PROSEDUR ENKRIPSI MAKLUMAT TERPERINGKAT

MICROSOF OFFICE (WORD / POWERPOINT / EXCEL)

PEJABAT SETIAUSAHA KERAJAAN TERENGGANU

1.0 OBJEKTIF

Prosedur ini bertujuan untuk memastikan perlindungan maklumat terperingkat dalam format elektronik dilaksanakan bagi melindungi data dan maklumat dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan tanpa izin serta menjamin kesinambungan perkhidmatan kerajaan.

2.0 SKOP

Prosedur ini diguna pakai untuk melindungi maklumat terperingkat SUK Terengganu yang disedia, disimpan dan diedar secara elektronik dengan menggunakan kaedah enkripsi daripada ancaman persekitaran.

3.0 RUJUKAN

(a) Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), 01 Oktober 2000, Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

(b) Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), 15 Januari 2002, *Malaysian Public Sector Management of Information & Communicat ions Technology Security Handbook (MyMIS) Version 2.0*; dan

(c) Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), 02 April 2009, Dasar Keselamatan ICT MAMPU Terengganu versi 5.2.

4.0 DEFINISI

Bil	Istilah	Keterangan
4.1	Rahsia besar	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada SUK Terengganu .
4.2	Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan SUK Terengganu, menyebabkan kerosakan besar kepada kepentingan dan martabat SUK Terengganu atau memberi keuntungan besar kepada pihak luar.
4.3	Sulit	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan SUK Terengganu tetapi memudaratkan kepentingan atau martabat SUK Terengganu atau kegiatan Kerajaan atau orang perseorangan atau akan menjatuhkan imej SUK Terengganu atau akan menguntungkan pihak luar.
4.4	Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap pelindungan keselamatan.

5.0 KLASIFIKASI DAN PENGENDALIAN MAKLUMAT

5.1 Pengelasan Maklumat

Maklumat rasmi hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan yang telah ditetapkan sepertimana yang dinyatakan di dalam Arahan Keselamatan:

i. Rahsia Besar;
ii. Rahsia;
iii. Sulit; atau
iv. Terhad

5.2 Perlindungan Maklumat Elektronik

Bagi memastikan integriti, kerahsiaan dan kebolehsediaan maklumat elektronik, langkah-langkah berikut hendaklah dipatuhi:

i. Memastikan penyimpanan dan pengedaran maklumat elektronik adalah selamat dan terjamin;
ii. Menggunakan tanda atau label keselamatan seperti rahsia besar, rahsia, sulit atau terhad pada dokumen; dan
iii. Menggunakan enkripsi ke atas dokumen terperingkat yang disedia, disimpan dan diedar secara elektronik.

5.3 Perlindungan Maklumat Elektronik Melalui Kaedah Enkripsi

Perlindungan maklumat digital atau elektronik memerlukan kaedah pengendalian media yang berbeza seperti penggunaan enkripsi. Kaedah ini melibatkan aktiviti penukaran teks biasa (*plaintext*) kepada kod yang t idak dapat difahami dan kod yang t idak difahami ini akan menjadi versi teks *cipher*. Bagi mendapatkan semula teks biasa tersebut, proses dekripsi digunakan.

Pengendalian Maklumat	Rahsia Besar	Rahsia	Sulit	Terhad	Terbuka
Penyimpanan					
Penyimpanan dalam Media Tetap / Media Boleh tukar (Fixed disk and exchangeable)	Enkripsi maklumat dilakukan jika diperlukan atau menggunakan kawalan lain seperti kawalan akses, pengurusan kata laluan dan bentuk-bentuk kawalan rangkaian lain.				Tidak diperlukan
Menghantar / Memindahkan					
Menghantar maklumat melalui Rangkaian Awam	Menggunakan kaedah enkripsi				Tidak diperlukan

Jadual 1: Pengendalian Maklumat Elektronik

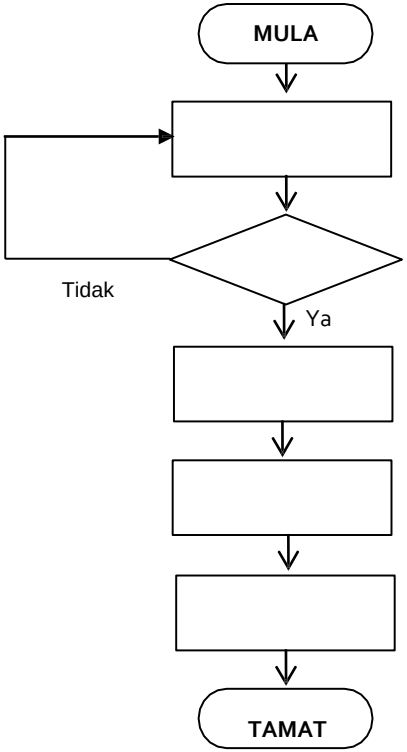
6.0 PROSES ENKRIPSI MAKLUMAT TERPERINGKAT

Enkripsi / Dekripsi

i. Salah satu kaedah yang praktikal untuk memelihara data adalah dengan menukarkannya ke dalam bentuk rahsia di mana penerima yang sah sahaja dapat memahaminya.
ii. Enkripsi (*Encryption*) ~ pengirim menukarkan mesej asal ke bentuk rahsia dan menghantar kepada penerima.
iii. Dekripsi (*Decrypt ion*) ~ menterbalikkan kembali proses enkripsi supaya mesej ditukar ke dalam bentuk yang asal.

Proses Enkripsi / Dekripsi

i. Pengirim menggunakan algorithma enkripsi dan kunci untuk menukarkan data asal (*plaintext*) ke dalam bentuk data yang disulitkan (*cipher text*)
ii. Penerima menggunakan algorithma dekripsi dan kunci untuk menukarkan *cipher text* kembali ke data asal (*plaintext*).
iii. Kaedah enkripsi dan dekripsi boleh dibahagikan kepada 2 kategori:
   – *Convent ional (secret key / symmetric)*
   – *Public key (asymmetric)*



Laksanakan pengkelasan dan pelabelan maklumat rasmi mengikut pengelasannya seperti dalam Arahan Keselamatan

Telah dikelaskan?

Rekod pengkelasan dan pelabelan maklumat rasmi

Simpan maklumat dengan menggunakan enkripsi maklumat atau menggunakan kawalan lain seperti kawalan akses, pengurusan kata laluan dan bentuk-bentuk kawalan rangkaian lain

Hantar maklumat dengan menggunakan enkripsi maklumat sekiranya menggunakan rangkaian awam

[7]

PROSEDUR ENKRIPSI/DEKRIPSI APLIKASI MICROSOFT OFFICE 2016

WORD
POWERPOINT
EXCEL

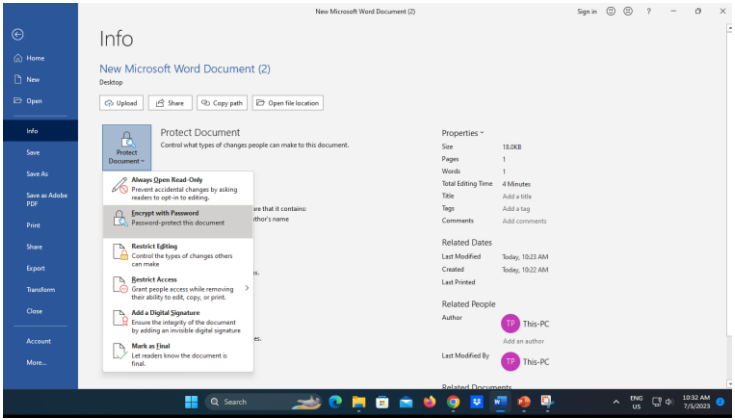
PROSEDUR ENKRIPSI/DEKRIPSI MICROSOFT WORD 2016

PENGENALAN

Aplikasi Microsoft Office sering digunakan dalam penghasilan dokumen seharian. Bahagian ini akan menerangkan prosedur enkripsi yang boleh dilakukan pada dokumen berkaitan sebagai langkah keselamatan asas.

LANGKAH-LANGKAH

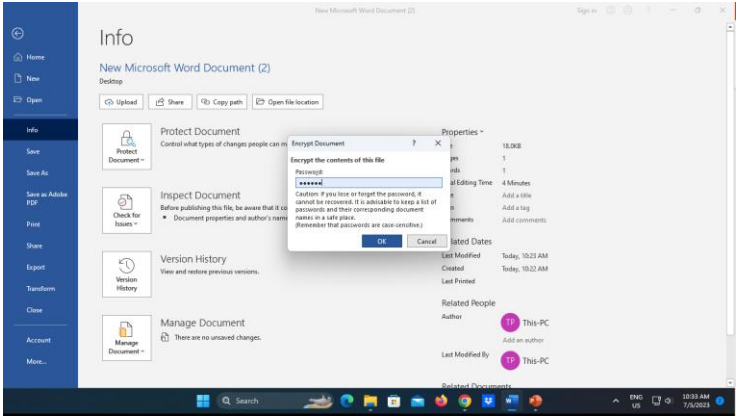
1. Buka fail dalam Microsoft Word dan pilih File>Info>Protect Document>Encrypt with Password (rujuk Rajah 1).



Rajah 1: Langkah 1 Penyulitan (Encrypt) dokumen dalam Microsoft Word

2. Masukkan kata laluan pada ruangan ***'Password'*** *(rujuk Rajah 2).*

3. *Klik* ***'OK'****.*



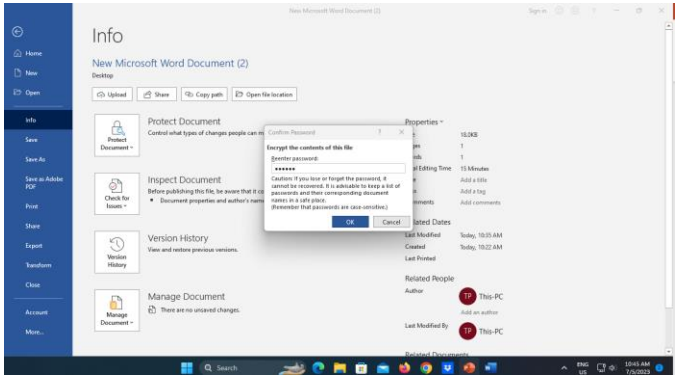
Rajah 2: Langkah 2 Penetapan kata laluan untuk membuka dokumen

4. Skrin untuk memasukkan '***Reenter Password***' sebagai pengesahan kata laluan yang telah dipilih akan dipaparkan (rujuk Rajah 3).

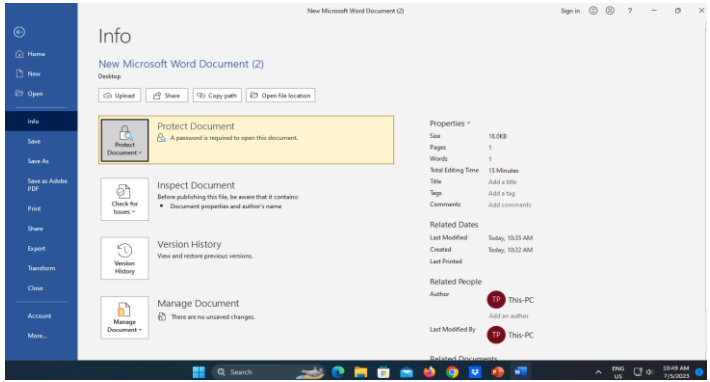
5. Sila klik '**OK**'.

6. Pada skrin yang dipaparkan, pada pilihan Tab Info, perkataan *Protect Document* telah bertukar warna dan menunjukkan enkripsi telah dilaksanakan untuk dokumen ini (rujuk Rajah 4).

7. Sila klik pilihan '***Save Document'*** setelah selesai

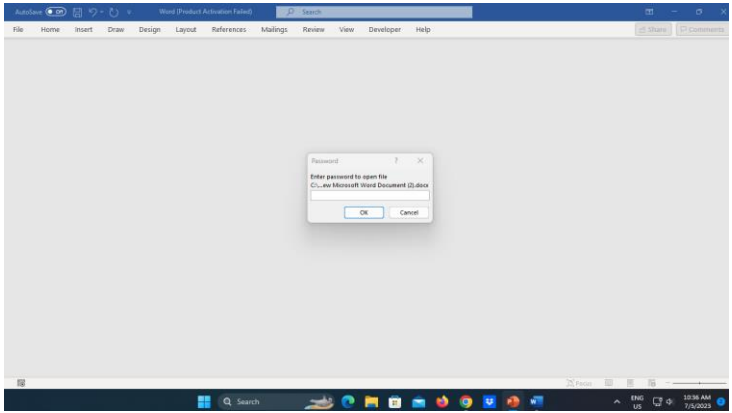


Rajah 3: Pengesahan Kata Laluan



Rajah 4: Perubahan warna teks 'Protect Document' selepas pelaksanaan enkripsi

8. Dokumen tersebut kini memerlukan kata laluan sebelum boleh dibuka dan/atau diubahsuai oleh pihak lain (rujuk Rajah 5).

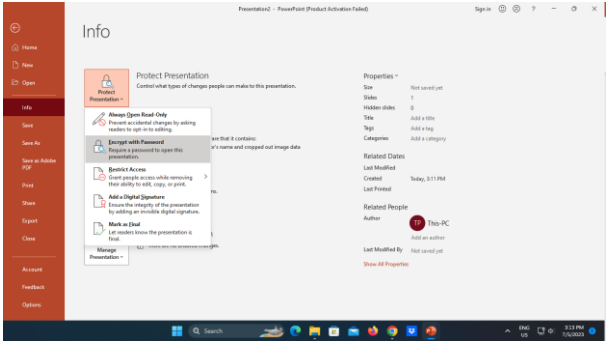


Rajah 5: Kata laluan untuk membuka dokumen

PROSEDUR ENKRIPSI/DEKRIPSI MICROSOFT POWERPOINT 2016

LANGKAH -LANGKAH

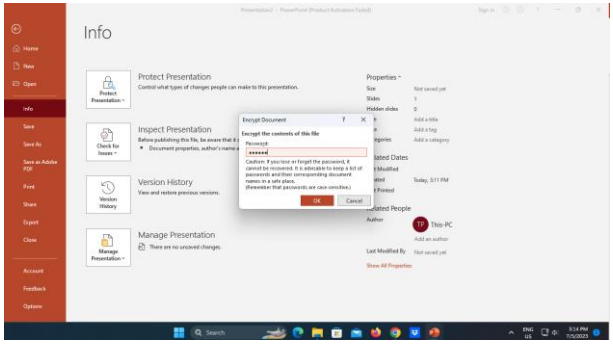
1. Buka fail dalam Microsoft Powerpoint dan pilih File>Info>Protect Document>Encrypt with Password (rujuk Rajah 6).



Rajah 6: Langkah 1 Penyulitan (Encrypt) dokumen dalam Microsoft Powerpoint

2. Masukkan kata laluan pada ruangan '***Password***' (rujuk Rajah 7).

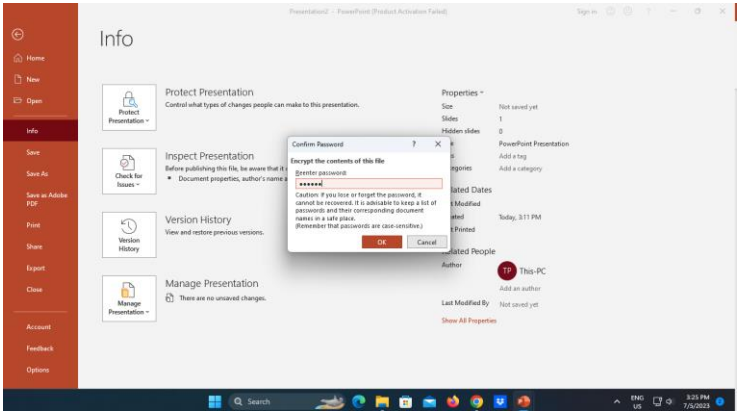
3. Klik **'OK'.**



Rajah 7: Penetapan kata laluan untuk membuka dokumen'

4. Skrin untuk memasukkan '***Reenter Password***' sebagai pengesahan kata laluan yang telah dipilih akan dipaparkan (rujuk Rajah 8).

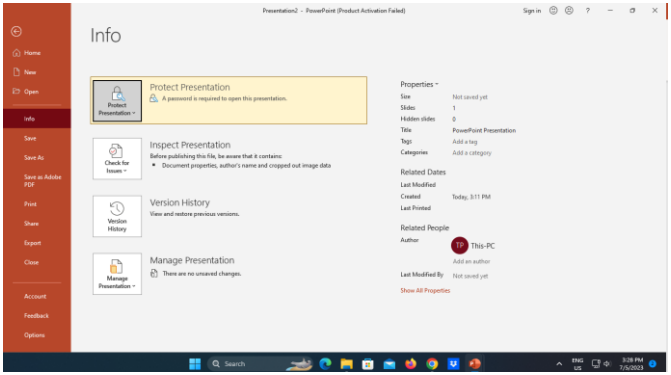
5. Klik '**OK**' setelah selesai



Rajah 8: Pengesahan Kata Laluan

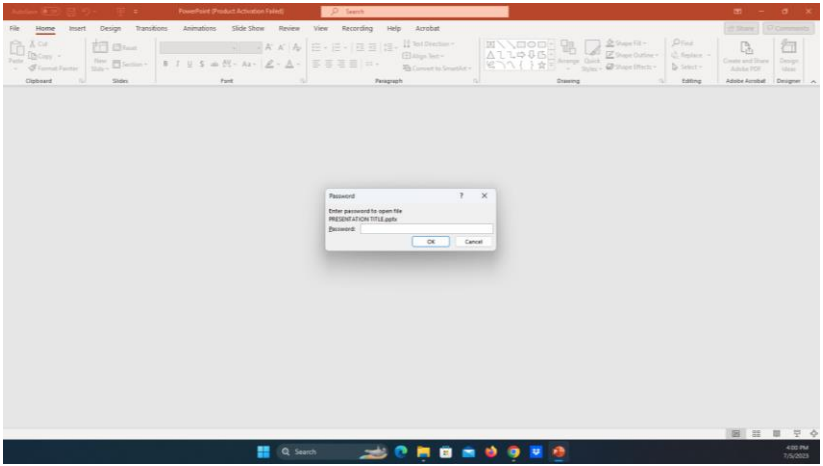
6. Pada skrin yang dipaparkan, pada pilihan Tab Info, perkataan *Protect Presentation* telah bertukar warna dan menunjukkan enkripsi telah dilaksanakan untuk dokumen ini (rujuk Rajah 9).

7. Sila klik pilihan '***Save Document***' setelah selesai.



Rajah 9: Perubahan warna teks 'Protect Presentation' selepas pelaksanaan enkripsi

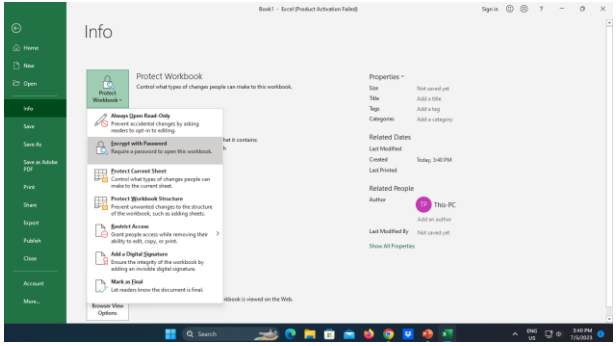
8. Dokumen tersebut kini memerlukan kata laluan sebelum boleh dibuka dan/atau diubahsuai oleh pihak lain (rujuk Rajah 10).



Rajah 10: Kata laluan untuk membuka dokumen

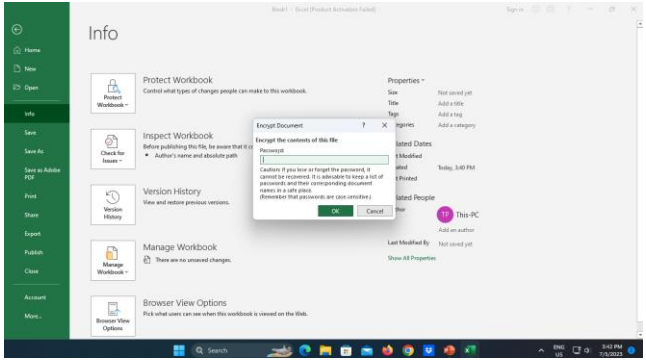
LANGKAH-LANGKAH

1. Buka fail dalam Microsoft Powerpoint dan pilih File>Info>Protect Document>Encrypt with Password (rujuk Rajah 11).



Rajah 11: Langkah 1

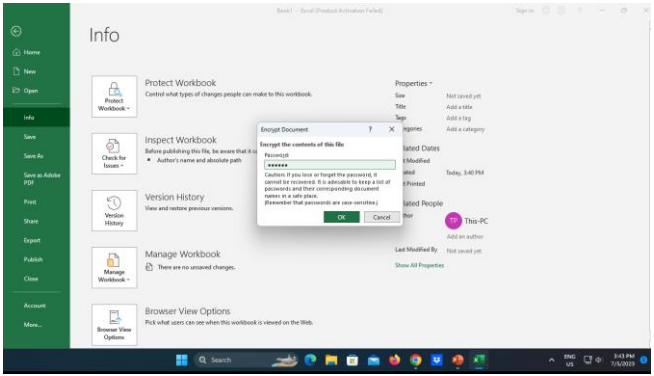
2. Skrin berikut akan dipaparkan (rujuk Rajah 12)



Rajah 12: Skrin untuk memasukkan '*Password*'

3. Masukkan kata laluan pada ruangan '***Password***' *(rujuk Rajah 13).*

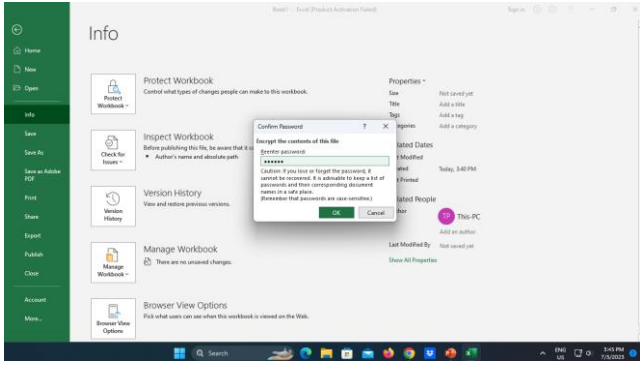
4. *Klik '**OK**'.*



Rajah 13: Memasukkan Kata Laluan

5. Skrin untuk memasukkan '***Reenter Password***' sebagai pengesahan kata laluan yang telah dipilih akan dipaparkan (rujuk Rajah 14).

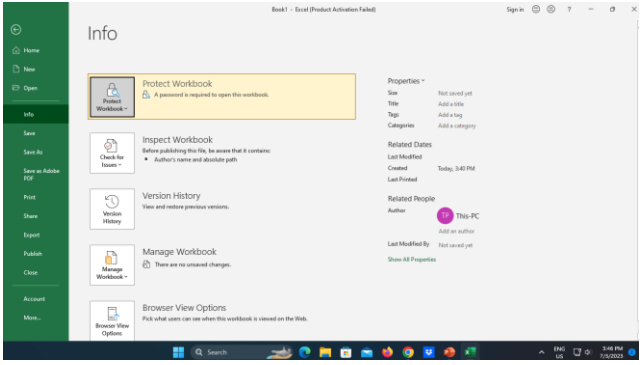
6. Sila klik '**OK**'.



Rajah 14: Pengesahan kata laluan untuk membenarkan dokumen diubah

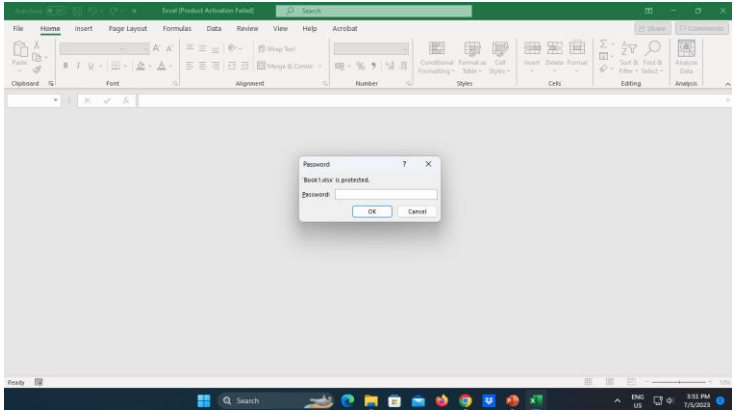
7. Pada skrin yang dipaparkan, pada pilihan Tab Info, perkataan *Protect Presentation* telah bertukar warna dan menunjukkan enkripsi telah dilaksanakan untuk dokumen ini (rujuk Rajah 15).

8. Sila klik pilihan '***Save Document'*** setelah selesai.



Rajah 15: Perubahan warna teks 'Protect Presentation' selepas pelaksanaan enkripsi

9. Dokumen tersebut kini memerlukan kata laluan sebelum boleh dibuka dan/atau diubahsuai oleh pihak lain (rujuk Rajah 16).



Rajah 16: Kata laluan untuk membuka dokumen

DISEDIAKAN OLEH:

PEJABAT SETIAUSAHA KERAJAAN TERENGGANU
(BAHAGIAN PEMBANGUNAN TEKNOLOGI MAKLUMAT)
TINGKAT 2, WISMA DARUL IMAN
20503 KUALA TERENGGANU

www.terengganu.gov.my

Telefon : 09-623 1957

Faks : 09 623 7485

PROSEDUR ENKRIPSI MAKLUMAT TERPERINGKAT

ADOBE ACROBAT PROFESSIONAL

PEJABAT SETIAUSAHA KERAJAAN TERENGGANU

1.0 OBJEKTIF

Prosedur ini bertujuan untuk memastikan perlindungan maklumat terperingkat dalam format elektronik dilaksanakan bagi melindungi data dan maklumat dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan tanpa izin serta menjamin kesinambungan perkhidmatan kerajaan.

2.0 SKOP

Prosedur ini diguna pakai untuk melindungi maklumat terperingkat SUK yang disedia, disimpan dan diedar secara elektronik dengan menggunakan kaedah enkripsi daripada ancaman persekitaran.

3.0 RUJUKAN

(a) Pejabat Setiausaha Kerajaan Terengganu (SUK), 01 Oktober 2000, Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

(b) Pejabat Setiausaha Kerajaan Terengganu (SUK), 15 Januari 2002, *Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS) Version 2.0*; dan

(c) Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (), 02 April 2009, Dasar Keselamatan ICT SUK versi 5.2.

4.0 DEFINISI

Bil	Istilah	Keterangan
4.1	Rahsia besar	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada SUK.
4.2	Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan SUK, menyebabkan kerosakan besar kepada kepentingan dan martabat SUK atau memberi keuntungan besar kepada pihak luar.
4.3	Sulit	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan SUK tetapi memudaratkan kepentingan atau martabat SUK atau kegiatan Kerajaan atau orang perseorangan atau akan menjatuhkan imej SUK atau akan menguntungkan pihak luar.
4.4	Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap pelindungan keselamatan.

5.0 KLASIFIKASI DAN PENGENDALIAN MAKLUMAT

5.1 Pengelasan Maklumat

Maklumat rasmi hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan yang telah ditetapkan sepertimana yang dinyatakan di dalam Arahan Keselamatan:

i. Rahsia Besar;
ii. Rahsia;
iii. Sulit; atau
iv. Terhad

5.2 Perlindungan Maklumat Elektronik

Bagi memastikan integriti, kerahsiaan dan kebolehsediaan maklumat elektronik, langkah-langkah berikut hendaklah dipatuhi:

i. Memastikan penyimpanan dan pengedaran maklumat elektronik adalah selamat dan terjamin;
ii. Menggunakan tanda atau label keselamatan seperti rahsia besar, rahsia, sulit atau terhad pada dokumen; dan
iii. Menggunakan enkripsi ke atas dokumen terperingkat yang disedia, disimpan dan diedar secara elektronik.

5.3 Perlindungan Maklumat Elektronik Melalui Kaedah Enkripsi

Perlindungan maklumat digital atau elektronik memerlukan kaedah pengendalian media yang berbeza seperti penggunaan enkripsi. Kaedah ini melibatkan aktiviti penukaran teks biasa (*plaintext*) kepada kod yang tidak dapat difahami dan kod yang tidak difahami ini akan menjadi versi teks *cipher*. Bagi mendapatkan semula teks biasa tersebut, proses dekripsi digunakan.

Pengendalian Maklumat	Rahsia Besar	Rahsia	Sulit	Terhad	Terbuka
Penyimpanan					
Penyimpanan dalam Media Tetap / Media Boleh tukar (Fixed disk and exchangeable)	Enkripsi maklumat dilakukan jika diperlukan atau menggunakan kawalan lain seperti kawalan akses, pengurusan kata laluan dan bentuk-bentuk kawalan rangkaian lain.				Tidak diperlukan
Menghantar / Memindahkan					
Menghantar maklumat melalui Rangkaian Awam	Menggunakan kaedah enkripsi				Tidak diperlukan

Jadual 1: Pengendalian Maklumat Elektronik

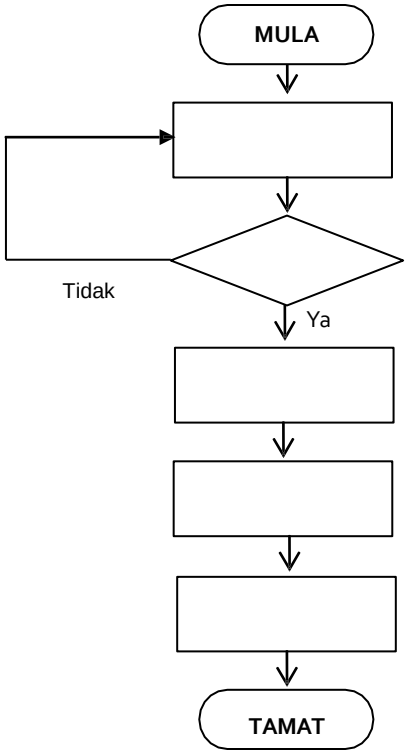
6.0 PROSES ENKRIPSI MAKLUMAT TERPERINGKAT

Enkripsi / Dekripsi

i. Salah satu kaedah yang praktikal untuk memelihara data adalah dengan menukarkannya ke dalam bentuk rahsia di mana penerima yang sah sahaja dapat memahaminya.
ii. Enkripsi (*Encryption*) ~ pengirim menukarkan mesej asal ke bentuk rahsia dan menghantar kepada penerima.
iii. Dekripsi (*Decryption*) ~ menterbalikkan kembali proses enkripsi supaya mesej ditukar ke dalam bentuk yang asal.

Proses Enkripsi / Dekripsi

i. Pengirim menggunakan algorithma enkripsi dan kunci untuk menukarkan data asal (*plaintext*) ke dalam bentuk data yang disulitkan (*cipher text*)
ii. Penerima menggunakan algorithma dekripsi dan kunci untuk menukarkan *cipher text* kembali ke data asal (*plaintext*).
iii. Kaedah enkripsi dan dekripsi boleh dibahagikan kepada 2 kategori:
   – *Conventional (secret key / symmetric)*
   – *Public key (asymmetric)*



Laksanakan pengkelasan dan pelabelan maklumat rasmi mengikut pengelasannya seperti dalam Arahan Keselamatan

Telah dikelaskan?

Rekod pengkelasan dan pelabelan maklumat rasmi

Simpan maklumat dengan menggunakan enkripsi maklumat atau menggunakan kawalan lain seperti kawalan akses, pengurusan kata laluan dan bentuk-bentuk kawalan rangkaian lain

Hantar maklumat dengan menggunakan enkripsi maklumat sekiranya menggunakan rangkaian awam

[7]

PROSEDUR ENKRIPSI/DEKRIPSI
APLIKASI ADOBE ACROBAT PROFESSIONAL

PROSEDUR ENKRIPSI/DEKRIPSI ADOBE ACROBAT PROFESSIONAL

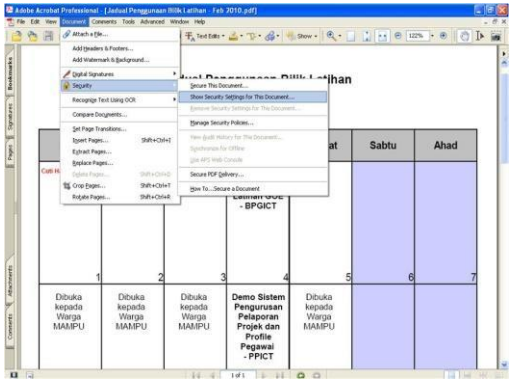
PENGENALAN

Aplikasi Adobe Acrobat Professional sering digunakan dalam penghasilan dokumen seharian. Bahagian ini akan menerangkan prosedur enkripsi yang boleh dilakukan pada dokumen berkaitan sebagai langkah keselamatan asas.

LANGKAH-LANGKAH

1. Pilih menu "***Document***"
2. Pilih menu "***Security***"
3. Klik "***Show Security Settings for This Document***"

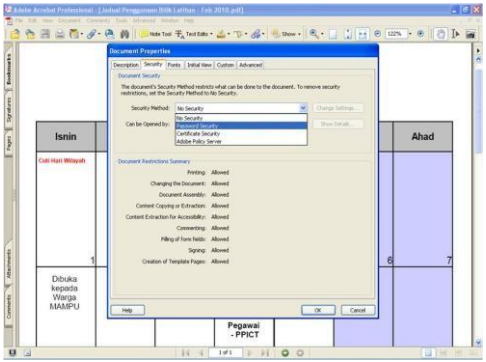
   Nota: Sila Rujuk Langkah 1



Rajah1

4. Pilih tab "***Security***"
5. Klik pilihan enkripsi pada arahan "***Security Method***"
6. Pilih "***Password Security***"

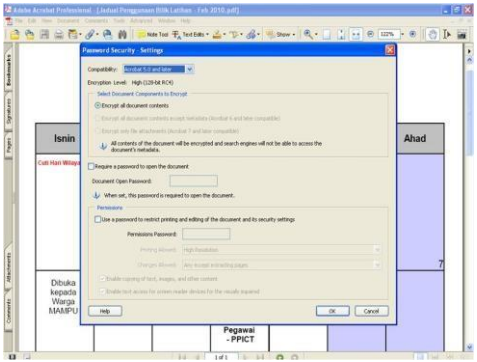
Nota: Sila Rujuk Langkah 2



Rajah 2

7. Pilih versi fail yang difikirkan sesuai untuk membuka dokumen tersebut pada menu '***Compatibility***'

Nota: Sila Rujuk Langkah 3

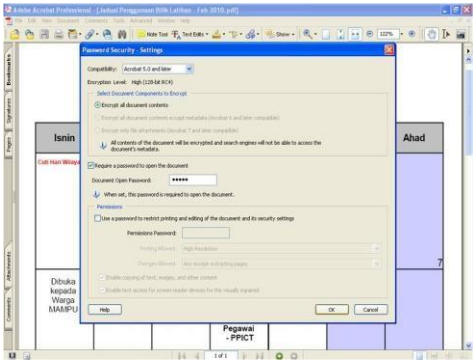


Rajah 3

8. Sila tanda √ pada menu '***Require a Password to Open the Document***'. Medan '***Document Open Password***' akan diaktifkan.

9. Taipkan kata laluan yang sesuai.

Nota: Sila Rujuk Langkah 4

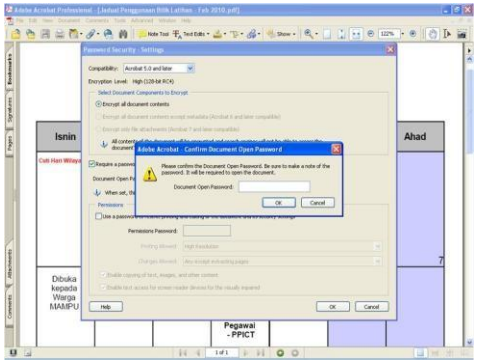


Rajah4

10. Taip kata laluan yang berkenaan bagi tujuan pengesahan.

11. Klik "**OK**".

Nota: Sila Rujuk Langkah 5



Rajah5

12. Sila klik pilihan '***Save Document'*** setelah selesai.

13. Seterusnya pemunya dokumen akan memaklumkan penerima tentang kata laluan melalui e-mel ataupun telefon bagi membuka dokumen berkenaan.

14. Dokumen tersebut kini memerlukan kata laluan sebelum boleh dibuka dan/atau diubahsuai oleh penerima.

PEJABAT SETIAUSAHA KERAJAAN TERENGGANU

DISEDIAKAN OLEH:

PEJABAT SETIAUSAHA KERAJAAN TERENGGANU
(BAHAGIAN PEMBANGUNAN TEKNOLOGI MAKLUMAT)
TINGKAT 2, WISMA DARULIMAN
20503 KUALA TERENGGANU

www.terengganu.gov.my

Telefon : 09-623 1957
Faks : 09-625 1990

PROSEDUR ENKRIPSI MAKLUMAT TERPERINGKAT

WINRAR

PEJABAT SETIAUSAHA KERAJAAN TERENGGANU

1.0 OBJEKTIF

Prosedur ini bertujuan untuk memastikan perlindungan maklumat terperingkat dalam format elektronik dilaksanakan bagi melindungi data dan maklumat dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan tanpa izin serta menjamin kesinambungan perkhidmatan kerajaan.

2.0 SKOP

Prosedur ini diguna pakai untuk melindungi maklumat terperingkat SUK Terengganu yang disedia, disimpan dan diedar secara elektronik dengan menggunakan kaedah enkripsi daripada ancaman persekitaran.

3.0 RUJUKAN

(a) Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), 01 Oktober 2000, Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

(b) Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), 15 Januari 2002, *Malaysian Public Sector Management of Information & Communicat ions Technology Security Handbook (MyMIS) Version 2.0*; dan

(c) Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), 02 April 2009, Dasar Keselamatan ICT MAMPU Terengganu versi 5.2.

4.0 DEFINISI

Bil	Istilah	Keterangan
4.1	Rahsiabesar	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada SUK Terengganu.
4.2	Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan SUK Terengganu, menyebabkan kerosakan besar kepada kepentingan dan martabat SUK Terengganu atau memberi keuntungan besar kepada pihak luar.
4.3	Sulit	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan SUK Terengganu tetapi memudaratkan kepentingan atau martabat SUK Terengganu atau kegiatan Kerajaan atau orang perseorangan atau akan menjatuhkan imej SUK Terengganu atau akan menguntungkan pihak luar.
4.4	Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap pelindungan keselamatan.

5.0 KLASIFIKASI DAN PENGENDALIAN MAKLUMAT

5.1 Pengelasan Maklumat

Maklumat rasmi hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan yang telah ditetapkan sepertimana yang dinyatakan di dalam Arahan Keselamatan:

i. Rahsia Besar;
ii. Rahsia;
iii. Sulit; atau
iv. Terhad

5.2 Perlindungan Maklumat Elektronik

Bagi memastikan integriti, kerahsiaan dan kebolehsediaan maklumat elektronik, langkah-langkah berikut hendaklah dipatuhi:

i. Memastikan penyimpanan dan pengedaran maklumat elektronik adalah selamat dan terjamin;
ii. Menggunakan tanda atau label keselamatan seperti rahsia besar, rahsia, sulit atau terhad pada dokumen; dan
iii. Menggunakan enkripsi ke atas dokumen terperingkat yang disedia, disimpan dan diedar secara elektronik.

5.3 Perlindungan Maklumat Elektronik Melalui Kaedah Enkripsi

Perlindungan maklumat digital atau elektronik memerlukan kaedah pengendalian media yang berbeza seperti penggunaan enkripsi. Kaedah ini melibatkan aktiviti penukaran teks biasa (*plaintext*) kepada kod yang tidak dapat difahami dan kod yang tidak difahami ini akan menjadi versi teks *cipher*. Bagi mendapatkan semula teks biasa tersebut, proses dekripsi digunakan.

Pengendalian Maklumat	Rahsia Besar	Rahsia	Sulit	Terhad	Terbuka
Penyimpanan					
Penyimpanan dalam Media Tetap / Media Boleh tukar (Fixed disk and exchangeable)	Enkripsi maklumat dilakukan jika diperlukan atau menggunakan kawalan lain seperti kawalan akses, pengurusan kata laluan dan bentuk-bentuk kawalan rangkaianlain.				Tidak diperlukan
Menghantar / Memindahkan					
Menghantar maklumat melalui Rangkaian Awam	Menggunakan kaedah enkripsi				Tidak diperlukan

Jadual 1: Pengendalian Maklumat Elektronik

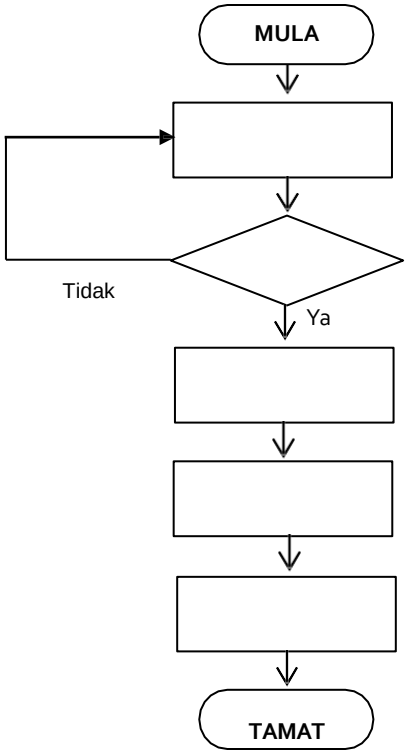
6.0 PROSES ENKRIPSI MAKLUMAT TERPERINGKAT

Enkripsi / Dekripsi

i. Salah satu kaedah yang praktikal untuk memelihara data adalah dengan menukarkannya ke dalam bentuk rahsia di mana penerima yang sah sahaja dapat memahaminya.
ii. Enkripsi (*Encryption*) ~ pengirim menukarkan mesej asal ke bentuk rahsia dan menghantar kepada penerima.
iii. Dekripsi (*Decryption*) ~ menterbalikkan kembali proses enkripsi supaya mesej ditukar ke dalam bentuk yang asal.

Proses Enkripsi / Dekripsi

i. Pengirim menggunakan algorithma enkripsi dan kunci untuk menukarkan data asal (*plaintext*) ke dalam bentuk data yang disulitkan (*cipher text*)
ii. Penerima menggunakan algorithma dekripsi dan kunci untuk menukarkan *cipher text* kembali ke data asal (*plaintext*).
iii. Kaedah enkripsi dan dekripsi boleh dibahagikan kepada 2 kategori:
   – *Conventional (secret key / symmetric)*
   – *Public key (asymmetric)*



Laksanakan pengkelasan dan pelabelan maklumat rasmi mengikut pengelasannya seperti dalam Arahan Keselamatan

Telah dikelaskan?

Rekod pengkelasan dan pelabelan maklumat rasmi

Simpan maklumat dengan menggunakan enkripsi maklumat atau menggunakan kawalan lain seperti kawalan akses, pengurusan kata laluan dan bentuk-bentuk kawalan rangkaian lain

Hantar maklumat dengan menggunakan enkripsi maklumat sekiranya menggunakan rangkaian awam

[7]

PROSEDUR ENKRIPSI WINRAR

PEJABAT SETIAUSAHA KERAJAAN TERENGGANU

PROSEDUR ENKRIPSI WINRAR

PENGENALAN

Aplikasi Winrar sering digunakan untuk mengecilkan saiz folder yang besar untuk memudahkan penghantaran melalui emel.

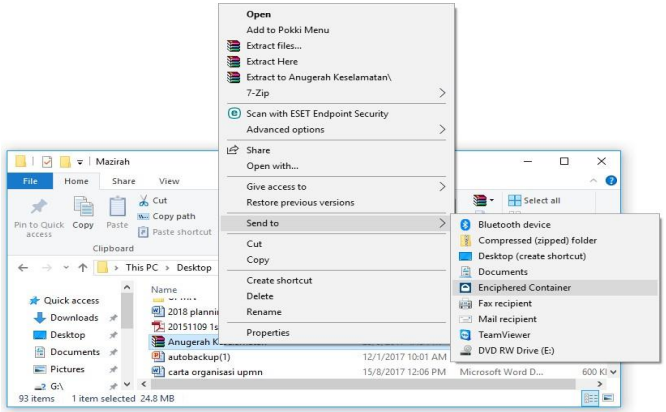
LANGKAH-LANGKAH

1. ***Download*** aplikasi encipher.it di https://encipher.it/download

2. ***Run*** aplikasi encipher.it pada komputer

3. Klik kanan dan ***Send to*** fail .zip ke ***Encipheres Container***

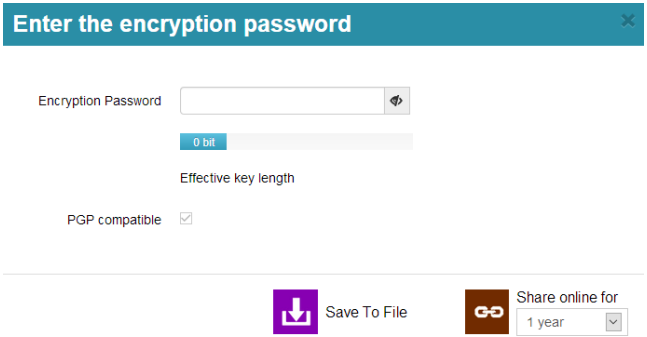
   Nota: Sila Rujuk Rajah1



Rajah1

4. Masukkan ***password*** dan klik ***save tofile***

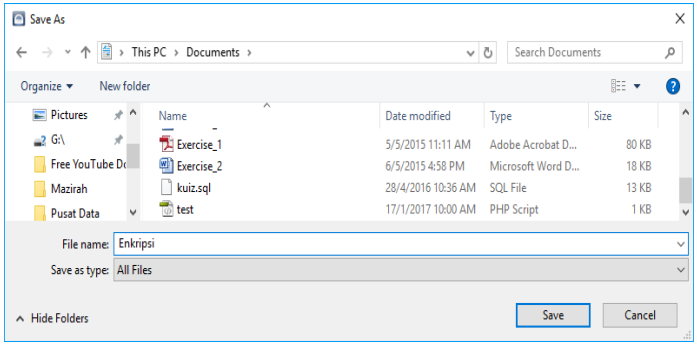
   Nota: Sila Rujuk Rajah 2



Rajah 2

5. ***Save*** nama fail yang dikehendaki

   Nota: Sila Rujuk Rajah 3



Rajah 3

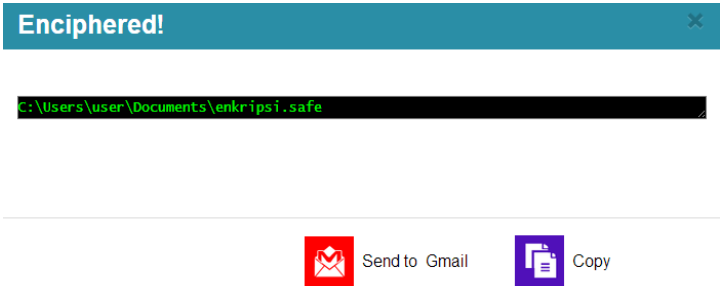
[10]

6. Enkripsi berjaya

7.Seterusnya pemunya fail winrar akan memaklumkan penerima tentang kata laluan melalui emel ataupun telefon bagi membuka fail winrar berkenaan

8. Fail winrar tersebut kini memerlukan kata laluan sebelum boleh dibuke dan/atau diubahsuai oleh penerima

Nota: Sila Rujuk Rajah 4



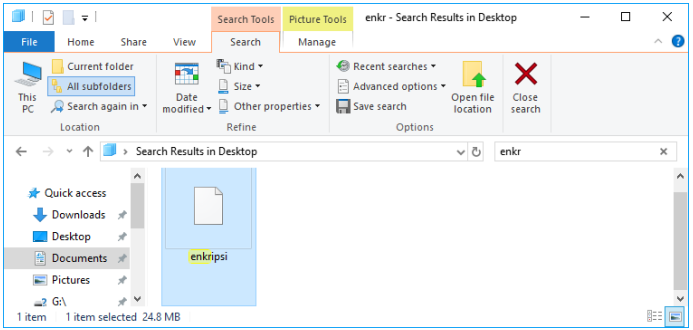
Rajah 4

PROSEDUR DEKRIPSI WINRAR

DEKRIPSI WINRAR

1. ***Double click*** pada fail winrar yang telah dibuat enkripsi.

   Nota: Sila Rujuk Rajah1

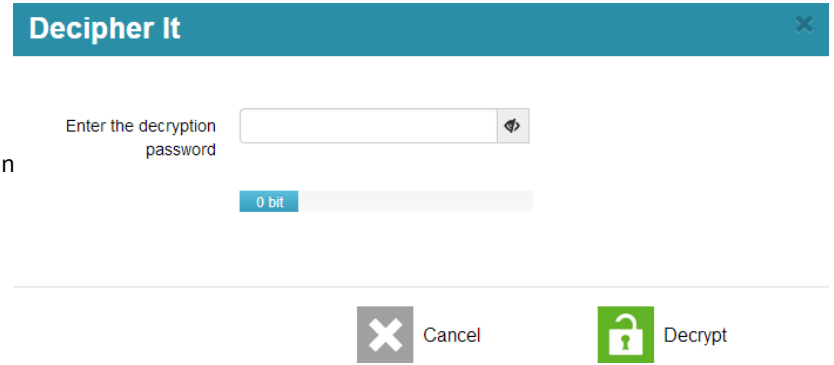


Rajah1

2. Masukkan password yang telah ditetapkan

3. Klik pada butang ***Decrypt***

   Nota: Sila Rujuk Rajah 2

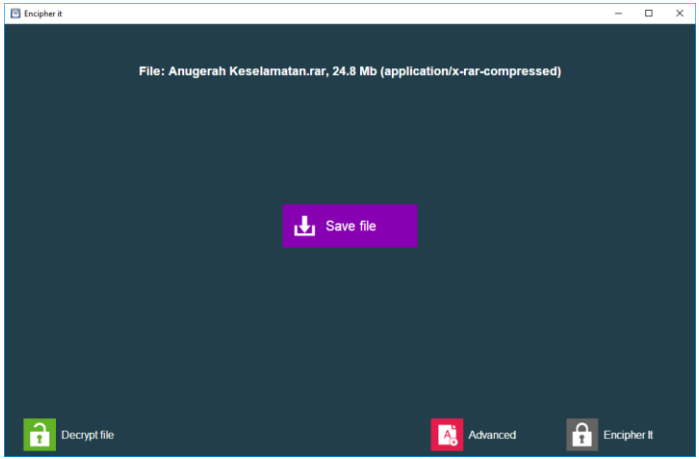


Rajah2

4. Proses dekripsi selesai

5. Save File winrar tersebut untuk di ***unzip***

Nota: Sila Rujuk Rajah3



Rajah3

DISEDIAKAN OLEH:

PEJABAT SETIAUSAHA KERAJAAN TERENGGANU
(BAHAGIAN PEMBANGUNAN TEKNOLOGI MAKLUMAT)
TINGKAT 2, WISMA DARULIMAN
20503 KUALA TERENGGANU

www.terengganu.gov.my

Telefon : 09-6231957

Faks : 09 6237485