John Steele

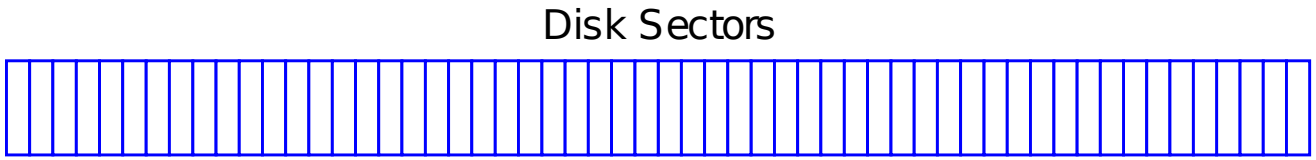
Securing your data

Introduction

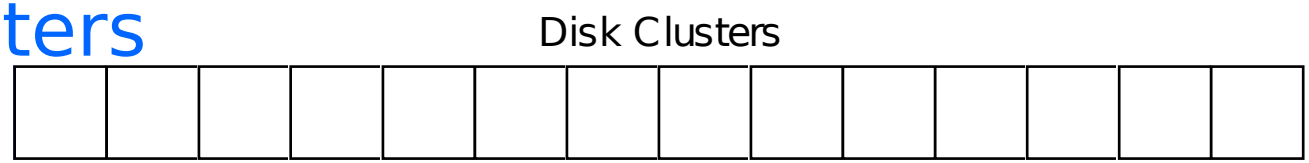
- Topical subject!
  - HMRC loss of disk in post
  - MoD theft of laptop from car
  - To name but two cases
- Protection of data on your computer
  - Data at rest
- Protection of data in transit
  - To your bank etc.

Files on Disk

- Disk are organised in Sectors

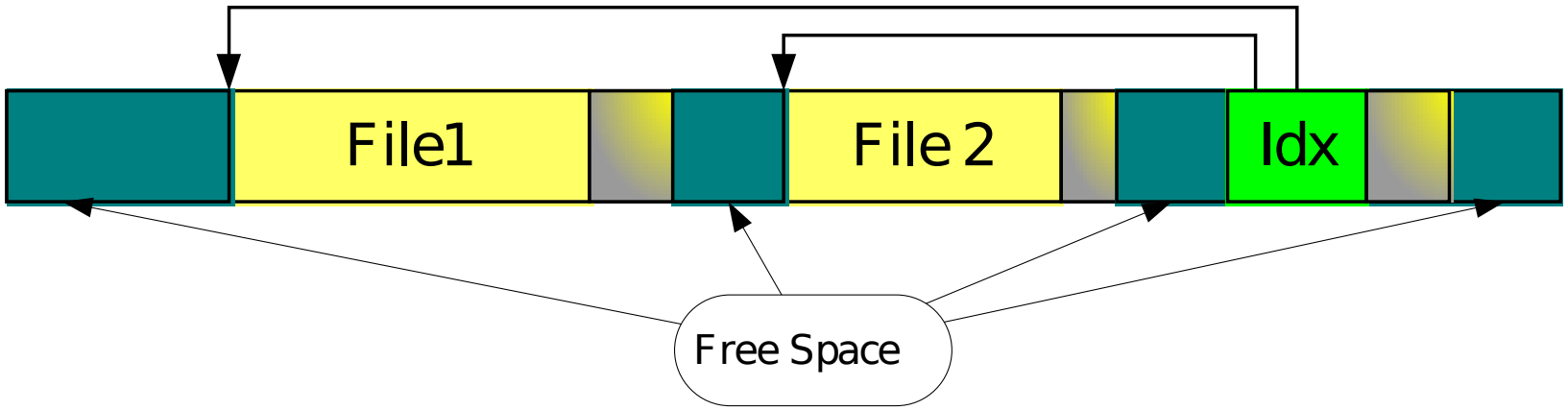


- Sectors are grouped together in Clusters



- Data is allocated in clusters

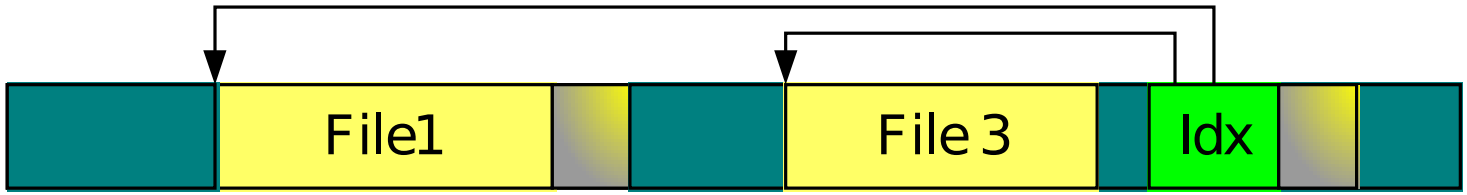
File Organisation



Delete a File

Deleting Files

- What happens when you delete a file?
- Is it recoverable?
  - UNDELETE
  - Can find bits of files and put them back together again
    - Unless parts have been overwritten



What can we do?

- Windows delete moves file to recycle bin, does not actually delete the file
- Eraser
  - Freeware (or course)
- Erase files multiple overwrites
- Erases Cluster tips
- Erases free space

Encryption

- Encryption is the means of protection
- Symmetric Encryption
  - Requires an encryption key and an agreed method of using it
  - Key is used to encrypt and decrypt
  - Been used in one form or another for centuries
- Electronic encryption examples
  - DES, 3*DES, AES

Protection of data on disk

- Disk can be
  - hard disk
  - CD/DVD
  - USB
- Encryption
  - Data is “scrambled” so it can’t be read unless you have the “key”

Key issues

- The encryption “key” needs to be known by all parties
- OK if you are encryption data locally
- But difficult if you are exchanging data with another party
  - Can you trust the delivery method
  - Can you be sure there is not another copy
  - Personal swap of keys

Characteristics Required

- Method used to scramble date must not have any weaknesses
- Key length must be sufficient to defeat a brute force attack
  - DES used 56 bit keys and no longer passes this test for maximum security
- Must not have a “back door”
  - DES is rumoured to have one but this has never been proved

Encryption Concept

plaintext	t	h	e		q	u	i	c	k		b	r	o	w	n	
key	d	e	m	o	d	e	m	o	d	e	m	o	d	e	m	o
Convert plaintext and key to character codes																
plaintext #	84	72	69	32	81	85	73	67	75	32	66	82	79	87	78	32
key #	68	69	77	79	68	69	77	79	68	69	77	79	68	69	77	79
Subtract 32 from each character in plainext and key, add them together take remainer of sum / 64 Add 32 to convert back to a character																
cipher text #	56	45	50	79	53	58	54	50	47	69	47	65	51	60	59	79
Convert number back to character																
cypher text	8	-	2	O	5	:	6	2	/	E	/	A	3	<	;	O

Decrypt Concept

cypher text	8	-	2	O	5	:	6	2	/	E	/	A	3	<	;	O
key	d	e	m	o	d	e	m	o	d	e	m	o	d	e	m	o
Convert ciphertext and key to character codes																
cipher text #	56	45	50	79	53	58	54	50	47	69	47	65	51	60	59	79
key #	68	69	77	79	68	69	77	79	68	69	77	79	68	69	77	79
Subtract 32 from each character in plainext and key, subtract key from ciphertext take remainer of result / 64 Add 32 to convert back to a character																
plaintext #	84	72	69	32	81	85	73	67	75	32	66	82	79	87	78	32
plaintext	T	H	E		Q	U	I	C	K		B	R	O	W	N	

Product for Disk Encryption

- Truecrypt
  - Freeware
- Create a file (as big as you like)
- Initialise encryption
- Mount file in Truecrypt
- Appears as a new Disk Drive letter
  - Can be used as any other disk drive
  - All data within it is scrambled

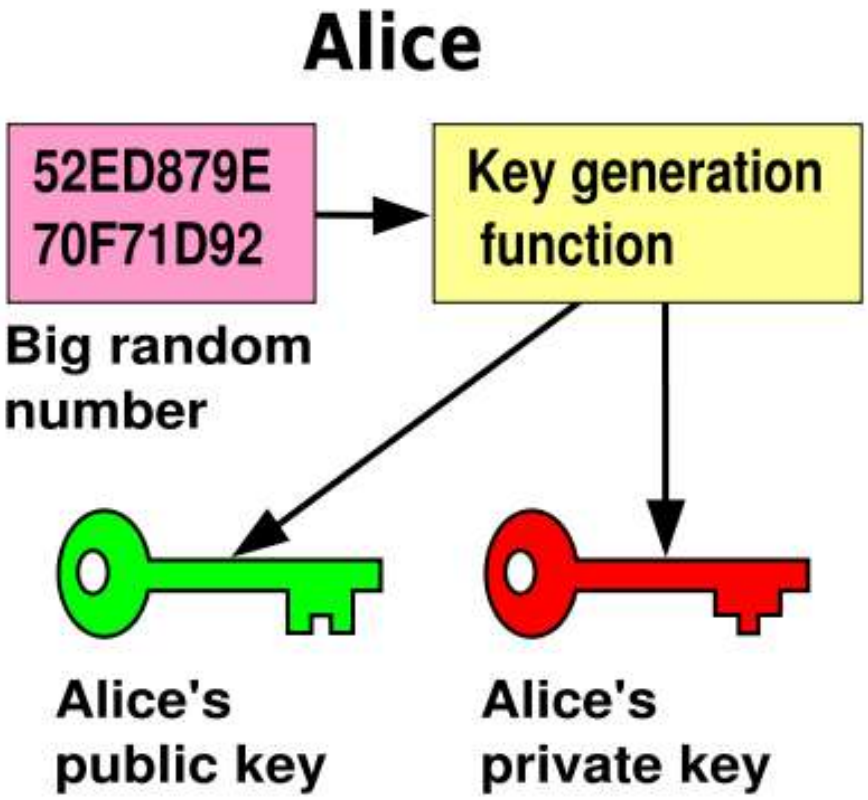
Whole disk encryption

- Professional end of market
  - No freeware as far as I am aware
  - Pointsec
    - Decrypts data on bootup if on same computer
  - Becrypt
    - Special username and two passwords before you van boot machine!
  - Flagstone
    - Encryption in disk drive
  - BitLocker
    - New Microsoft encryption – Vista (Enterprise)/Server 2008

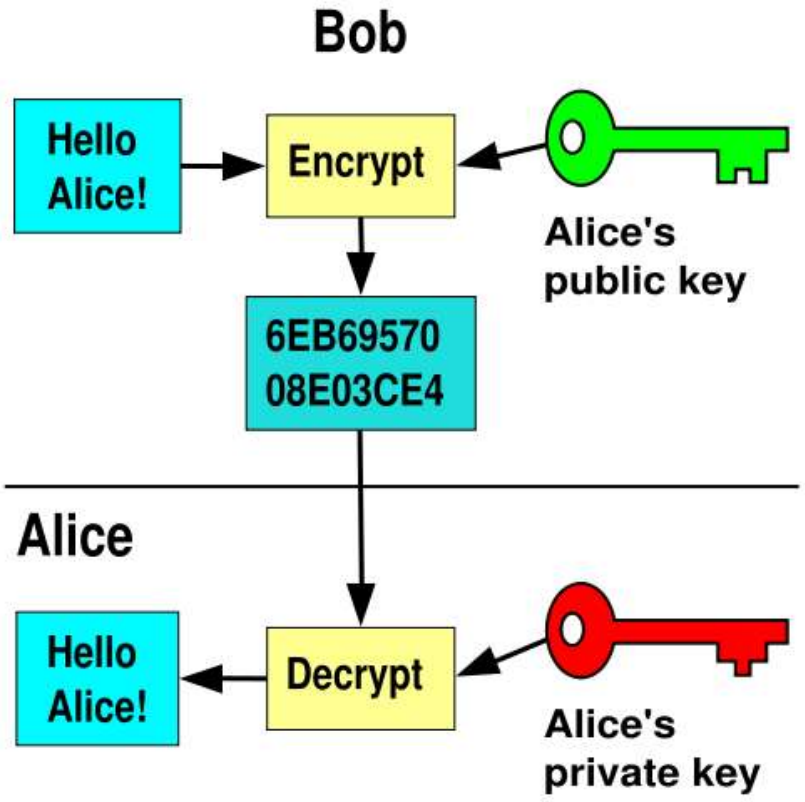
Data over the Internet

- Encryption is GOOD for privacy
- How do you transfer the crypto key to the other party?
- You could meet
  - Not always feasible
- You could email it
  - It could be intercepted!
  - Could lead to a “man in the middle” interception

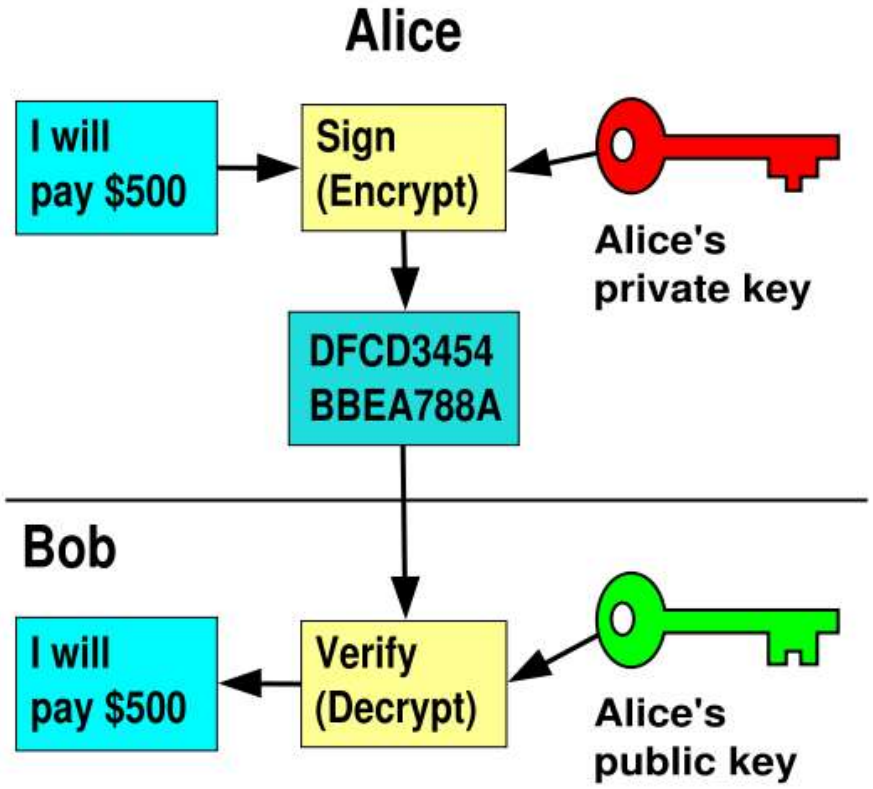
Public Key Principle



Encrypt with Public key



Sign with Private Key



Secure Internet Browsing

- Based on Public Key encryption
- Connect to a Server
- It sends a “certificate”
  - Public Key plus
    - Validity date
    - Certificate authority
      - You can check (click the padlock)
- Certificates can be stored
- Certificates can be revoked

What happens next?

- Client has a certificate from server – Public Key
  - Client encrypts a random number with server's Public Key
  - Sends to Server
  - Server decrypts with Private Key
  - Both ends generate a Session Key from this random number
  - Session continues using symmetric encryption

In Practice

- Public Key encryption takes a lot of processing power
  - Asymmetric Encryption
- Used to send a Session Key for a Symmetric Encryption algorithm
  - DES
  - Triple DES
  - AES

Making a hash of it

- An alternative way of making a key for a symmetric algorithm is a Hash function
- Takes a “pass phrase” and converts it to a number
  - Non reversible
    - MD5
    - SHA
- Pass phrase is “hashed” and the result used as symmetric encryption key

Email Encryption

- Uses Public key of recipient to encrypt message
- Recipient uses their private key to decrypt message
- Signing a message uses senders private key to encrypt a digest (hash) of message
- Recipient decrypts hash with public key and checks the hash value by re-computing it

Practical implementations

- PGP – Pretty Good Privacy
  - Was public domain
  - Caused a furore in the USA when it was exported
  - Writer (Phil Zimmermann) was threatened with prison!
    - Export of high grade encryption from USA was illegal

How was it exported

- Source code printed in a book
  - Export of book was legal – protected under the “first amendment”
  - Recipients scanned and OCR the code
  - Recompile
  - You now had PGP
- Second version was sent electronically to Canada (legal)
- Sent to a server in Sweden (also legal)

What has happened since

- PGP went commercial from being open source and still exists
- There is now an OpenPGP
- And GPG which fully implements the standard and is fully open source
- Available in most version of UNIX/Linux

Products

- Crypto Anywhere (OpenPGP)
  - Outlook Express plugin
    - http://www.bytefusion.com/products/ens/cryptoanywhere/microsoftoutlookexpressplug.htm
- Enigmail (GPG derivative)
  - Thunderbird
    - https://enigmail.mozdev.org/documentation/gpgsetup.php
- Neither tested by me (yet)

And finally

- Encrypting files or folders
  - Finecrypt
    - http://www.freedownloadscenter.com/Utilities/File_Encryption_Utilities/FineCrypt.html
      - (not the supplier's site – not accessible when I tried it)
  - Free version of professional package
  - Creates a self extracting executable if required
    - so does not need software on recipient
    - assuming that executable not blocked by recipient as email!