicuro!)

LUKS

- Specifica uno standard di cifratura hard disk
- Tecnica del device-mapper
- Dm-crypt + cryptsetup su GNU/Linux
- Utile impostare in fase di installazione (magari dopo aver 'wipeato' l'hd)
- Possibilita' di avere certificati e chiavi di vario tipo (anche su USB)

EncFS

- File system crittato in user space
- File-by-file invece del device-mapper

Vantaggi:

- Non c'e' bisogno di formattare
- Facilissimo da usare

Svantaggi:

- Metadati non cifrati

ecryptfs

- Filesystem vero e proprio
- Possibilita' di selezionare cosa crittare e cosa no
- Trasparente
- Possibilita' di cifrare solo determinati file e condividerli in rete tranquillamente (informazioni di crypt/decrypt nell'header metadata)

Cifrare Windows

- BitLocker (nativo da Vista in poi solo per versioni Business/Ultimate)
- TrueCrypt (terze parti)
- FreeOTFE (terze parti)

Cifrare Windows: BitLocker

- Disponibile solo per Windows Vista Ultimate/Enterprise e Windows 7 Ultimate

- Cifra l'intero hard disk e dischi removibili (USB)

- Necessita due partizioni: una di boot (= per far avviare il sistema operativo) e una con Windows (che verra' cifrata)

- Crittografia simmetrica (AES 128bit o 256bit)

Cifrare Windows: TrueCrypt

- Open Source
- Crittografia disco/file-disk
- Crittografia simmetrica (AES 256bit ed altri) e HASH (SHA-512 ed altri)
- Hidden Operating System

FreeOTFE

- Stile TrueCrypt
- File-disk/full disk
- Cifratura simmetrica AES ed hashing MD5/SHA

Cosa cifrare

Linux:

- swap
- /tmp
- /home
- eventuali in /etc

Tutti:

- Password
- Carte di credito e PIN
- Altre chiavi crittografiche
- Tutto quello che ritenete privato e volete mantenere privato