Encryption and Forensics/Data Hiding

Cryptography Background

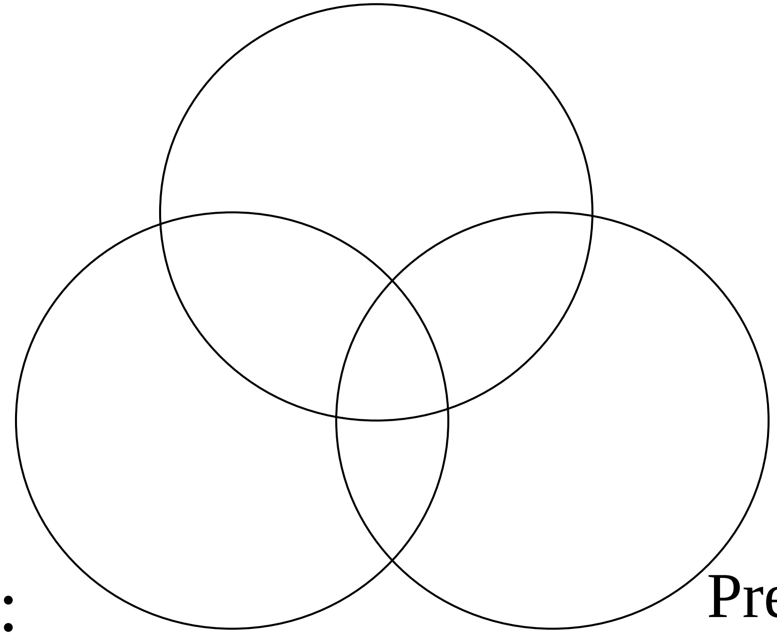
See:

http://www.cacr.math.uwaterloo.ca/hac/

For more information

Security Objectives

Confidentiality (Secrecy):
Prevent/Detect/Deter improper disclosure of information



Integrity:
Prevent/Detect/Deter improper modification of information

Availability:
Prevent/Detect/Deter improper denial of access to services provided by the system

Security Services

- Confidentiality: protection of any information from being exposed to unintended entities.
  - Information content
  - Parties involved
  - Where they are, how they communicate, how often, etc.
- Authentication: assurance that an entity of concern or the origin of a communication is authentic - it's what it claims to be or from
- Integrity: assurance that the information has not been tampered with

Encryption/Decryption

$$\text{plaintext} \xrightarrow{\text{encryption}} \text{ciphertext} \xrightarrow{\text{decryption}} \text{plaintext}$$

- Plaintext: a message in its original form
- Ciphertext: a message in the transformed, unrecognized form
- Encryption: the process for producing ciphertext from plaintext
- Decryption: the reverse of encryption
- Key: a secret value used to control encryption/decryption

Cryptanalysis: Break an Encryption Scheme

- Ciphertext only
  - Analyze only with the ciphertext
  - Exhaustive search until “recognizable plaintext”
  - Need enough ciphertext
- Known Plaintext
  - <plaintext, ciphertext> is obtained
  - Great for monoalphabetic cipher
- Chosen Plaintext:
  - Choose plaintext, get the ciphertext
  - Useful if limited set of messages

Methods for Attacking Encrypted Text

- Table 4-1 of the textbook
- Cryptanalysis
  - Ciphertext only
    - Analyze only with the ciphertext
    - Exhaustive search until “recognizable plaintext”
    - Need enough ciphertext
  - Known Plaintext
    - <plaintext, ciphertext> is obtained
  - Chosen Plaintext:
    - Choose plaintext, get the ciphertext
    - Useful if limited set of messages
- Password Guess (Similar to known plaintext)
  - Dictionary
  - Educated Guess
  - Brute Force

Methods for Attacking Encrypted Text – Con’t

- Scavenge Password
  - Physical Search
  - Logical Search
  - Network Sniff
- …

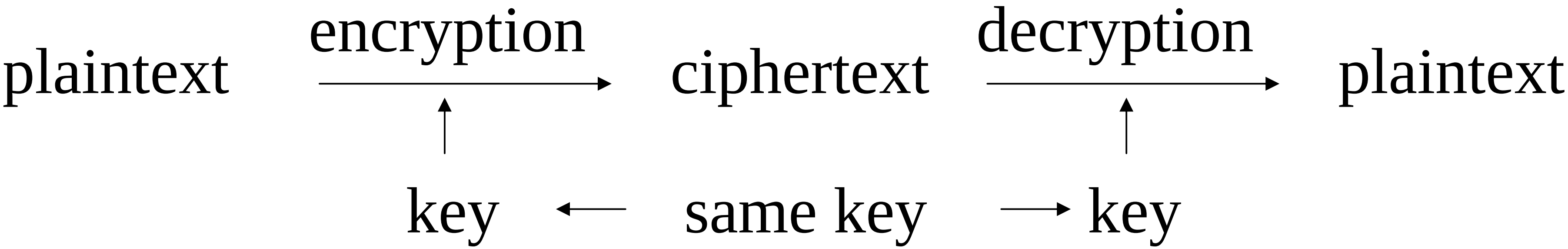
Computationally Difficult

- Cryptographic algorithms need to be reasonably efficient
- Cryptographic algorithms are not impossible to break with the key
  - e.g. try all the keys – brute-force cryptanalysis
  - Time can be saved by spending money on more computers.
- A scheme can be made more secure by making the key longer
  - Increase the length of the key by one bit
    - The good guy’s job just a little bit harder
    - The bad guy’s job up to twice as hard.

Types of Cryptographic functions

- Secret Key Cryptography
  - One key
- Public Key Cryptography
  - Two keys: public, private
- Hash function
  - No key

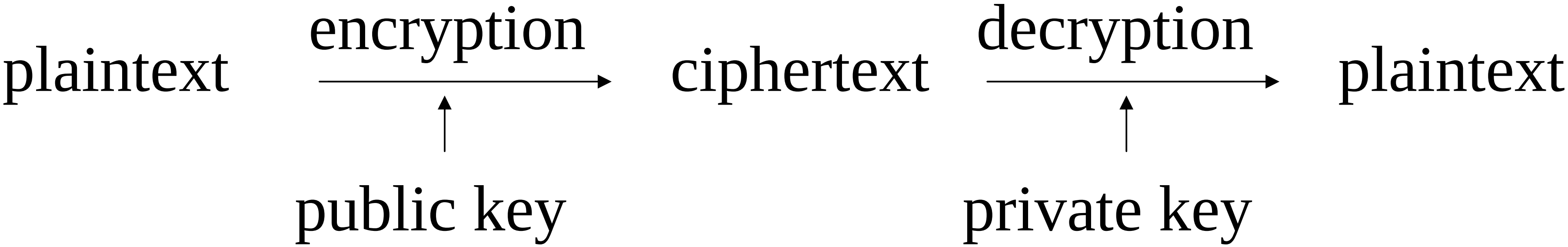
Secret Key Cryptography



plaintext
encryption
ciphertext
decryption
plaintext
key
same key
key

- Same key is used for both encryption and decryption
  - Symmetric cryptography
  - Conventional cryptography
- Ciphertext is about the same length as the plaintext
- Examples: DES, IDEA, AES…

Public Key Cryptography



plaintext

encryption

ciphertext

decryption

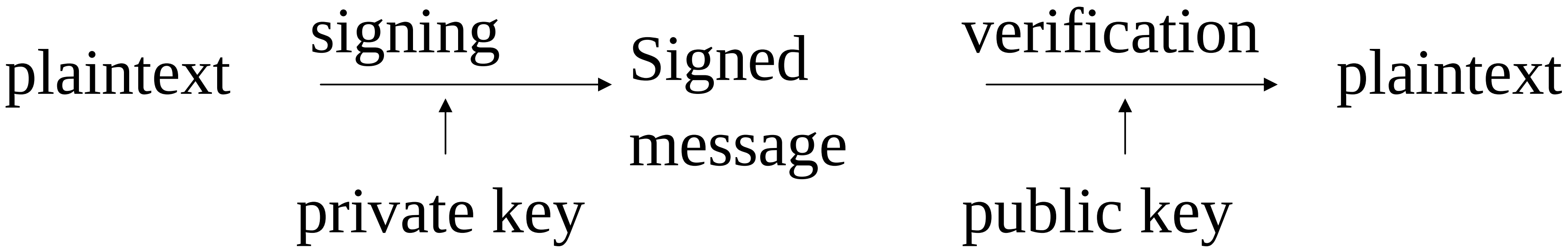
plaintext

public key

private key

- Invented/published in 1975
- Each individual has two keys:
  - Private key is kept secret
  - Public key is publicly known
- Much slower than secret key cryptography
- Also known as
  - Asymmetric cryptography

Public Key Cryptography cont’d



plaintext

signing

private key

Signed message

verification

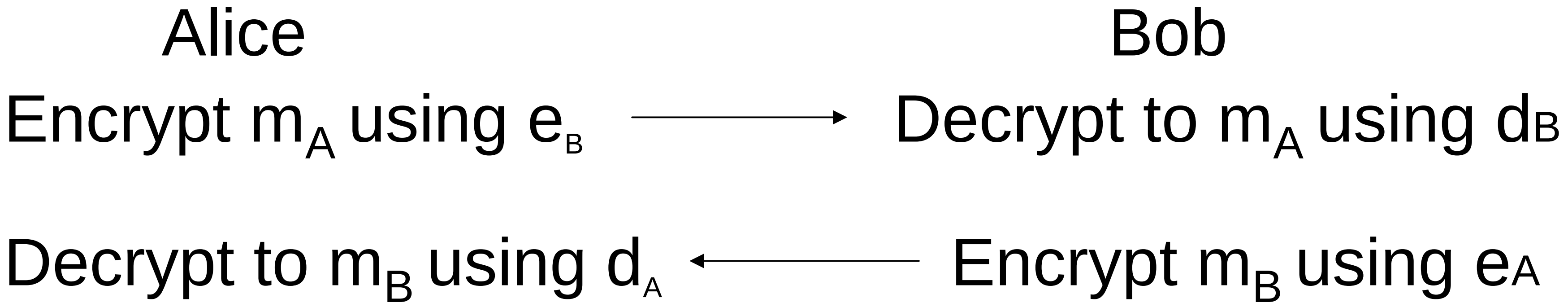
public key

plaintext

- Digital Signature
  - Only the party with the private key can generate a digital signature
  - Verification of the signature only requires the knowledge of the public key
  - The signer cannot deny he/she has done so.
  - Example illustrated in Fig. 4-4 and 4-5

Applications of Public Key Cryptography

- Security uses of public key cryptography
  - Known public key cryptography is orders of magnitude slower than the best known secret key cryptographic algo.
- Transmitting over an Insecure Channel



Alice

Bob

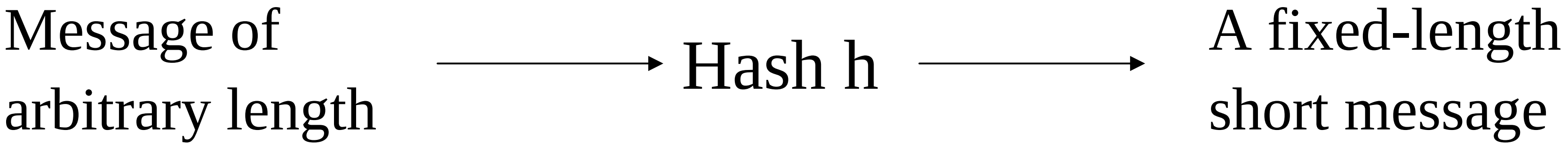
Encrypt m_A using e_B → Decrypt to m_A using d_B

Decrypt to m_B using d_A ← Encrypt m_B using e_A

- e: public key, d: private key
- Secure Storage on Insecure Media
  - Because of performance issues, you can randomly generate a secret key, encrypt the data with that secret key, and encrypt the secret key with the public key
  - Using public key of a trusted person

Hash Algorithms

- Message digests, one-way transformations



Message of arbitrary length

Hash h

A fixed-length short message

- Easy to compute h(m)
- Given h(m), no easy way to find m
- Computationally infeasible to find m_1 and m_2, so that $h(m_1) = h(m_2)$

Trusted Intermediaries

- Cannot do pair-wise authentication with secret key technology
  - Each computer needs to know n-1 keys
- Key Distribution Center (KDC)
- Certification Authorities (CAs)
- Certificate

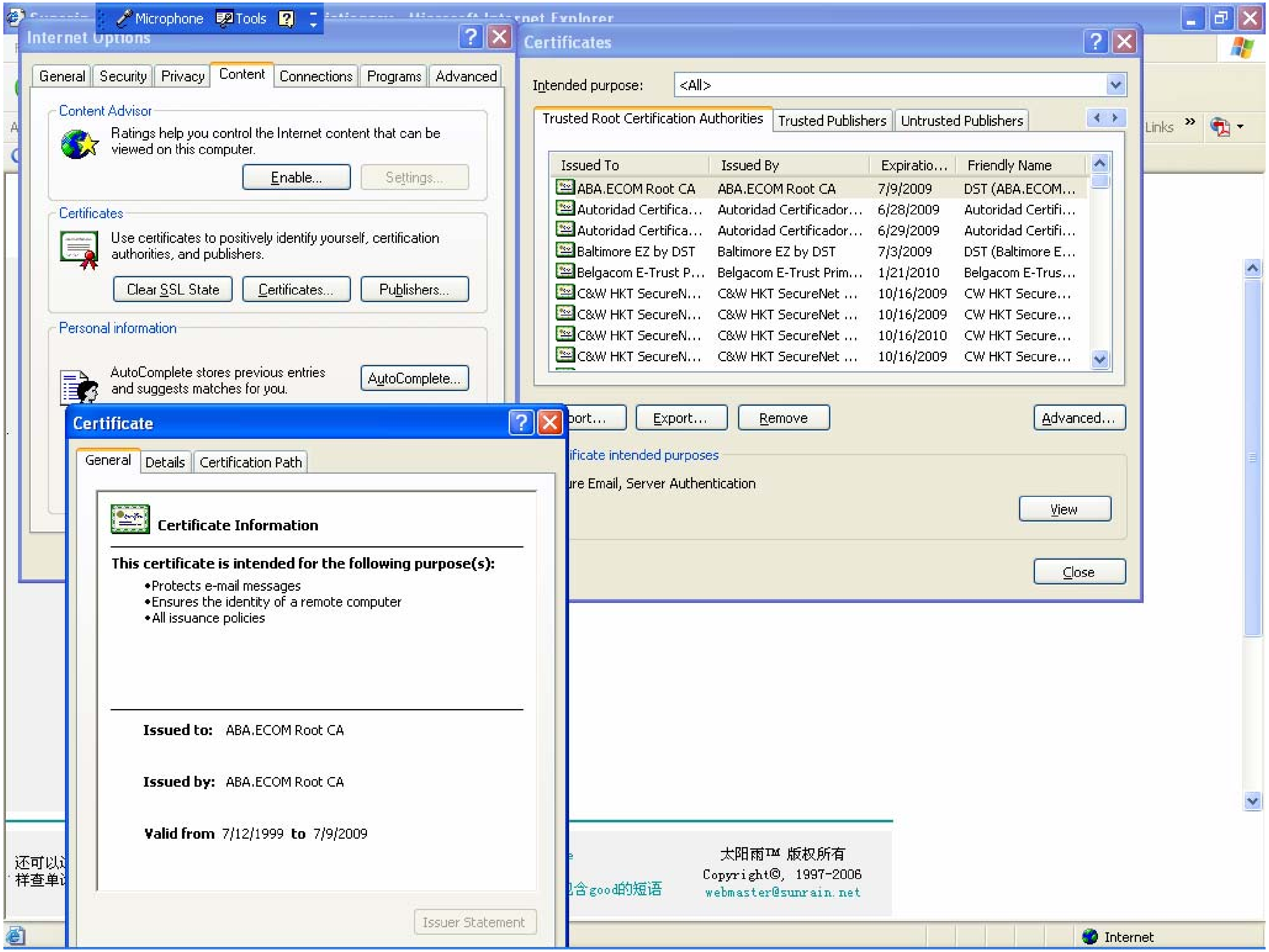
Key Distribution Center

- Use a trusted node known as Key Distribution Center (KDC)
  - Secret key cryptography
- The KDC knows keys for all nodes
  - α asks KDC for secret (securely) to talk to β
  - KDC encrypts $R_{\alpha\beta}$ with the key shared between α and KDC, send to α
  - KDC encrypts $R_{\alpha\beta}$ with the key shared between β and KDC, send to β : ticket

Certification Authorities (CAs)

- Public key cryptography
  - Problem: How can you be sure that the public keys are correct?
- CA: ensure validity of public keys
- Certificates
  - Signed messages specifying a name (Alice) and the corresponding public key
  - All nodes need to be preconfigured with the CA’s public key

Certificate Authorities Trusted by IE



Ratings help you control the Internet content that can be viewed on this computer.

Use certificates to positively identify yourself, certification authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
ABA.ECOM Root CA	ABA.ECOM Root CA	7/9/2009	DST (ABA.ECOM...
Autoridad Certifica...	Autoridad Certificador...	6/28/2009	Autoridad Certifi...
Autoridad Certifica...	Autoridad Certificador...	6/29/2009	Autoridad Certifi...
Baltimore EZ by DST	Baltimore EZ by DST	7/3/2009	DST (Baltimore E...
Belgacom E-Trust P...	Belgacom E-Trust Prim...	1/21/2010	Belgacom E-Trus...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2010	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/2009	CW HKT Secure...

...ificate intended purposes

...ure Email, Server Authentication

Certificate Information

This certificate is intended for the following purpose(s):

- Protects e-mail messages
- Ensures the identity of a remote computer
- All issuance policies

Issued to: ABA.ECOM Root CA

Issued by: ABA.ECOM Root CA

Valid from 7/12/1999 **to** 7/9/2009

还可以让
样查单i

...含good的短语

太阳雨™ 版权所有
Copyright©, 1997-2006
webmaster@sunrain.net

- http://www.microsoft.com/technet/prodtechnol/ie/reskit/6/part2/c06ie6rk.mspx?mfr=true

Certification Practice Statement

- Certification Practice Statement (CPS)
  - How certificate authorities operate, maintain the security of their infrastructures.
  - Certificate Revocation List
- One example:
  - Verisign CPS
    - http://www.verisign.com/repository/CPS/

Codes and Compression

- uuencode
  - http://www.winzip.com/uu00002.htm
  - Uuencoding obscures binary data, but not ASCII text
  - Winzip can open and extract uuencoded files
- Compression
  - Recognizable patterns
  - Lossless data compression
    - Zip, gzip
    - GIF, TIFF..
  - Lossy data compression
    - JPEG, MPEG…
- Data is often compressed before it is encrypted

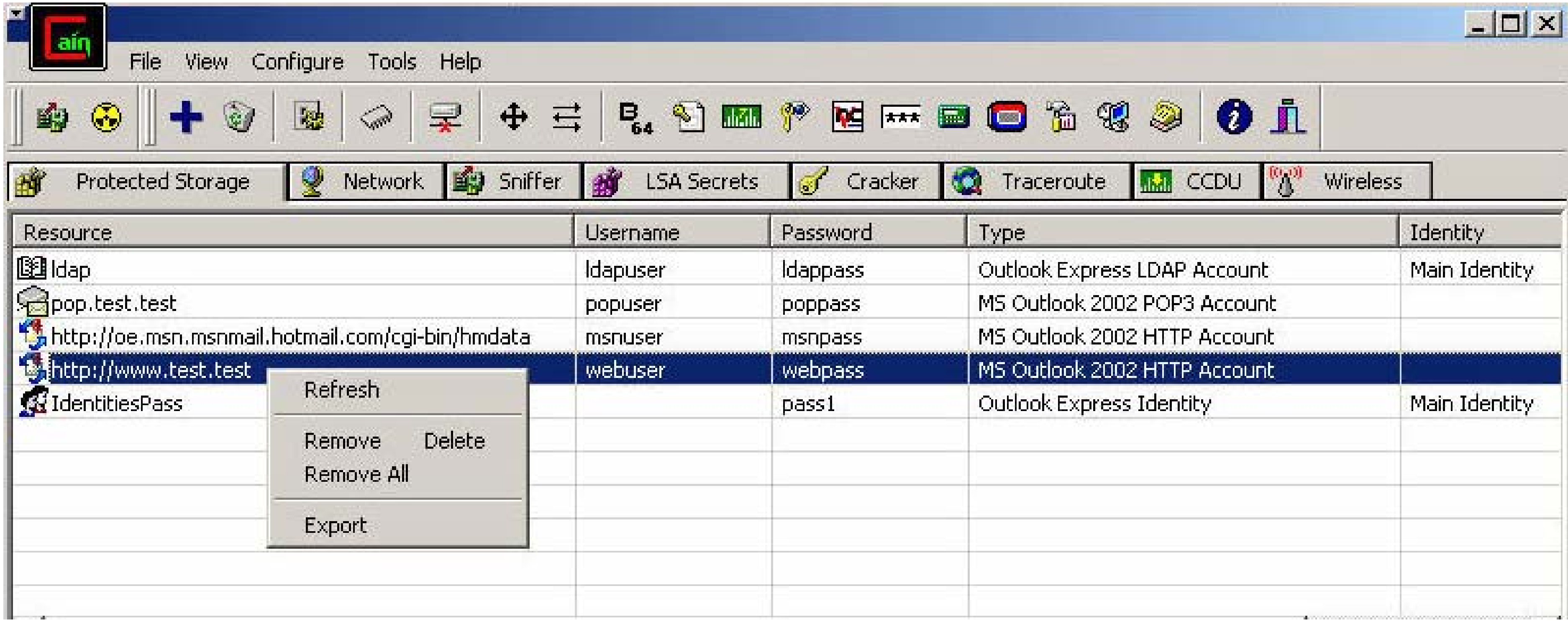
Challenges

- Any transformation performed on text data make it difficult or impossible to do a batch search for keywords!
- How to identify encrypted data
  - – To see if it can be compressed

Password recovery tool for Windows

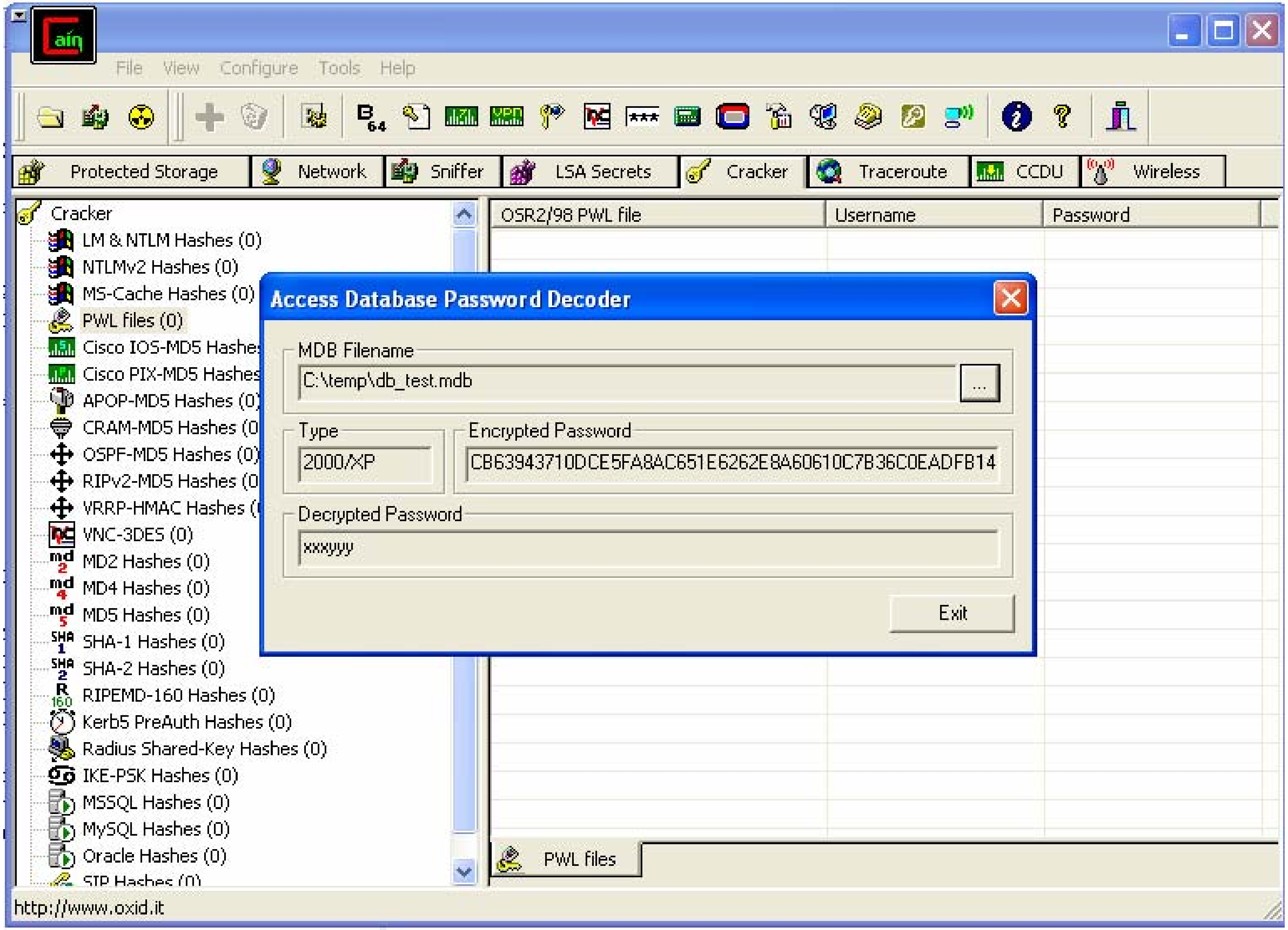
- Cain:
  - *http://www.oxid.it/cain.html (Doc: http://www.oxid.it/ca_um/)*
  - Uncovering cached password
  - Recovering password by sniffing the network
  - Cracking encrypted password using Dictionary
  - Brute-force and Cryptanalysis attacks
  - …

Cain – uncover password from protected storage



Resource	Username	Password	Type	Identity
ldap	ldapuser	ldappass	Outlook Express LDAP Account	Main Identity
pop.test.test	popuser	poppass	MS Outlook 2002 POP3 Account	
http://oe.msn.msnmail.hotmail.com/cgi-bin/hmdata	msnuser	msnpass	MS Outlook 2002 HTTP Account	
http://www.test.test	webuser	webpass	MS Outlook 2002 HTTP Account	
IdentitiesPass		pass1	Outlook Express Identity	Main Identity

Cain – attack against encrypted password



Access Database Password Decoder

MDB Filename: C:\temp\db_test.mdb

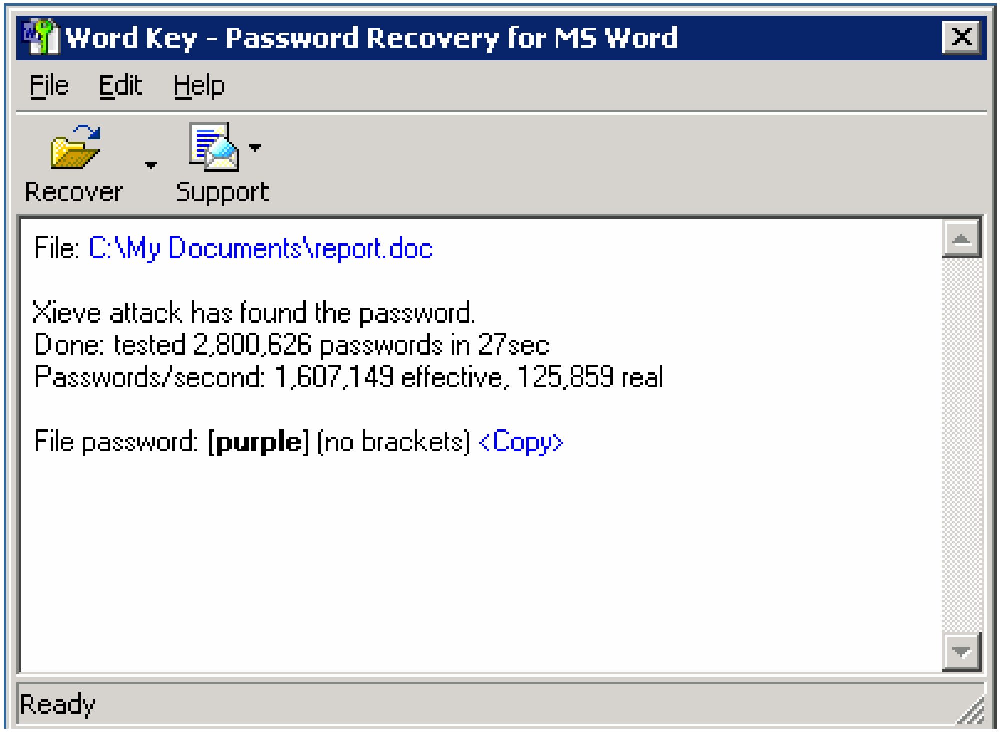
Type: 2000/XP

Encrypted Password: CB63943710DCE5FA8AC651E6262E8A60610C7B36C0EADFB14

Decrypted Password: xxxyyy

Password Cracker

- www.lostpassword.com



File: C:\My Documents\report.doc

Xieve attack has found the password.
Done: tested 2,800,626 passwords in 27sec
Passwords/second: 1,607,149 effective, 125,859 real

File password: [**purple**] (no brackets) <Copy>

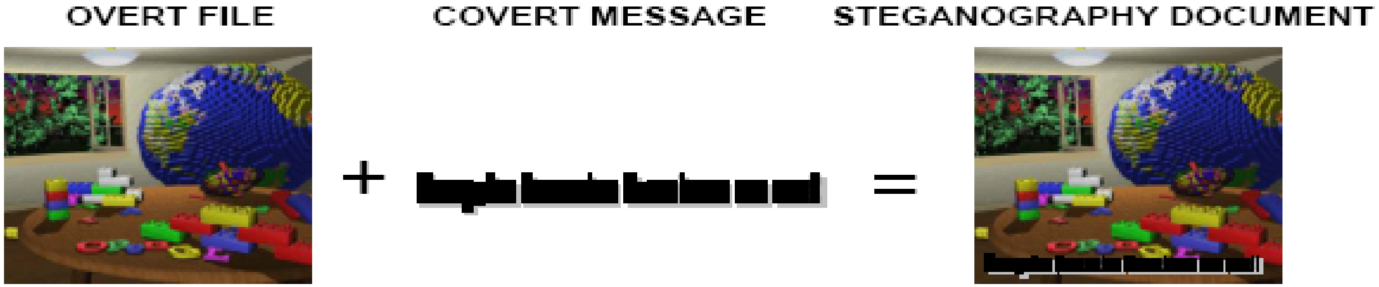
- L0phCrack
- ZipPassword

Hiding and Finding Data

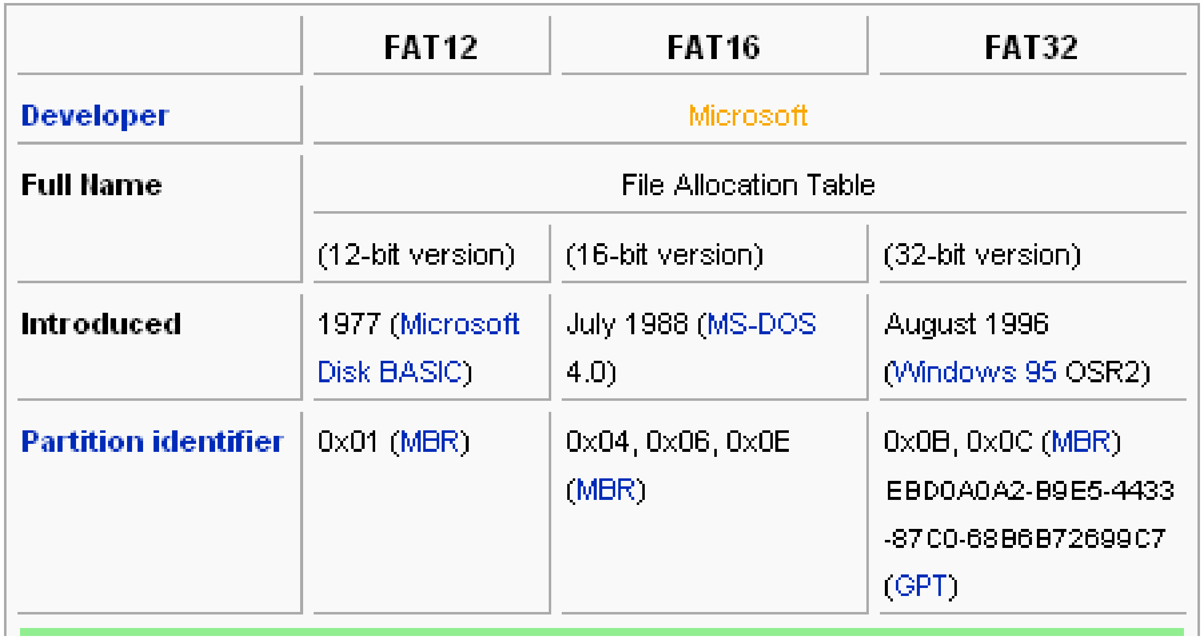
- Changing a file’s extension
  - Windows uses the filename extension to identify the data type of the file
  - *Quick View Plus*
- Check the file header
  - Contain a hexadecimal value that can be usually be correlated to file type
- File Format Information
  - *http://www.wotsit.org/*

Steganography

- Steganos: secret or hidden
- Graphy: drawing or writing
- http://www.stegoarchive.com/



File Systems



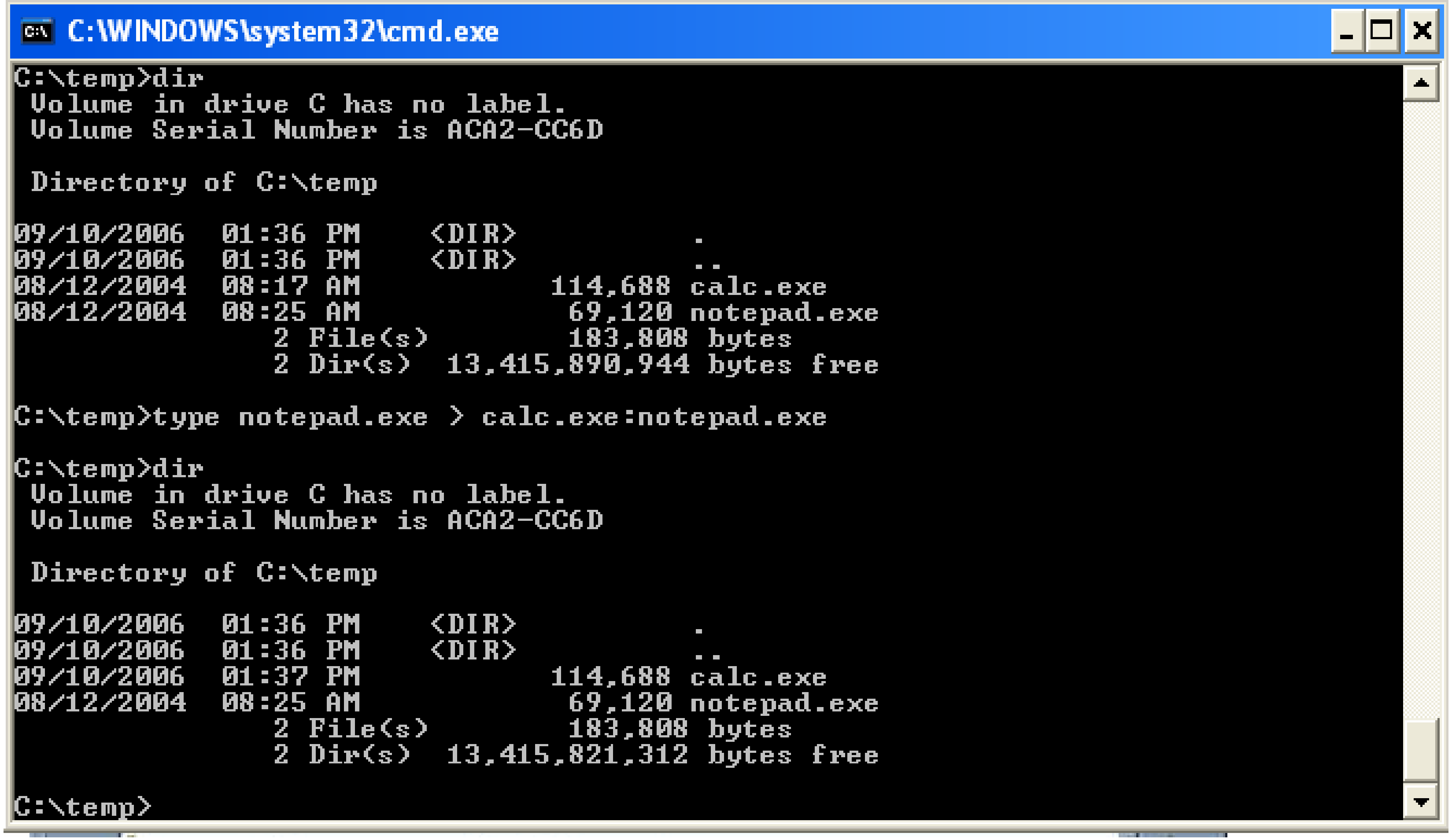
	FAT12	FAT16	FAT32
Developer	Microsoft		
Full Name	File Allocation Table		
	(12-bit version)	(16-bit version)	(32-bit version)
Introduced	1977 (Microsoft Disk BASIC)	July 1988 (MS-DOS 4.0)	August 1996 (Windows 95 OSR2)
Partition identifier	0x01 (MBR)	0x04, 0x06, 0x0E (MBR)	0x0B, 0x0C (MBR) EBD0A0A2-B9E5-4433-87C0-68B6B72699C7 (GPT)

- Windows NT and Windows XP support NTFS, FAT16, and FAT 32.

NTFS Alternate Data Streams (ADS)

- NTFS file systems supports multiple data streams
- Allow files to be associated with more than one data stream
- Method of hiding executables or proprietary content
- Uses NTFS file system multiple attributes
- Syntax – {file name}:{stream name}
- Create: type file > visible:hidden
- Reference:
  - – http://www.windowsecurity.com/articles/Alternate_Data_Streams.html

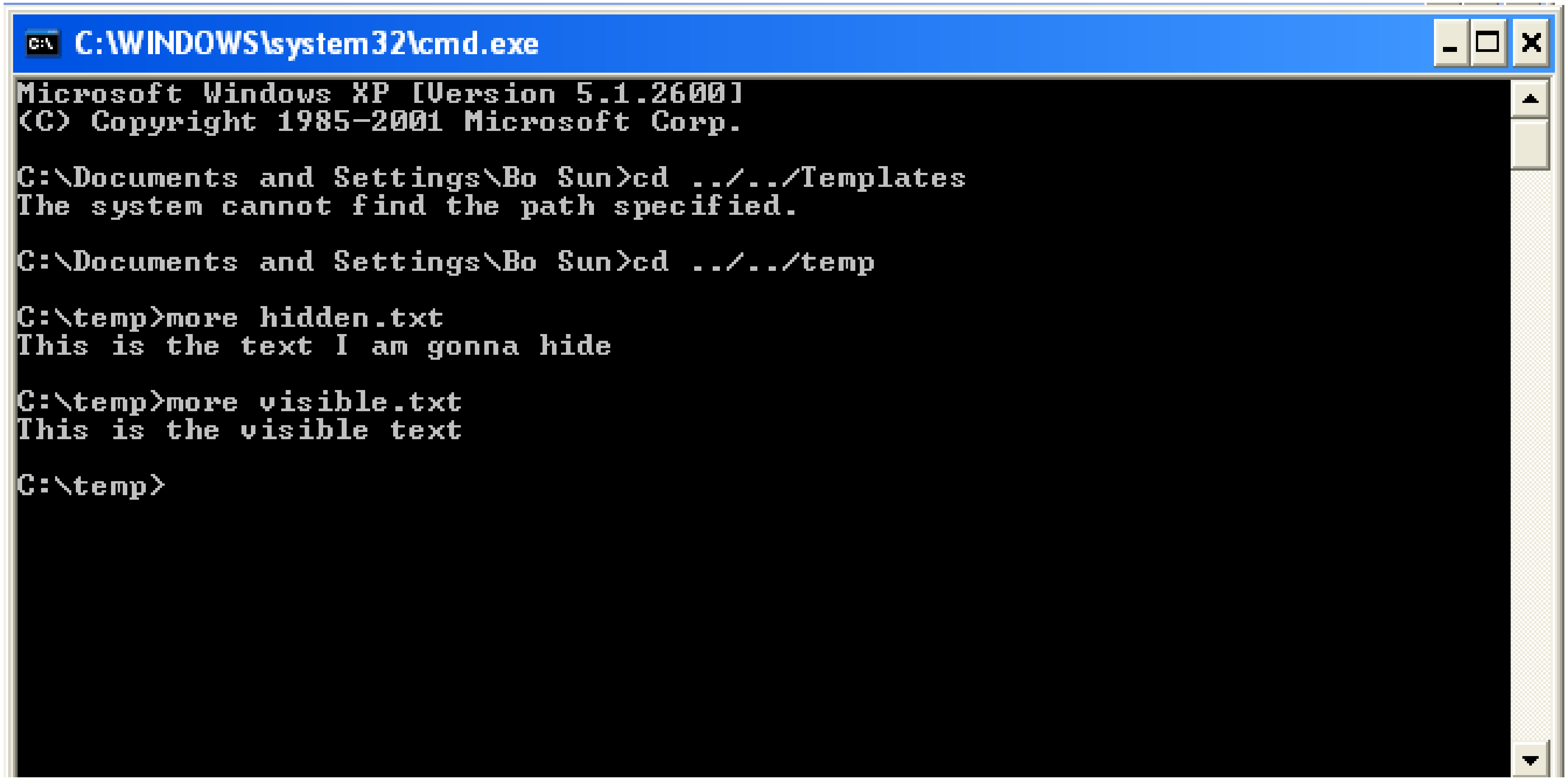
ADS Example 1



```
C:\temp>dir
 Volume in drive C has no label.
 Volume Serial Number is ACA2-CC6D

 Directory of C:\temp

09/10/2006  01:36 PM    <DIR>          .
09/10/2006  01:36 PM    <DIR>          ..
08/12/2004  08:17 AM           114,688 calc.exe
08/12/2004  08:25 AM            69,120 notepad.exe
               2 File(s)        183,808 bytes
               2 Dir(s)  13,415,890,944 bytes free

C:\temp>type notepad.exe > calc.exe:notepad.exe

C:\temp>dir
 Volume in drive C has no label.
 Volume Serial Number is ACA2-CC6D

 Directory of C:\temp

09/10/2006  01:36 PM    <DIR>          .
09/10/2006  01:36 PM    <DIR>          ..
09/10/2006  01:37 PM           114,688 calc.exe
08/12/2004  08:25 AM            69,120 notepad.exe
               2 File(s)        183,808 bytes
               2 Dir(s)  13,415,821,312 bytes free

C:\temp>
```

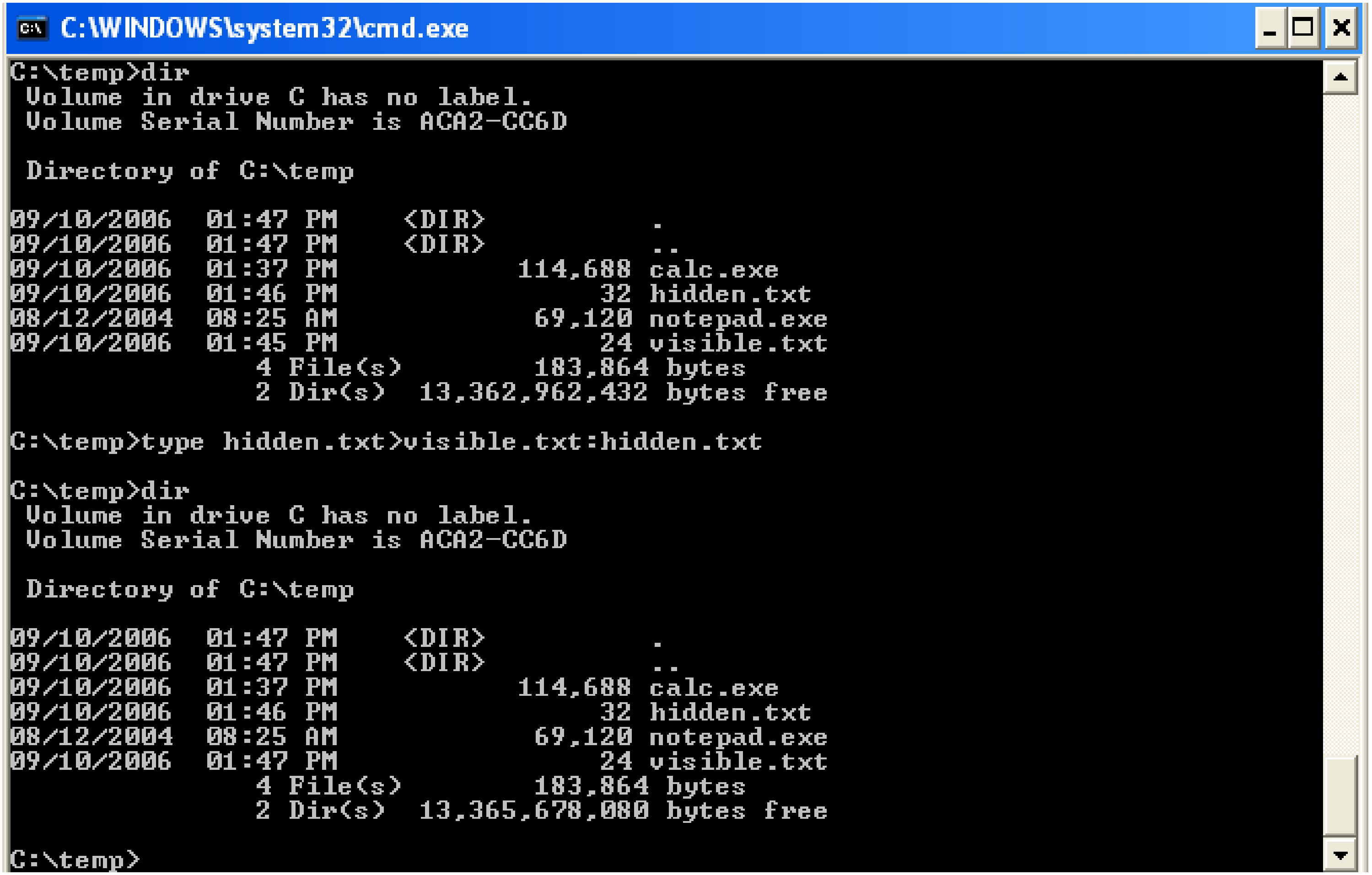
- *start c:\temp\calc.exe:notepad.exe*

ADS Example 2



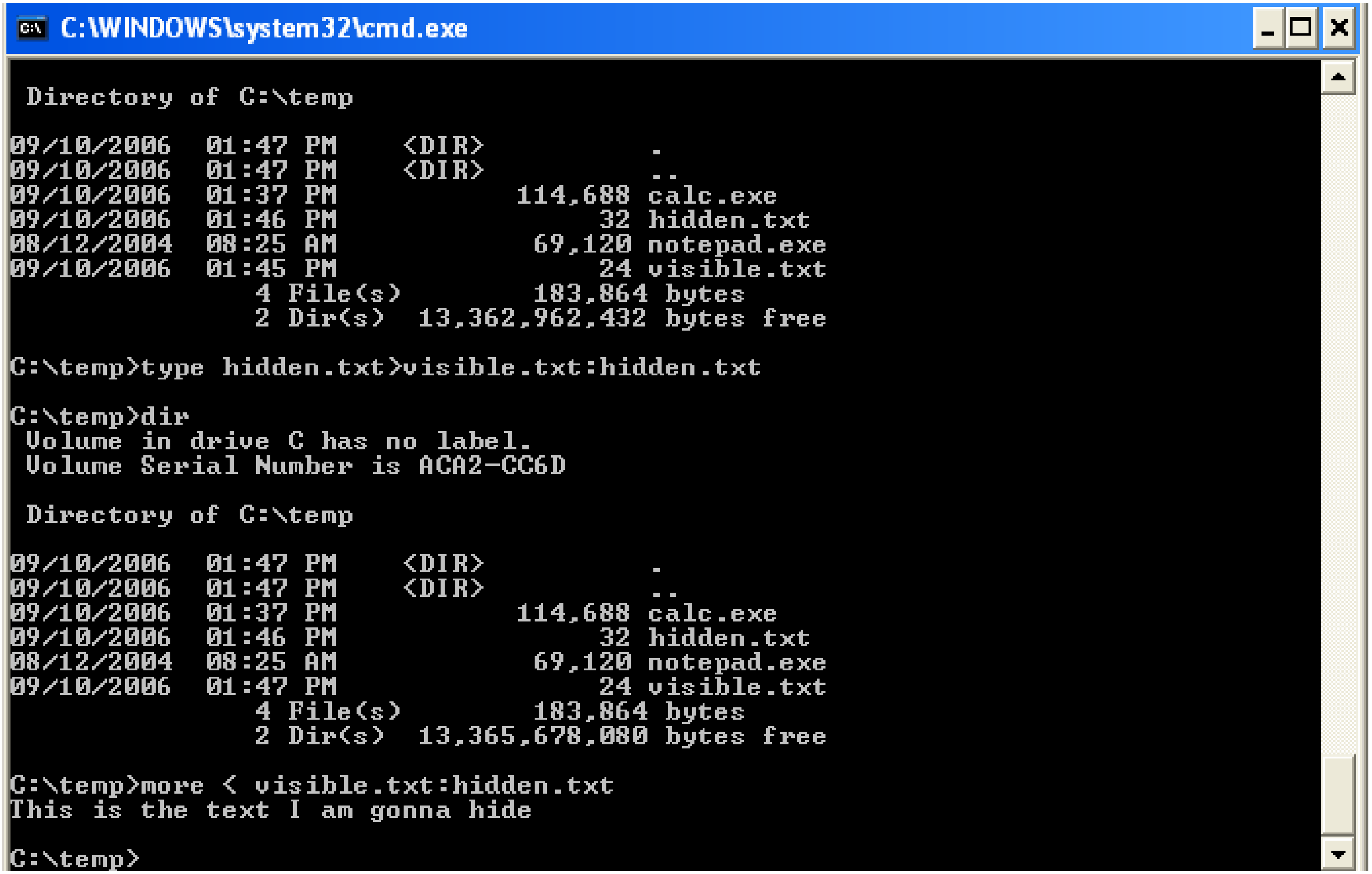
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Bo Sun>cd ../../Templates
The system cannot find the path specified.

C:\Documents and Settings\Bo Sun>cd ../../temp

C:\temp>more hidden.txt
This is the text I am gonna hide

C:\temp>more visible.txt
This is the visible text

C:\temp>
```

ADS Example 2 – Con’t



```
C:\temp>dir
 Volume in drive C has no label.
 Volume Serial Number is ACA2-CC6D

 Directory of C:\temp

09/10/2006  01:47 PM    <DIR>          .
09/10/2006  01:47 PM    <DIR>          ..
09/10/2006  01:37 PM           114,688 calc.exe
09/10/2006  01:46 PM                32 hidden.txt
08/12/2004  08:25 AM            69,120 notepad.exe
09/10/2006  01:45 PM                24 visible.txt
               4 File(s)        183,864 bytes
               2 Dir(s)  13,362,962,432 bytes free

C:\temp>type hidden.txt>visible.txt:hidden.txt

C:\temp>dir
 Volume in drive C has no label.
 Volume Serial Number is ACA2-CC6D

 Directory of C:\temp

09/10/2006  01:47 PM    <DIR>          .
09/10/2006  01:47 PM    <DIR>          ..
09/10/2006  01:37 PM           114,688 calc.exe
09/10/2006  01:46 PM                32 hidden.txt
08/12/2004  08:25 AM            69,120 notepad.exe
09/10/2006  01:47 PM                24 visible.txt
               4 File(s)        183,864 bytes
               2 Dir(s)  13,365,678,080 bytes free

C:\temp>
```

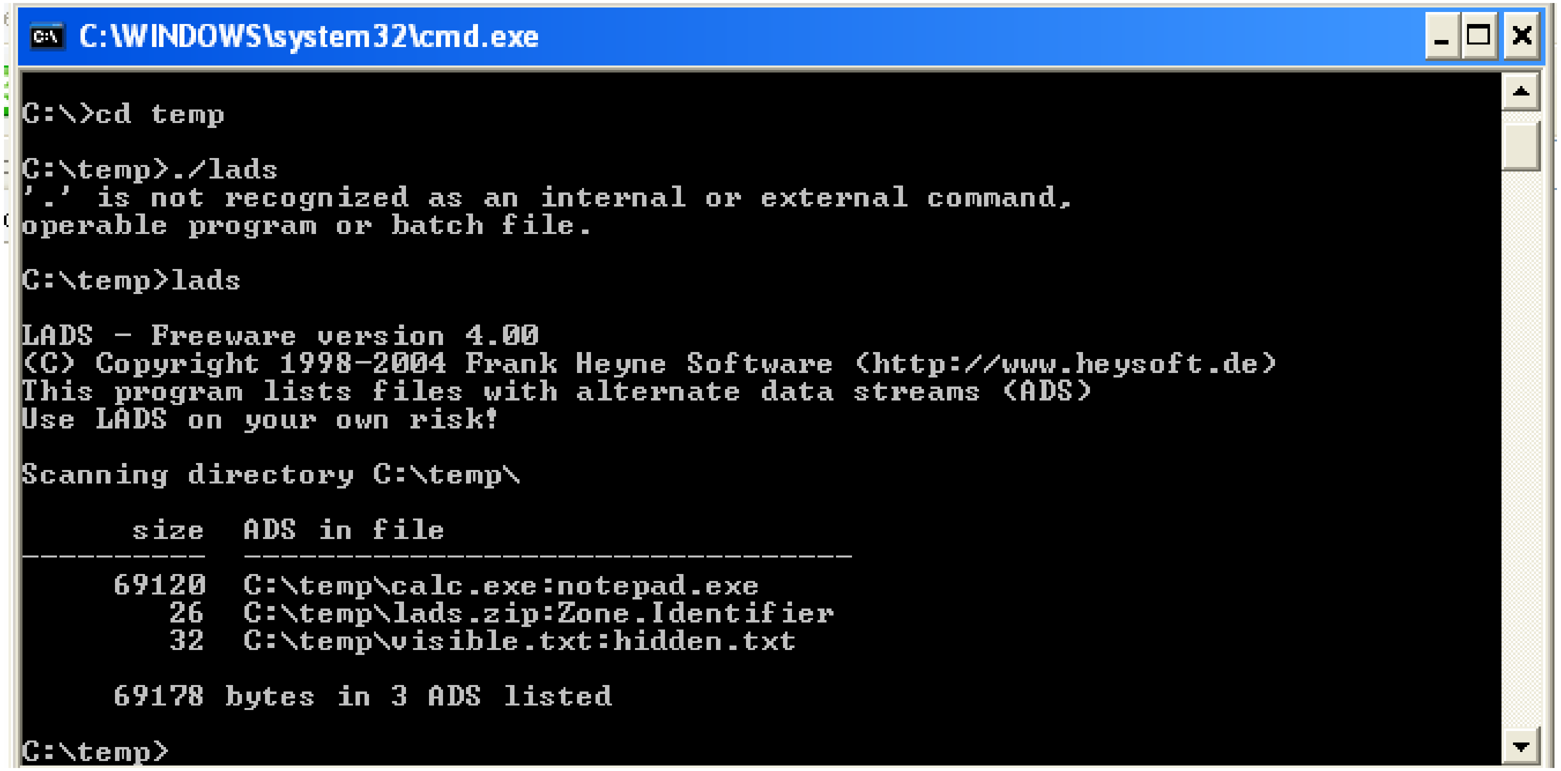
ADS Example 2– Con’t



```
 Directory of C:\temp

09/10/2006  01:47 PM    <DIR>          .
09/10/2006  01:47 PM    <DIR>          ..
09/10/2006  01:37 PM           114,688 calc.exe
09/10/2006  01:46 PM                32 hidden.txt
08/12/2004  08:25 AM            69,120 notepad.exe
09/10/2006  01:45 PM                24 visible.txt
               4 File(s)        183,864 bytes
               2 Dir(s)  13,362,962,432 bytes free

C:\temp>type hidden.txt>visible.txt:hidden.txt

C:\temp>dir
 Volume in drive C has no label.
 Volume Serial Number is ACA2-CC6D

 Directory of C:\temp

09/10/2006  01:47 PM    <DIR>          .
09/10/2006  01:47 PM    <DIR>          ..
09/10/2006  01:37 PM           114,688 calc.exe
09/10/2006  01:46 PM                32 hidden.txt
08/12/2004  08:25 AM            69,120 notepad.exe
09/10/2006  01:47 PM                24 visible.txt
               4 File(s)        183,864 bytes
               2 Dir(s)  13,365,678,080 bytes free

C:\temp>more < visible.txt:hidden.txt
This is the text I am gonna hide

C:\temp>
```

LADS – List Alternate Data Streams

- http://www.heysoft.de/nt/ep-lads.htm



```
C:\>cd temp

C:\temp>./lads
'.' is not recognized as an internal or external command,
operable program or batch file.

C:\temp>lads

LADS - Freeware version 4.00
(C) Copyright 1998-2004 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Scanning directory C:\temp\

      size  ADS in file
----------  ---------------------------------
     69120  C:\temp\calc.exe:notepad.exe
        26  C:\temp\lads.zip:Zone.Identifier
        32  C:\temp\visible.txt:hidden.txt

     69178 bytes in 3 ADS listed

C:\temp>
```