SECURITY WITH PLYMOUTH UNIVERSITY

Technology & Information Services

SEC-GDL-007 - Document Encryption

Author:	Paul Ferrier
Date:	02/07/2015
Document Security Level:	**PUBLIC**
Document Version:	1.0
Document Ref:	SEC-GDL-007
Document Link:	
Review Date:	01/06/2016

Document Control

Version	Author	Position	Details	Date/Time	Approved by	Position	Date/Time
1.0	Paul Ferrier	Enterprise Security Architect	Created the document	30/06/2015 12:30	tbc	tbc	tbc
1.1	PF	ESA	Amendments following comments from BPs, EA, TAs and DPO	02/07/2015 13:30			

Contents

SEC-GDL-007 - Document Encryption

1. Introduction

Encryption in terms of documents, relates to password protection; to open (for reading or editing) an encrypted document you must be able to provide this password.

There are two options for encrypting documents and these are:

- File level encryption for individual documents or spreadsheets
- Folder, or multiple file encryption for groups of documents or spreadsheets

Information or data that is **restricted** (including commercial in confidence, as denoted by the Data Classification Policy[1]) must be encrypted before being communicated to another party either within or outside of the University. Email is inherently insecure; not only once you have sent it to a recipient you lose control of the communication – you cannot prevent forwarding to other parties for example, email very rarely goes directly to the recipients mailbox, it will likely be processed by a number of mail servers to transport the message to a target mailbox (email is like sending a postcard as opposed to a sealed envelope); communicating information that risks the University or individuals to lose material (including Intellectual Property (IP)) and personal or sensitive personal data (as defined within the Data Protection Act 1998[2]); encrypting this information means if it falls into the wrong hands it is not accessible unless the password can be broken.

Microsoft Office has the ability to encrypt documents this is detailed in the next section. Groups of files or folders can be encrypted using 7-Zip this is detailed further in the guidelines.

This document covers the software for Windows computers that are available to staff and students.

In summary

If sending information by email which contains restricted information the process is as follows:

1. Encrypt the document/folder with a password following the instructions in section **3. File Encryption**
2. Attach to an email and send ensuring the addressee is correct
3. Provide the password to the recipient verbally or by text message

2. Important Information

There are three really important points that need to understand around encrypting documents:

1. When a document or file is encrypted with a password, if you forget the password the contents of the file or folder cannot be retrieved.
2. It is extremely important to provide the password to the recipient via a different communication method than how the files are sent. If the same method is used, for example, you email the documents and send an additional email with the password, should that email be compromised you are providing the padlock and the key to any malicious user for access.
3. Strong password creation is a skill that can be difficult to learn. There are however many tips available such as: http://www.howtogeek.com/195430/how-to-create-a-strong-password-and-

[1] EIM-POL-001 Data Classification Policy
[2] Information Commissioner's Officer - Data Protection Act, Key Definitions

remember-it/ and tools for generating and remembering strong passwords for you for example Random Generator[3], please refer to section **6. Password Generation** if you require more information about this.

[3] Random Password Generator (www.random.org/passwords)

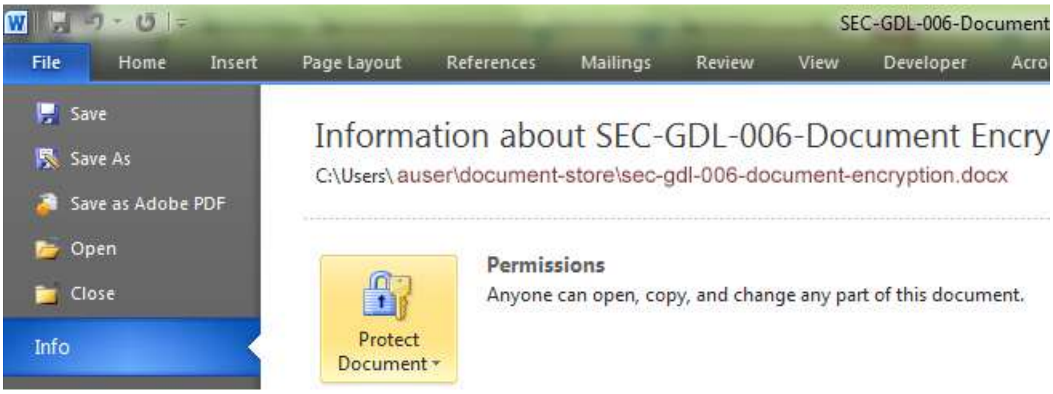
3. File Encryption

Encrypting Microsoft Office documents is very simple, the following section covers the how to perform this action on a number of different varieties of Microsoft Office suite.

In the Office 2010 suite, 3.2 Microsoft Excel, 3.3 Microsoft PowerPoint and Microsoft Word have the ability to Protect Documents in a number of different ways, Microsoft Visio does not support encryption.

3.1 Microsoft Word 2010

1.



Information about SEC-GDL-006-Document Encry

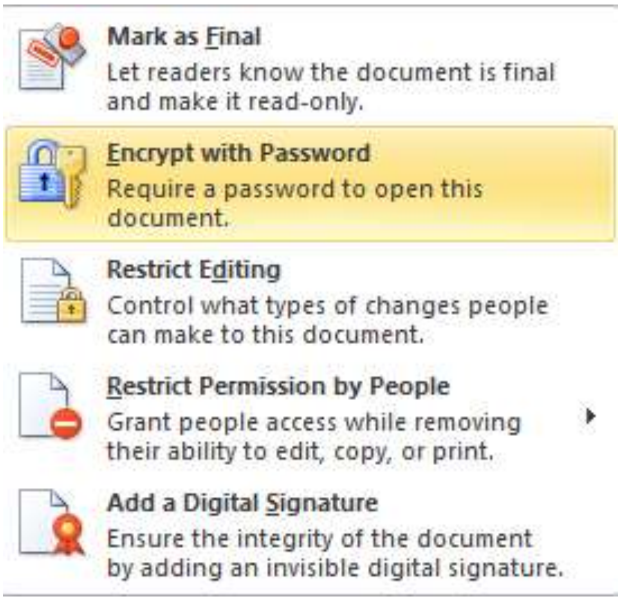
C:\Users\ auser\document-store\sec-gdl-006-document-encryption.docx

Permissions

Anyone can open, copy, and change any part of this document.

Navigate to the File Menu and select the Info option. This will then show additional information click the Protect Document button, to reveal a selection of options to secure your document.

2.



Mark as Final: Let readers know the document is final and make it read-only.

Encrypt with Password: Require a password to open this document.

Restrict Editing: Control what types of changes people can make to this document.

Restrict Permission by People: Grant people access while removing their ability to edit, copy, or print.

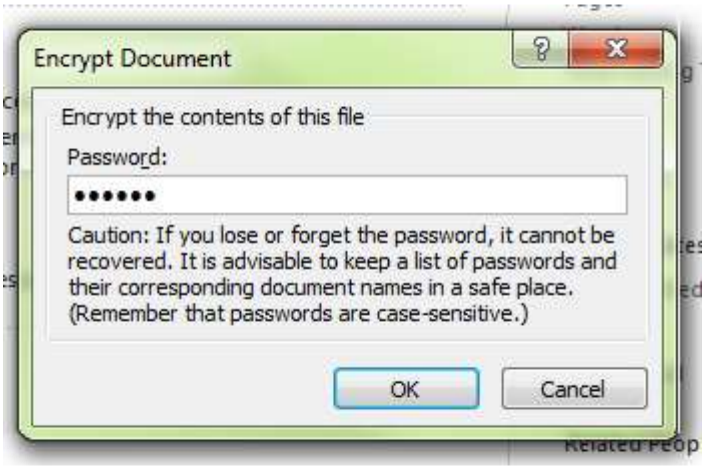
Add a Digital Signature: Ensure the integrity of the document by adding an invisible digital signature.

The options that are provided allow various restrictions on the editing or protection of the document.

This guideline document is solely concerned with the encryption of information with the use of passwords.

Select Encrypt with Password.

3.



Encrypt Document

Encrypt the contents of this file

Password:

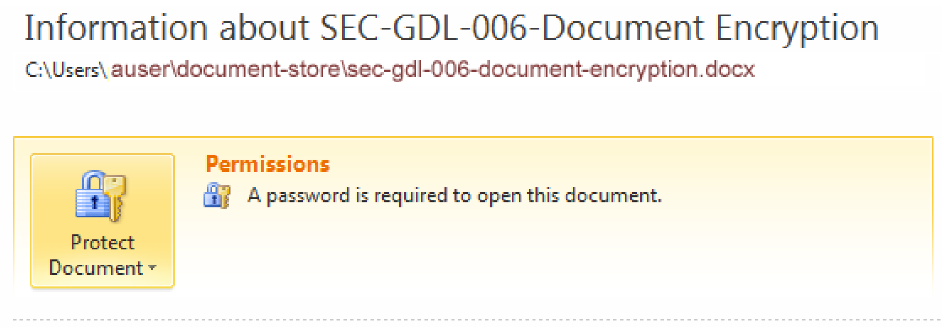
••••••

Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)

You are then presented with the ability to add a password. It is recommended that the strength of the password is appropriate to the information it is protecting.
For example, a document detailing business in confidence information would benefit from a robust password that is not found in a dictionary.

This password is case sensitive and without it the document can’t be accessed.

4.



Information about SEC-GDL-006-Document Encryption

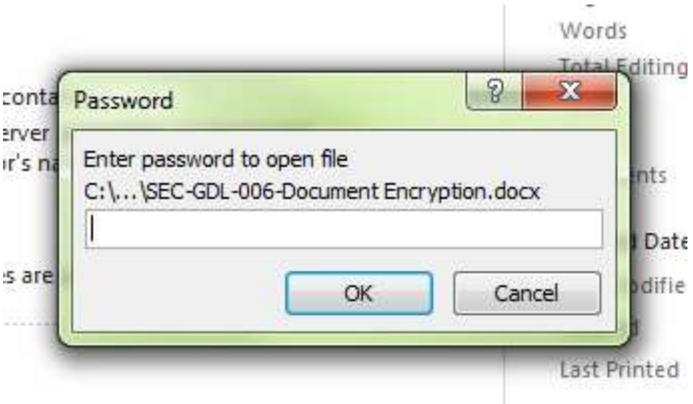
C:\Users\auser\document-store\sec-gdl-006-document-encryption.docx

Permissions

A password is required to open this document.

When the password has been provided and re-entered to ensure accuracy, you are returned to the protect document screen with confirmation that a password must be provided to open the document.

5.



Password

Enter password to open file

C:\...\SEC-GDL-006-Document Encryption.docx

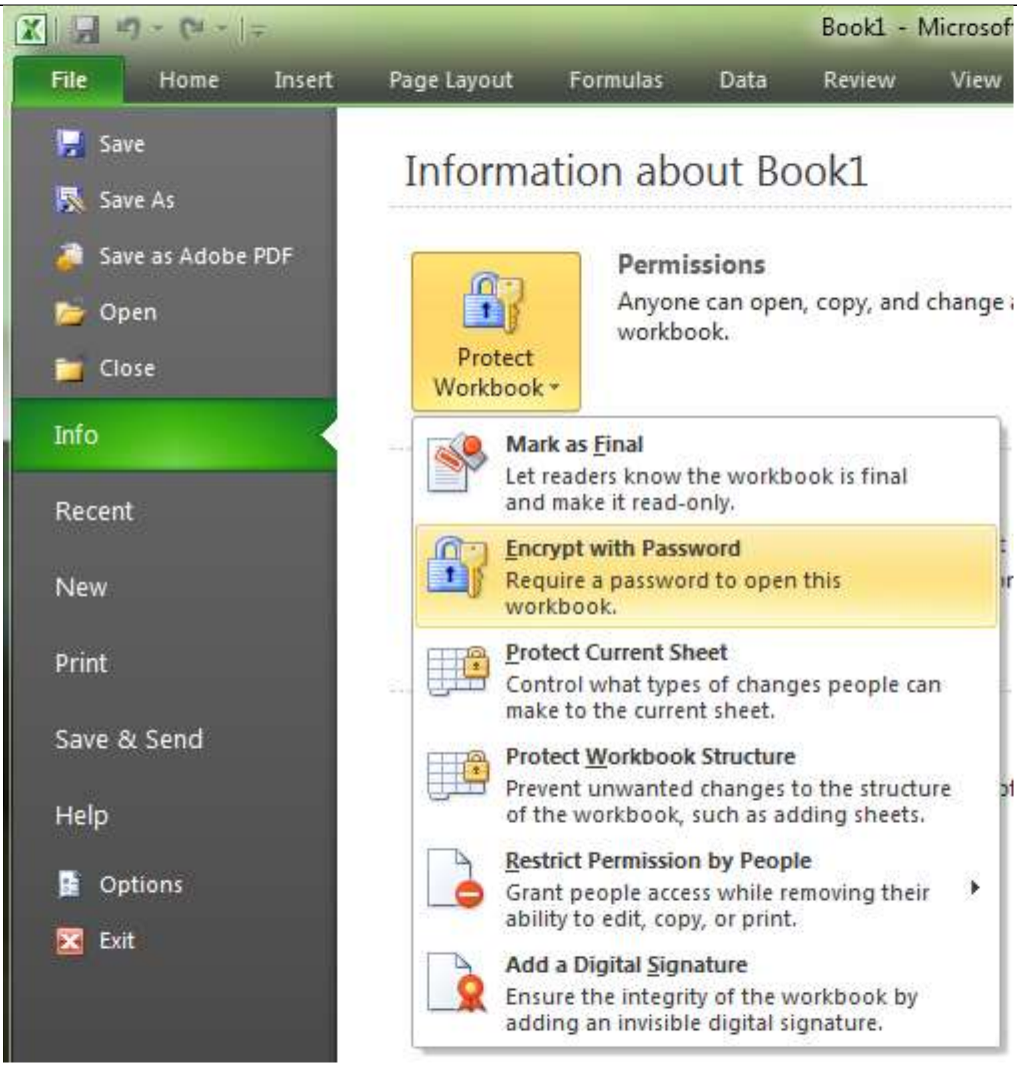
Whenever the document is accessed, you will need to re-enter the password before it will open.

6. After the document has been sent, you can remove the password from the originating document by following steps 1 and 2 and entering a blank (no content) password.

7. For the sending of the document, please refer to section **5.Common Steps Surrounding Communication**.

3.2 Microsoft Excel 2010

1.



Information about Book1

Permissions

Anyone can open, copy, and change a workbook.

Mark as Final
Let readers know the workbook is final and make it read-only.

Encrypt with Password
Require a password to open this workbook.

Protect Current Sheet
Control what types of changes people can make to the current sheet.

Protect Workbook Structure
Prevent unwanted changes to the structure of the workbook, such as adding sheets.

Restrict Permission by People
Grant people access while removing their ability to edit, copy, or print.

Add a Digital Signature
Ensure the integrity of the workbook by adding an invisible digital signature.

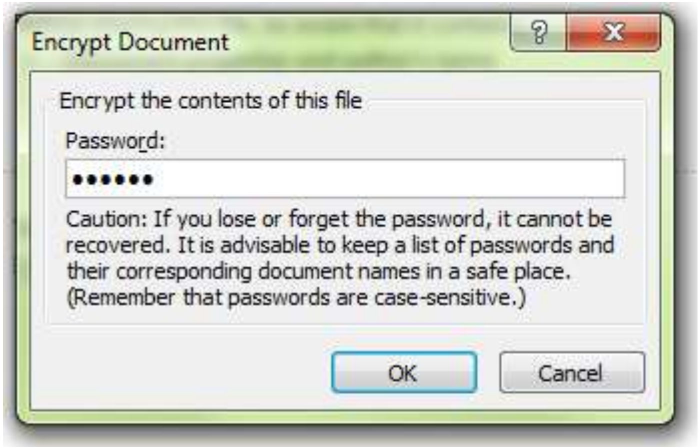
To password protect in Excel, select File, then Info and then Protect Workbook.

Slightly more controls are provided in Excel to protect documents; as restrictions can be placed on the editing of worksheets as well as the entire workbook itself.

This document only deals with the Encryption with Passwords.

Select Encrypt with Password.

2.



Encrypt Document

Encrypt the contents of this file

Password:

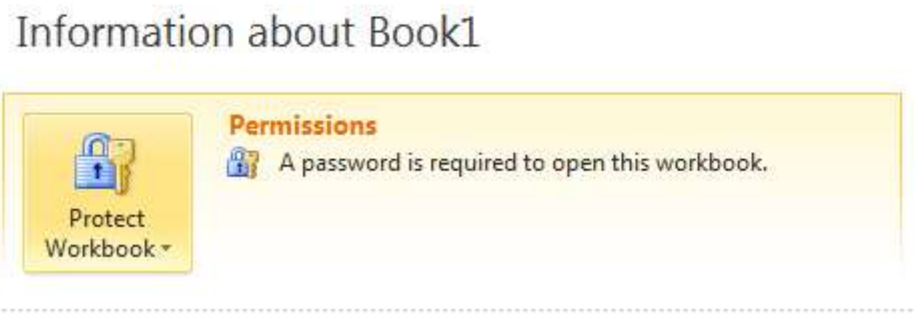
••••••

Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)

You are required to provide a password. You must consider the strength of the password being used to protect the information contained within the spreadsheet or workbook.

This password is case sensitive and without it the document can't be accessed.

3.

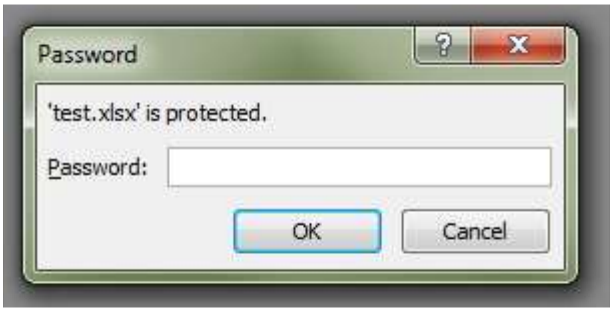


Information about Book1

Permissions

A password is required to open this workbook.

When the password has been entered twice your Excel document is now protected.

4. 

'test.xlsx' is protected.

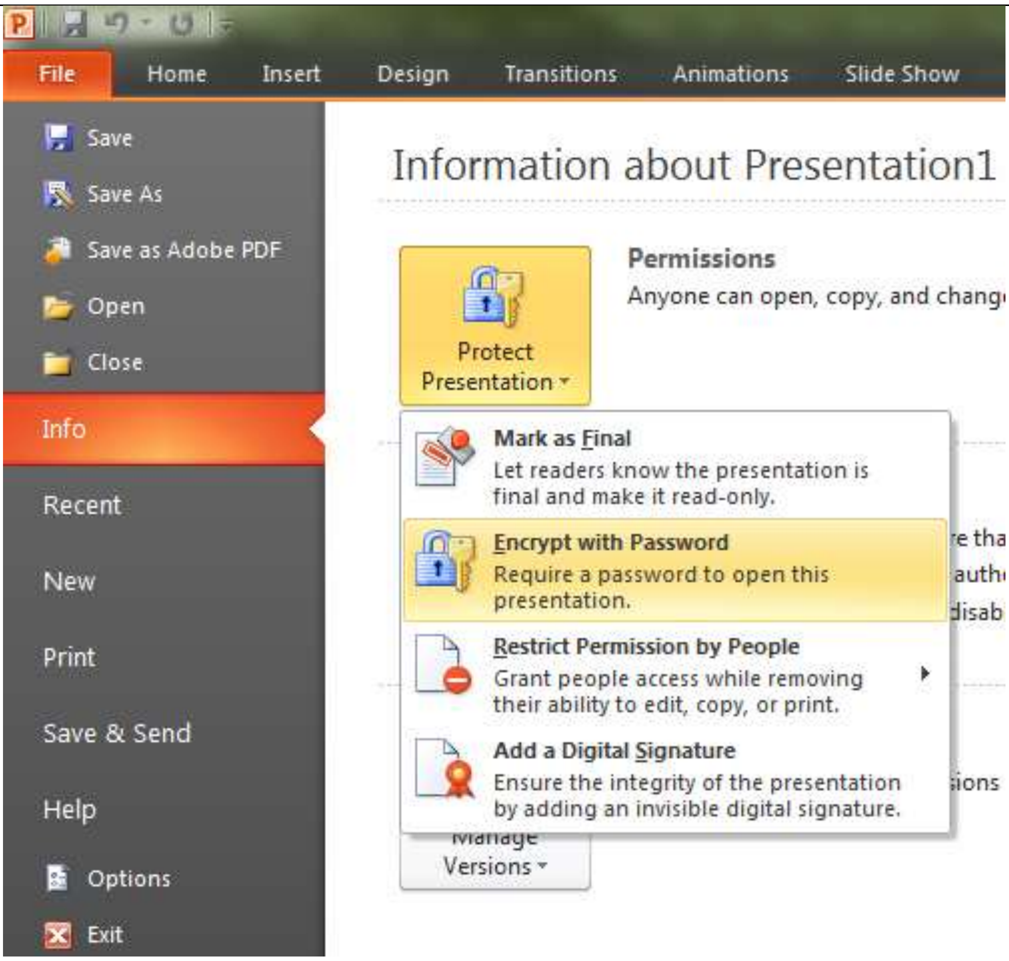
Password:

Whenever the workbook or worksheet is accessed you will need to re-enter the password before it will open.

5. After the document has been sent, you can remove the password from the originating document by following steps 1 and 2 and entering a blank (no content) password.

6. For the sending of the document, please refer to section **5. Common Steps Surrounding Communication**.

3.3 Microsoft PowerPoint 2010

1. 

Information about Presentation1

Permissions

Anyone can open, copy, and chang

Mark as Final

Let readers know the presentation is final and make it read-only.

Encrypt with Password

Require a password to open this presentation.

Restrict Permission by People

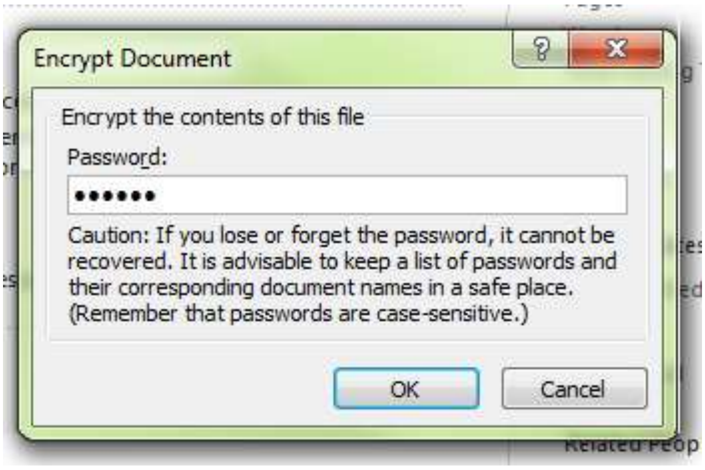
Grant people access while removing their ability to edit, copy, or print.

Add a Digital Signature

Ensure the integrity of the presentation by adding an invisible digital signature.

Once the document is ready to be secured, this can be accessed via the File Menu and the Info item. The Protect Presentation drop down will allow the Encrypt with Password option to be selected.

2.



Encrypt Document

Encrypt the contents of this file

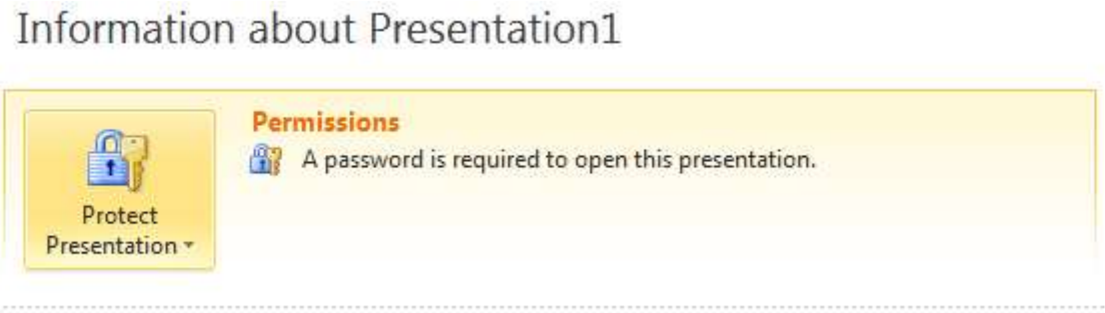
Password:

••••••

Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)

To protect the document you are required to provide and confirm a password.

3.



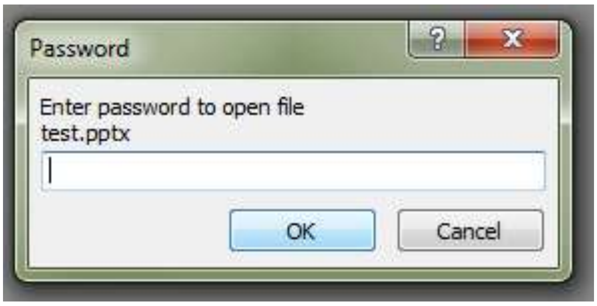
Information about Presentation1

Permissions

A password is required to open this presentation.

The PowerPoint presentation is now secured.

4.



Password

Enter password to open file test.pptx

The recipient will be required to enter the password to access the materials.

This password is case sensitive and without it the document can’t be accessed.

5. After the document has been sent, you can remove the password from the originating document by following steps 1 and 2 and entering a blank (no content) password.

6. For the sending of the document, please refer to section **5. Common Steps Surrounding Communication**.

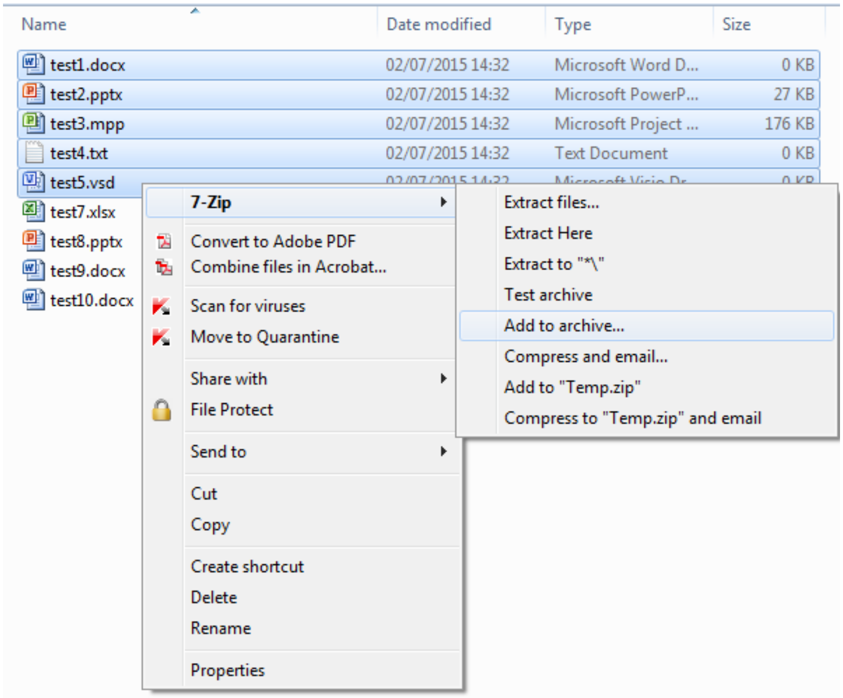
4. Multiple File or Folder Information

This section covers how to password protect (encrypt) groups of documents or entire folders.

4.1 7-Zip

7-Zip is installed on University managed computers, including the staff and student windows computers. It is a very lightweight and is used to compress files for transmission or storage.

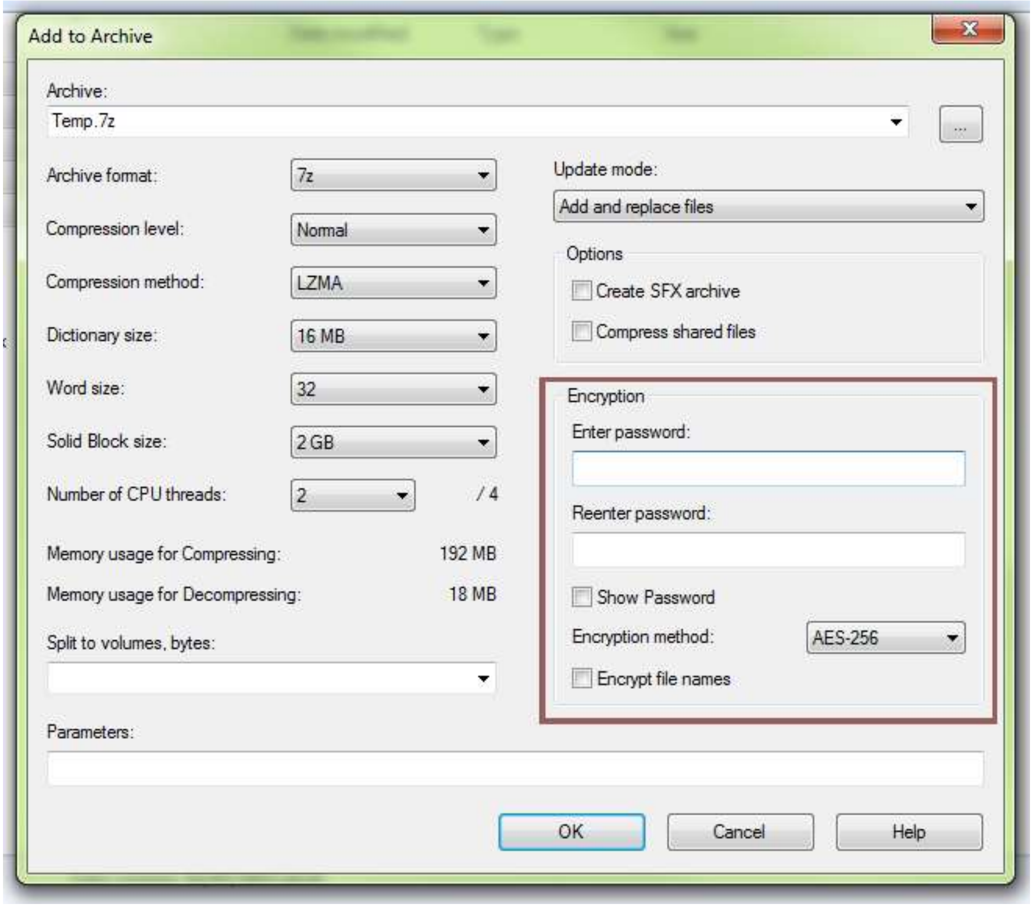
1\.



Name	Date modified	Type	Size
test1.docx	02/07/2015 14:32	Microsoft Word D...	0 KB
test2.pptx	02/07/2015 14:32	Microsoft PowerP...	27 KB
test3.mpp	02/07/2015 14:32	Microsoft Project ...	176 KB
test4.txt	02/07/2015 14:32	Text Document	0 KB
test5.vsd	02/07/2015 14:32	Microsoft Visio Dr...	0 KB
test7.xlsx			
test8.pptx			
test9.docx			
test10.docx			

Select the file(s) and/or folder(s) that you want to protect. Right click on one of the highlighted files and select 7-Zip and then Add to archive.

2\.



Add to Archive

Archive: Temp.7z

Archive format: 7z

Compression level: Normal

Compression method: LZMA

Dictionary size: 16 MB

Word size: 32

Solid Block size: 2 GB

Number of CPU threads: 2 / 4

Memory usage for Compressing: 192 MB

Memory usage for Decompressing: 18 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Options

□ Create SFX archive

□ Compress shared files

Encryption

Enter password:

Reenter password:

□ Show Password

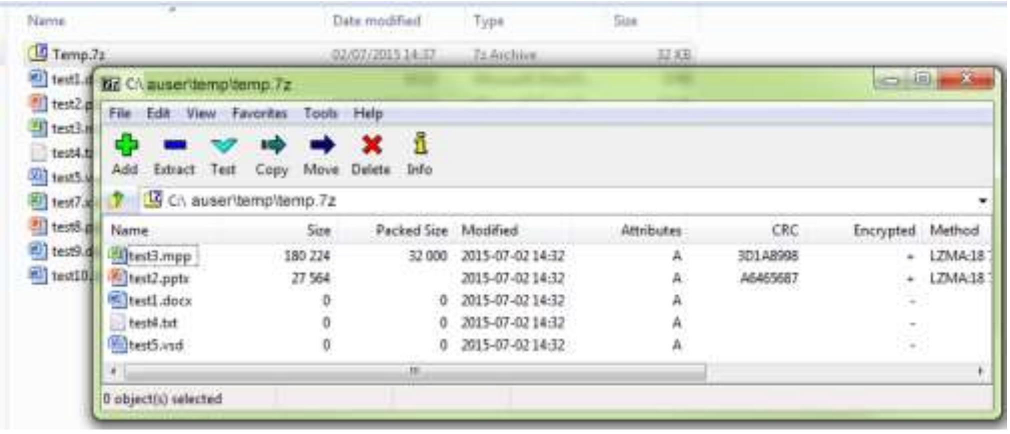
Encryption method: AES-256

□ Encrypt file names

7-Zip then opens to show a number of options that are available, the Encryption section has been highlighted.

Once you have a provided a password appropriate to the files or folders being protected you can also Encypt file names. This prevents the files being displayed when the zip file is opened. If this box is checked, move to point 4.

3.



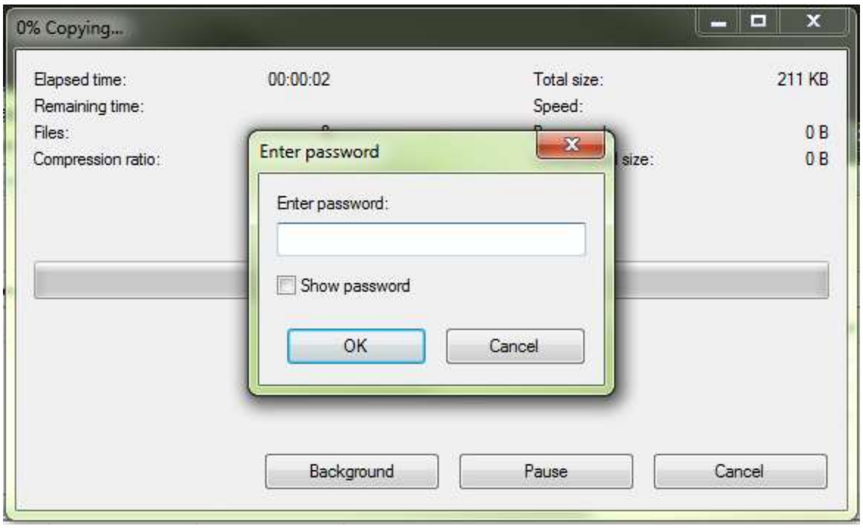
C:\ auser\temp\temp.7z

Name	Size	Packed Size	Modified	Attributes	CRC	Encrypted	Method
test3.mpp	180 224	32 000	2015-07-02 14:32	A	3D1A8998	+	LZMA:18
test2.pptx	27 564		2015-07-02 14:32	A	A6465687	+	LZMA:18
test1.docx	0	0	2015-07-02 14:32	A		-	
test4.txt	0	0	2015-07-02 14:32	A		-	
test5.vsd	0	0	2015-07-02 14:32	A		-	

0 object(s) selected

The files are compressed and then presented, for additional files to be added or removed etc.

4.



0% Copying...

Elapsed time: 00:00:02
Remaining time:
Files:
Compression ratio:
Total size: 211 KB
Speed:
0 B
size: 0 B

Enter password

Enter password:

□ Show password

When the recipient tries to open the zip file they are prompted to provide the password before access is granted.

5. This compressed file is now ready for communicating.

5. Common Steps Surrounding Communication

Now the documents, files or folders are ready to send to the recipient. **Do not send the document and password using the same form of communication.** If you send the document via email for example, you might wish to consider ringing through or sending a text message containing the password.

6. Password Generation

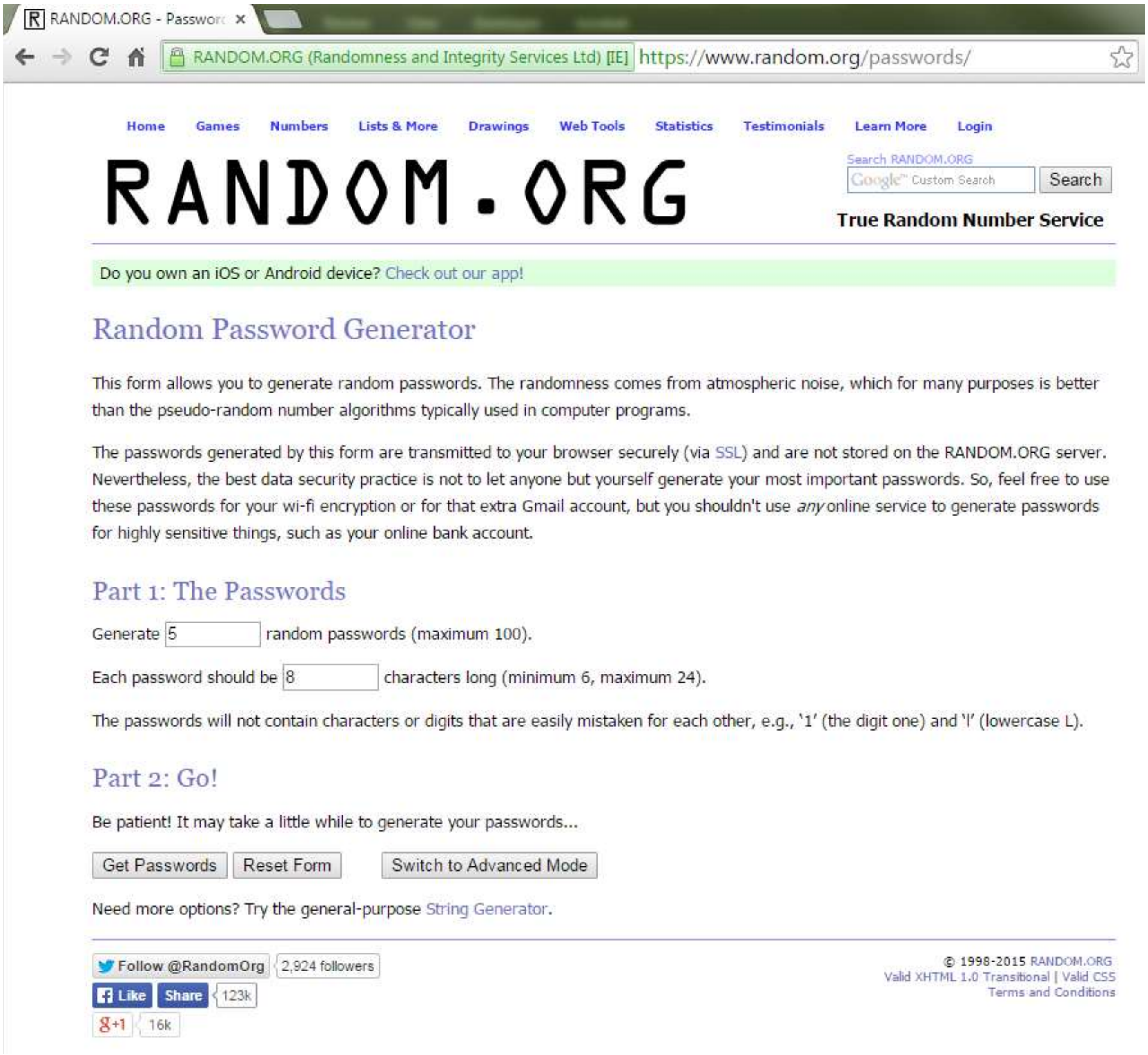
A document is only as secured as the password that is used to protect it. Consider a very sensitive University document encrypted with the password of **Plymouth**; for our organisation this would likely be one of the many passwords that could sensibly be attempted if the document fell into the wrong hands.

The password that protects your University computing account has a minimum set of requirements[4] that must be met. The same principle must apply to the information and data that you create, process, store or transmit.

If creating passwords is challenging there are websites that make the task easy, such as Random.org[5] and this is depicted over the page.

[4] SEC-GDL-003 University password requirements

[5] Random.org website – www.random.org/passwords


RANDOM.ORG - Passwor
RANDOM.ORG (Randomness and Integrity Services Ltd) [IE] https://www.random.org/passwords/
Home Games Numbers Lists & More Drawings Web Tools Statistics Testimonials Learn More Login
RANDOM.ORG
Search RANDOM.ORG
Google™ Custom Search
Search
True Random Number Service

Do you own an iOS or Android device? Check out our app!

Random Password Generator

This form allows you to generate random passwords. The randomness comes from atmospheric noise, which for many purposes is better than the pseudo-random number algorithms typically used in computer programs.

The passwords generated by this form are transmitted to your browser securely (via SSL) and are not stored on the RANDOM.ORG server. Nevertheless, the best data security practice is not to let anyone but yourself generate your most important passwords. So, feel free to use these passwords for your wi-fi encryption or for that extra Gmail account, but you shouldn't use *any* online service to generate passwords for highly sensitive things, such as your online bank account.

Part 1: The Passwords

Generate 5 random passwords (maximum 100).

Each password should be 8 characters long (minimum 6, maximum 24).

The passwords will not contain characters or digits that are easily mistaken for each other, e.g., '1' (the digit one) and 'l' (lowercase L).

Part 2: Go!

Be patient! It may take a little while to generate your passwords...

Need more options? Try the general-purpose String Generator.

© 1998-2015 RANDOM.ORG
Valid XHTML 1.0 Transitional | Valid CSS
Terms and Conditions