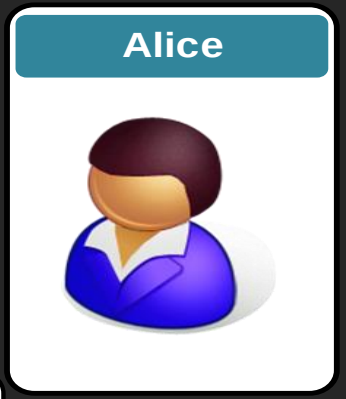
Advanced Crypto

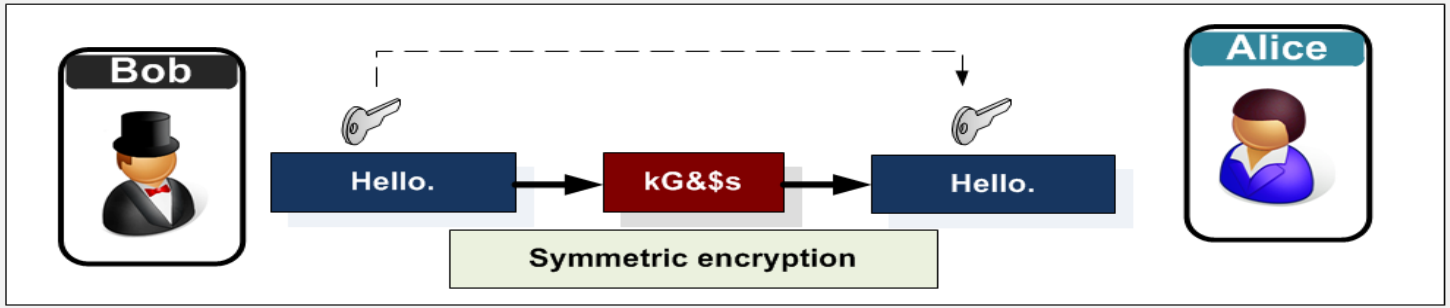
5. Disk Encryption



Introduction

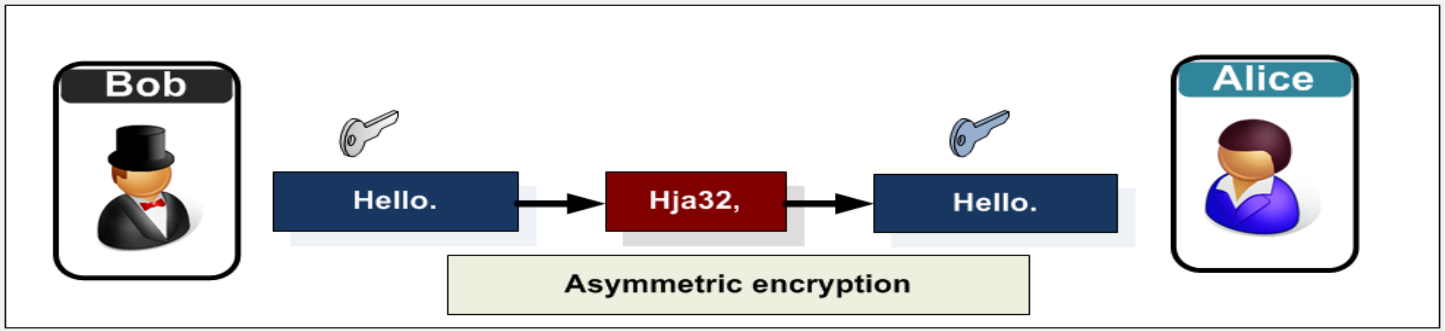
http://asecuritysite.com/crypto

Author: Prof Bill Buchanan



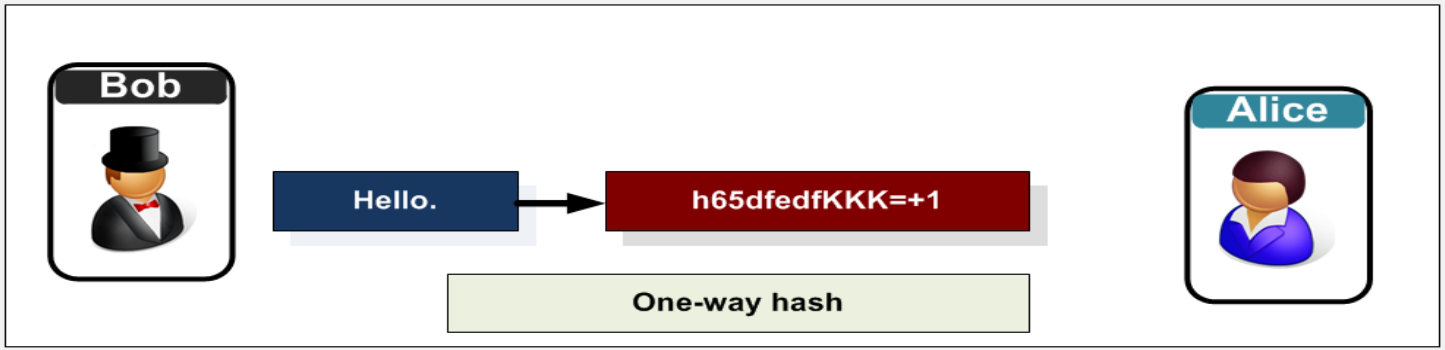
Private-key

Private-key: RC2, RC4, DES, 3DES, AES



Public-key

Public-key: RSA, DSA (factoring prime numbers) FIPS 186-2, ElGamal (Elliptic curve)



Hashing

Hashing: MD5, SHA-1

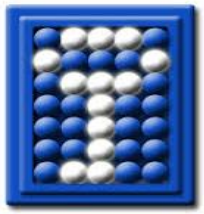
Strength: 80-bit DES -> 1024 RSA -> 160 bit Elliptic

File/Folder Encryption

Disk Encryption

Microsoft Bitlocker

Check Point Full Disk Encryption Software



TrueCrypt

McAfee Endpoint Encryption
Encryption Software

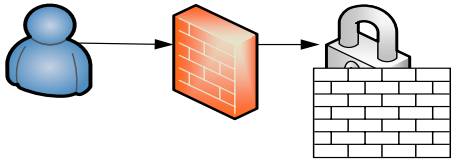
Axanum (.AXX)

Sophos SafeGuard Disk Encryption

Author: Prof Bill Buchanan

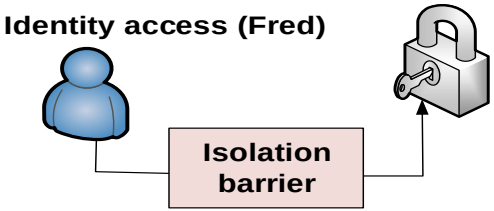
FIPS 140-2 Level 4

- Physical security requirements more stringent.
- Robustness against environmental attacks.



FIPS 140-2 Level 3

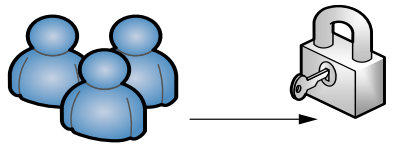
- Physical tamper-resistance.
- Identity-based authentication.
- Physical or logical separation between the interfaces by which where the key security parameters are entered or passed.



FIPS 140-2 Level 2

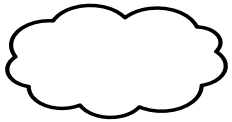
- Physical tamper-evidence.
- Role-based authentication.

O/S must be compliant for Level 2 and above



FIPS (Federal Information Processing Standards) 140-2 Level 1

- Lowest level with limited requirements.

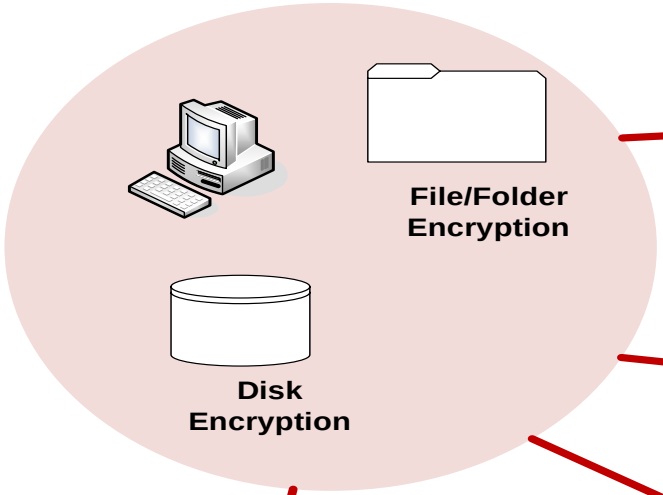


NIST

NIST publish 140 publication series for cryptography

- **FIPS 140-2 May 2001**
- **FIPS 140-3 Software limited to L1/L2.**

Author: Prof Bill Buchanan



File/Folder Encryption

Disk Encryption

Password or passphrase

NapI5r123$

USB drive with encryption key

OTP device such as an RSA token

Biometric device (eg fingerprint reader) with Trusted Platform Module which holds the actual encryption key

Multi-factor authentication uses two or more of these

Access

Disk Encryption

Author: Prof Bill Buchanan

Non-encrypted in transit

Non-encrypted
In memory

Non-encrypted in storage

Directory
structure

API/DLL
Integration
(c:, d:, etc)

Encryption Layer

Disk Storage

Cloud
Storage

Disk Image

File Image

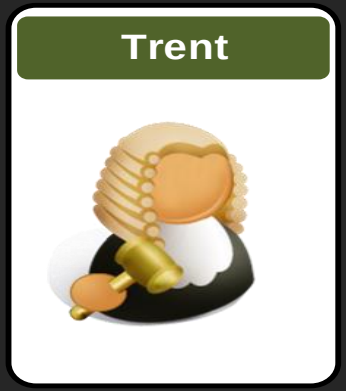
Access

Disk Encryption

Author: Prof Bill Buchanan

Advanced Crypto

5. Disk Encryption



BitLocker/EFS

http://asecuritysite.com/crypto

Author: Prof Bill Buchanan

EFS – Drive or Folder encryption

Transparent operation mode Uses TPM

- Trusted Platform Module (TPM) 1.2 hardware where user powers up and logs into Windows as normal.
- Encryption key is sealed (encrypted) in the TPM chip and released to the OS loader code if the early boot files appear to be unmodified.
- Pre-OS components of BitLocker use Static Root of Trust Measurement defined by the Trusted Computing Group (TCG). Mode is vulnerable with cold boot attack, where the intruder can boot the powered-down machine.

BitLocker Logical volume encryption

- NTFS Drive 1: Boot drive (unencrypted)
- NTFS Drive 2: Operating system – eg c: drive (encrypted)

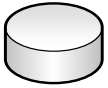
User authentication mode

Pre-boot PIN required

USB Key Mode

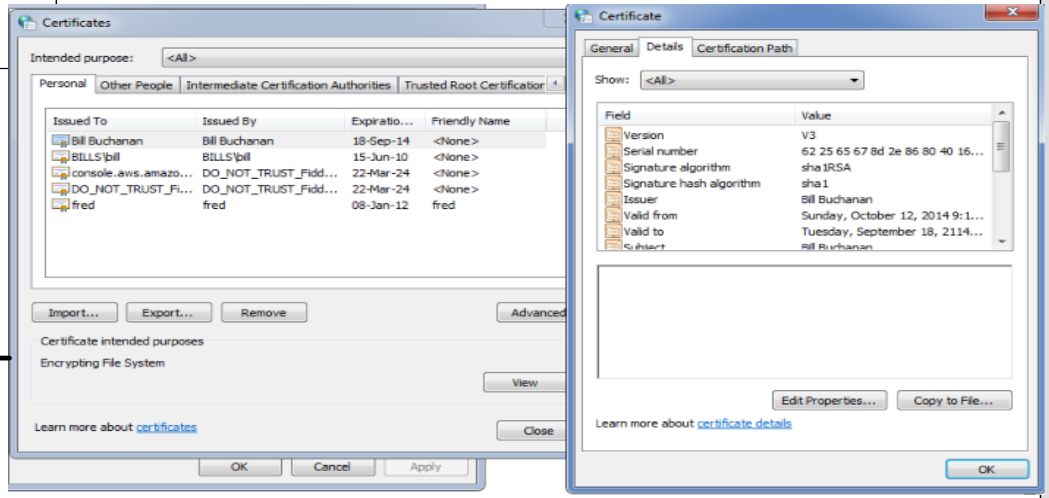
- Users inserts a USB device with a startup key into the computer for the boot to protected OS.
- BIOS must support the reading of USB devices in the pre-OS environment.

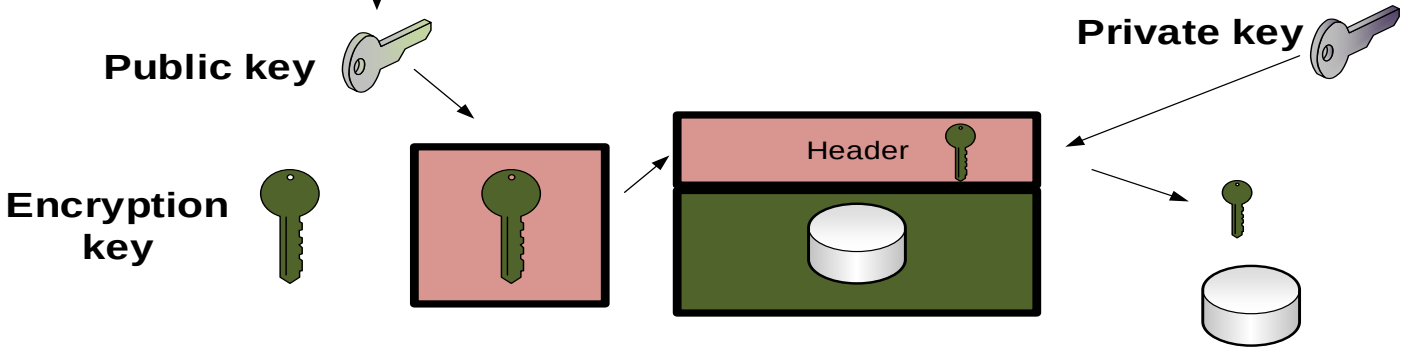
Author: Prof Bill Buchanan



EFS – Drive or Folder encryption

- CER file – Contains certificate.
- PFX – Contains certificate and private key.



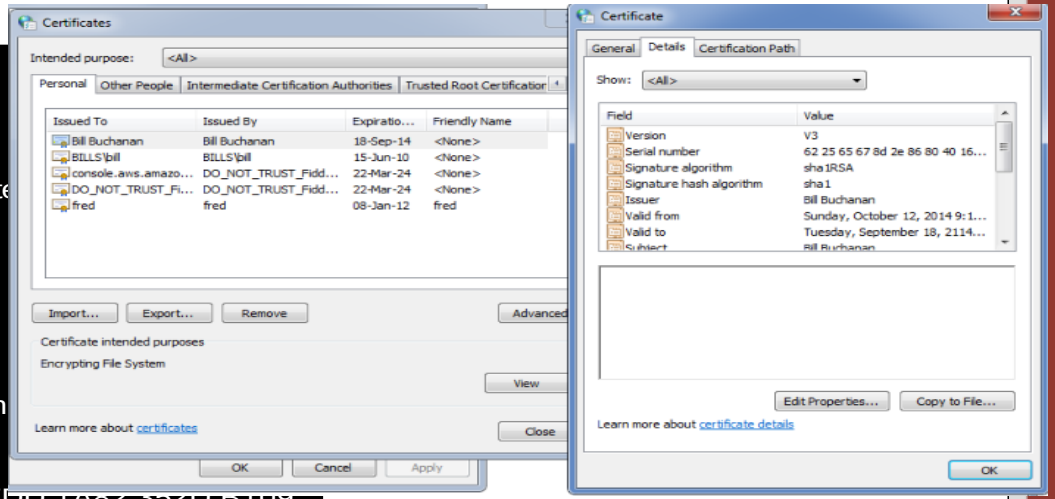


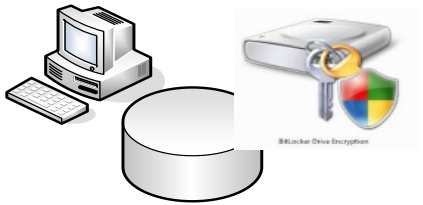
Author: Prof Bill Buchanan

Bitlocker

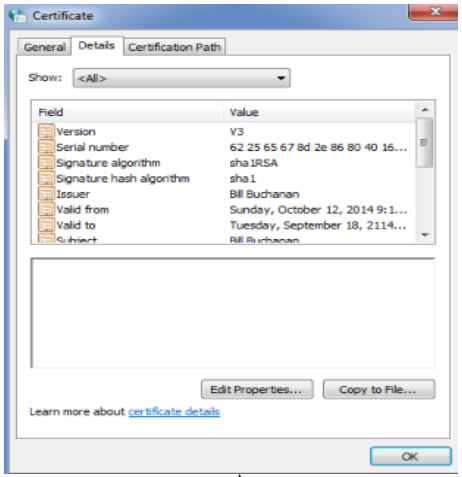
Disk Encryption

```
C:\enc\test>cipher /c test.docx

 Listing C:\enc\test\
 New files added to this directory will be encrypte

E test.docx
  Compatibility Level:
    Windows XP/Server 2003

  Users who can decrypt:
    WIN-98UTFANB55G\Bill Buchanan [Bill Buch
Buchanan@WIN-98UTFANB55G

    Certificate thumbprint: 1E77 C3D6 BCCB DFDD 1A82 352D B109
3136 A830 76E0

  No recovery certificate found.

  Key Information:
    Algorithm: AES
    Key Length: 256
    Key Entropy: 256
```



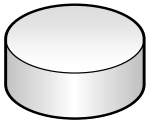


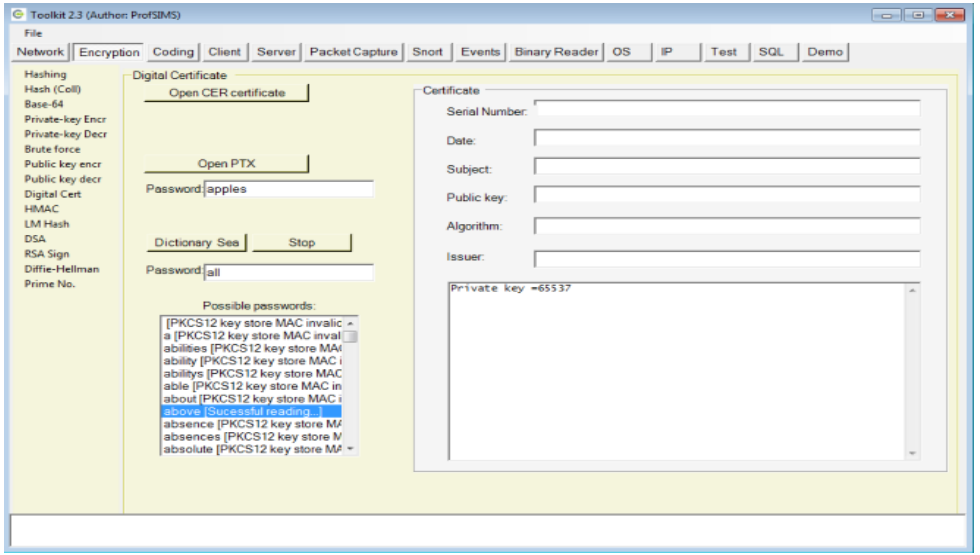
```
C:\enc\test>cipher /r:test.docx
Please type in the password to protect your .PFX file:
Please retype the password to confirm:

Your .CER file was created successfully.
Your .PFX file was created successfully.

C:\enc\test>dir
12-Oct-14  08:39 PM            11,432 test.docx
12-Oct-14  08:43 PM               912 test.docx.CER
12-Oct-14  08:43 PM             2,710 test.docx.PFX
```



PFX file

Dictionary attack





CER – Contains the certificate
PFX – Contains the certificate and private key

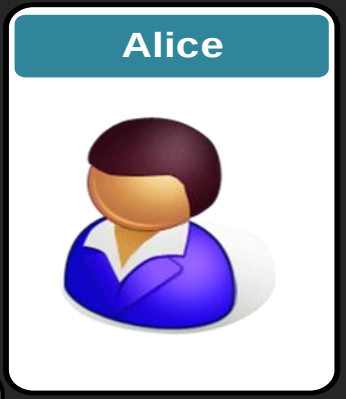
12-Oct-14 09:12 PM 11,437 test.docx
12-Oct-14 09:37 PM 912 test.docx.CER
12-Oct-14 09:37 PM 2,710 test.docx.PFX

Import PFX certificate

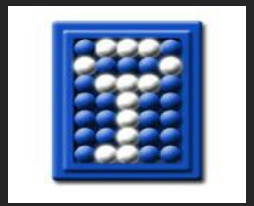
Author: Prof Bill Buchanan

Advanced Crypto

5. File Encryption and SSL debug



TrueCrypt

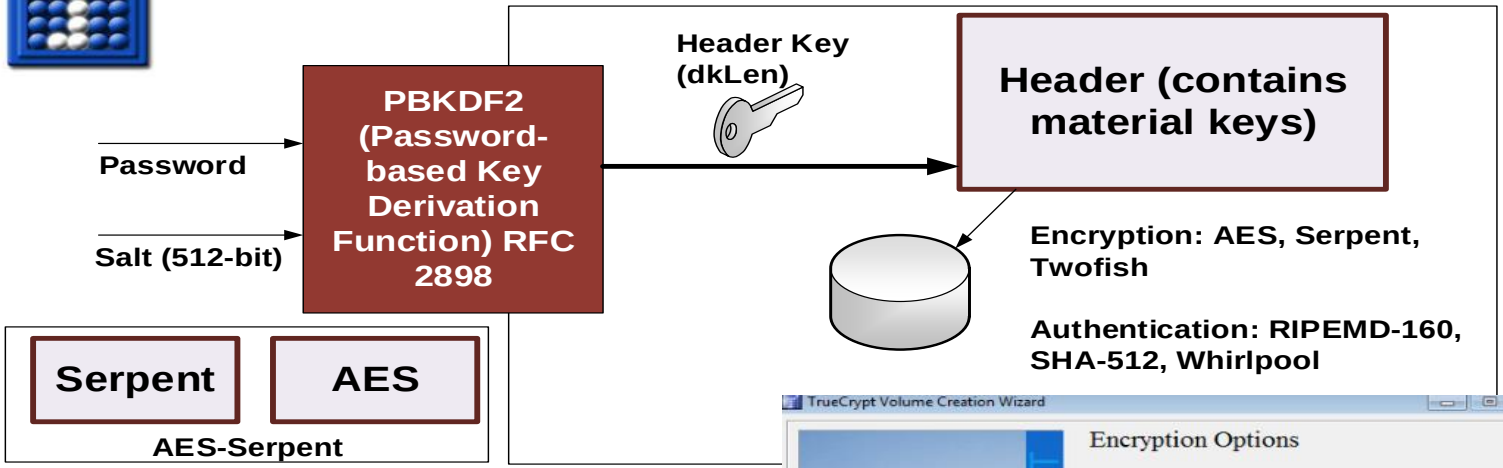


http://asecuritysite.com/crypto

Author: Prof Bill Buchanan

TrueCrypt

Advantages: Open-source. Windows/Linux/OS X. Free
Disadvantages: If you lose the pass phrase – almost impossible to recover. Current support is patchy.



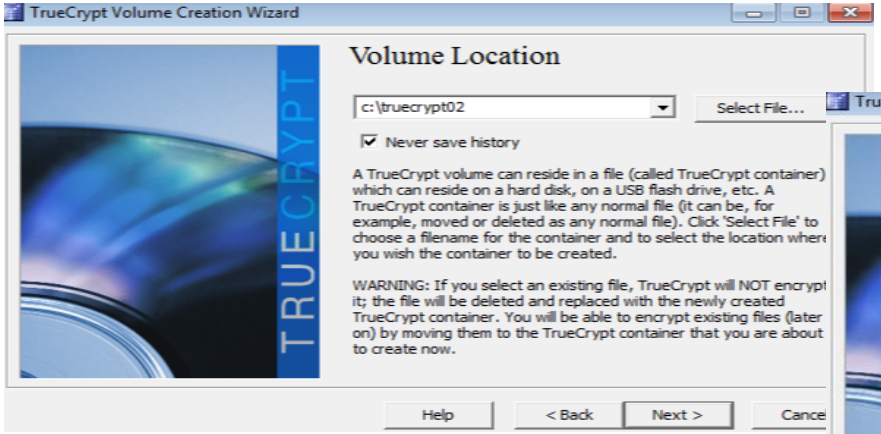
DK = PBKDF2(PRF, Password,Salt, c, dkLen)
DK = PBKDF2(HMAC-SHA1, passphase, ssid,4096,256)

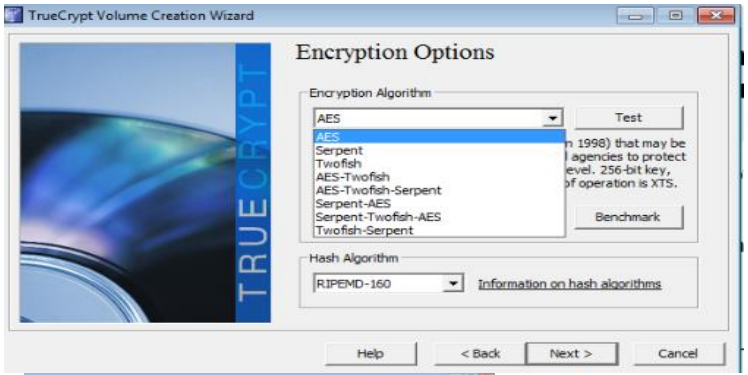
- **Serpent**. Ross Anderson et al. 1998. 256-bit key. 128-bit block (one of the AES finalists).
- **Twofish**. Bruce Schneier et all. 1998. 256-bit key. 128-bit block (one of the AES finalists).
- **AES**. FIPS-approved (Rijndael). 1998. 256-bit key. 128-bit block.

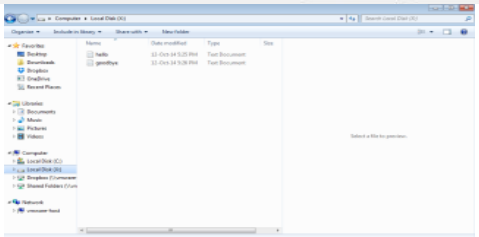
Author: Prof Bill Buchanan

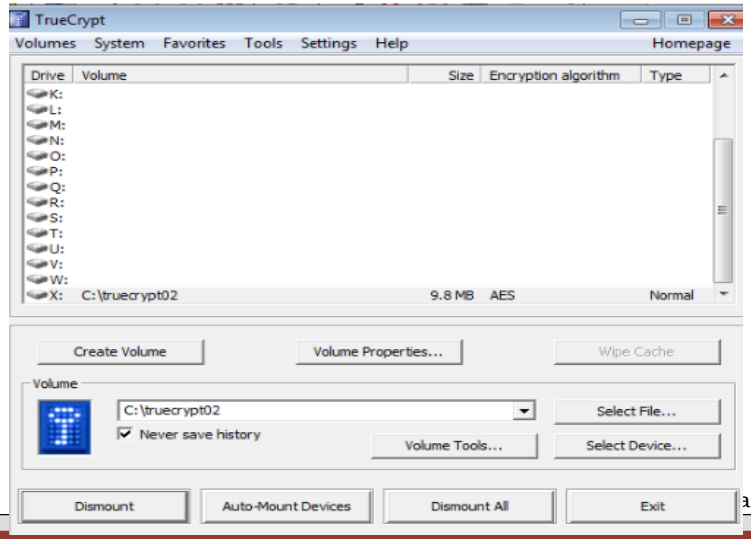
TC

Disk Encryption

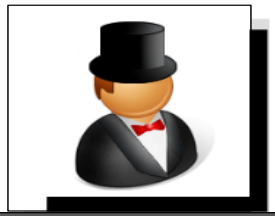








TrueCrypt



Bob

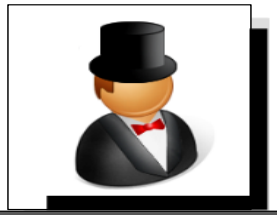
TrueCrypt is an open source disk cryptography package - February 2004 - TrueCrypt Foundation.

David Tesařík registered the TrueCrypt trademarking the US and Czech Republic, and Ondrej Tesarik registered the not-for-profit TrueCrypt company in the US.

Alice (Web)

Trent

Version 7.1a, there had been an audit on the code, with an announcement on 28 May 2014 that there was a discontinuation of TrueCrypt, along with the release of version of 7.2 (which was intentionally crippled and contained lots of warnings in the code). The updated licence (TrueCrypt License v 3.1) contained the removal of a specific language that required attribution of TrueCrypt.



Bob

WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues

This page exists only to help migrate existing data encrypted by TrueCrypt.

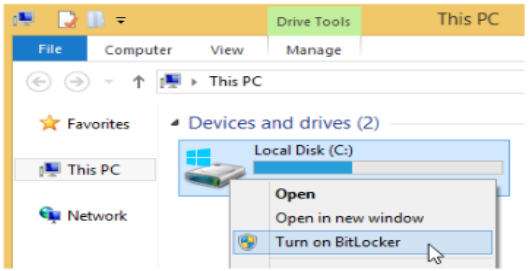
The development of TrueCrypt was ended in 5/2014 after Microsoft terminated support of Windows XP. Windows 8/7/Vista and later offer integrated support for encrypted disks and virtual disk images. Such integrated support is also available on other platforms (click here for more information). You should migrate any data encrypted by TrueCrypt to encrypted disks or virtual disk images supported on your platform.

Migrating from TrueCrypt to BitLocker:

If you have the system drive encrypted by TrueCrypt:

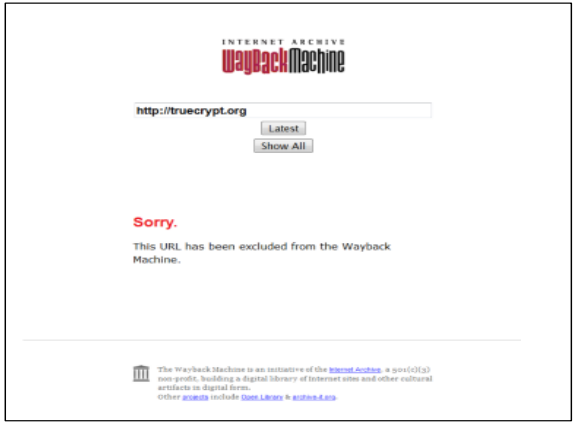
1. Decrypt the system drive (open **System** menu in TrueCrypt and select **Permanently Decrypt System Drive**). If you want to encrypt the drive by BitLocker before decryption, disable Trusted Platform Module first and do not decrypt the drive now.
2. Encrypt the system drive by BitLocker. Open the Explorer:

3. Click the drive C: (or any other drive where system encryption is or was used) using the right mouse button and select **Turn on BitLocker**:



Within the code, "U.S." has been changed to "United States", which could point to an automated search and replace method of changing the code to reflect a possible change of ownership of the code

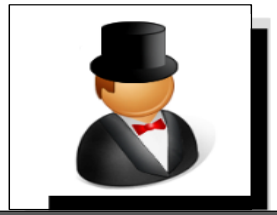
Novice Web page. Very poor layout of message.



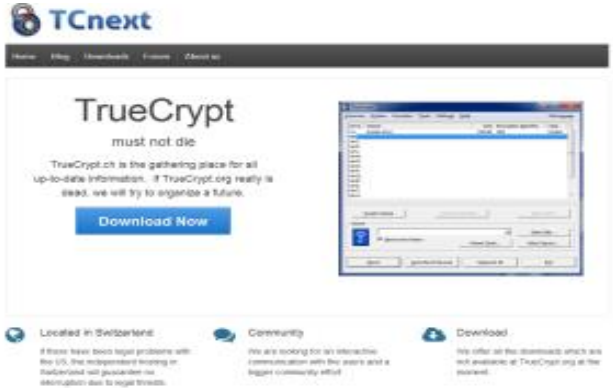
Code bug? Generation of a pseudo random number, randomly use the time between key strokes for users.

Binary code exploit? Binary distribution could have been modified.

TrueCrypt mystery



Bob



Alice (Web)

Trent

Truecrypt.ch

TrueCrypt must not die

TrueCrypt.ch is the gathering place for all up-to-date information. If TrueCrypt.org really is dead, we will try to organize a future.

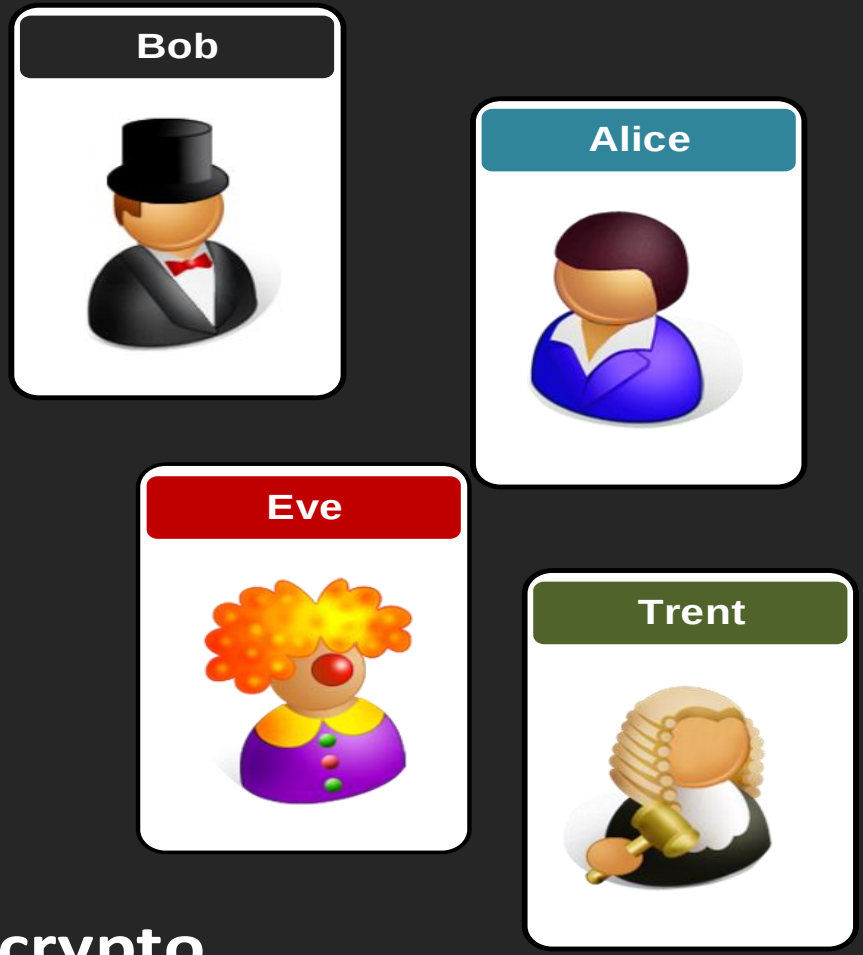
@TrueCryptNext

Where next?

Advanced Crypto

5. Disk Encryption

Detecting Encryption/ Compression



http://asecuritysite.com/crypto

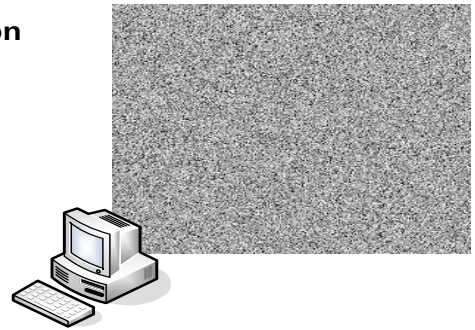
Author: Prof Bill Buchanan

File Compression

PKZIP: 50 4B 03 04 [PK]
GZIP: 1F 8B 08
Tar: 75 73 74 61 72
Zlib: 78 01, 78 9C or 78 DA

```
[00000000] 50 4B 03 04 14 00 02 00 08 00 80 9D 6C 39 DA 4D   PK..........l9.M
[00000016] B8 0F 90 01 00 00 27 06 00 00 09 00 00 00 61 6E   ......'.......an
[00000032] 69 6D 2E 78 61 6D 6C ED 54 D1 4E 83 30 14 7D 37   im.xaml.T.N.0.}7
[00000048] F1 1F 9A 7E 00 C5 69 4C 24 B0 C4 CD A9 0F 6A 96   ...~..iL$.....j.
[00000064] 8D 64 CF 15 EE A0 B1 B4 A4 2D 8A 7F 6F 2D 6C 63   .d.......-..o-lc
[00000080] CA 14 13 1F 7C 90 A7 02 E7 9C 7B EF 39 E9 0D 57   ....|.....{.9..W
[00000096] 4C A4 F2 05 D5 C1 94 53 AD 23 BC 2A D7 97 65 C9   L......S.#.*..e.
```

File Encryption

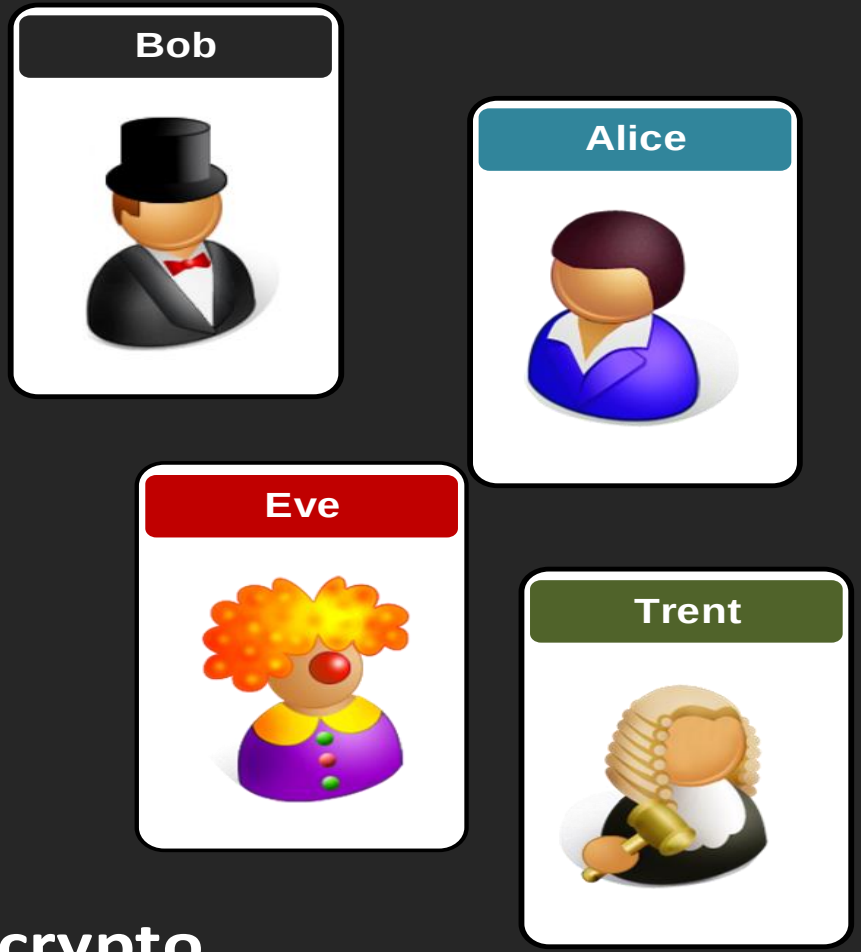


```
47 c3 dd 4e 94 15 ce af 76 d6 94 9d 5d 82 88 99
34 d3 db 0d e4 ae af 57 e3 87 62 fd 14 7e f5 7d
02 7a 67 40 2b 2c 71 41 24 92 9d 54 1c 75 bb 54
0b f8 95 a9 92 d7 33 ad 2f 00 cb 8c 9f 90 66 49
b2 bd 0f 90 52 e3 aa 0a 59 6b 78 65 1f 5b 35 19
0f e3 32 ed c3 f0 04 88 67 51 33 cb 03 40 9f 3b
```

Author: Prof Bill Buchanan

Advanced Crypto

5. Disk Encryption



http://asecuritysite.com/crypto

Author: Prof Bill Buchanan