KEAMANAN INFORMASI

Disusun oleh:

(Abdoe Rahman Sadiq)

(1310651035)

(Kelas A)

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2015

Soal 1.

Aspek keamanan informasi mempunyai ruang lingkup yang luas. Menurut referensi dari ebook CISSP, ruang lingkup materi dari keamanan informasi terdiri dari 10 pokok permasalahan. Dari 10 pokok permasalahan tersebut, silakan buatlah resume salah satu pokok permasalahan dari keamanan informasi mengacu terhadap ebook CISSP yang sudah saya upload di elearning. Resume bukan hasil translate, melainkan inti-intinya saja dari materi yang sudah Anda pahami pada ebook tersebut. Hasil resume **tidak boleh** sama dengan teman-temannya, akan tetapi tema yang dibahas boleh sama.

Cryptography

Perkenalan

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengiriman ke penerima tanpa mengalami gangguan dari pihak ketiga.

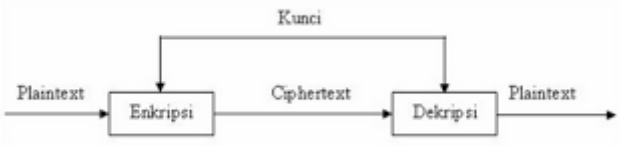
Kriptografi adalah cabang dari ilmu matematika yang memiliki banyak fungsi dalam pengamanan data. Kriptografi adalah proses mengambil pesan/message dan menggunakan beberapa fungsi untuk menggenerasi materi kriptografis (sebuah digest atau message terenkripsi).

Confidentiality, integrity, authentication, and nonrepudiation

1. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas beberapa informasi yang telah disandi.
2. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah, untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubtitusian data lain kedalam data yang sebenarnya.
3. Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4. Non-repudiasi., atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

Symetric Encryption

Algoritma simetris atau sering disebut algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses deskripsi. Algoritma kriptografi simetris dibagi menjadi dua kategori yaitu algoritma aliran (Stream Ciphers) dan algoritma blok (Block Ciphers). Dimana pada algoritma aliran, proses penyandiannya akan beriorientasi pada satu bit/byte data. Sedangkan pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit/byte data (per blok). Adapun contoh algoritma kunci simetris adalah DES (Data Encryption Standard), Blowfish, Twofish, MARS, IDEA, 3DES (DES diaplikasikan 3 kali), AES(Advanced Encryption Standard) yang bernama asli Rijndael.



Asymetric Encryption

Kriptografi asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan deskripsi. Dimana kunci enkripsi dapat disebarkan kepada umum dan dinamakan sebagai kunci publik (public key), sedangkan kunci deskripsi disimpan untuk digunakan sendiri dan dinamakan sebagai kunci pribadi (private key). Oleh karena itu, kriptografi ini dikenal pula dengan nama kriptografi kunci publik (public key cryptography). Adapun contoh algoritma yang menggunakan kunci asimetris adalah RSA (Riverst Shamir Adleman) dan ECC (Elliptic Curve Cryptography). Adapun pada kriptografi asimetris, dimana setiap pelaku sistem informasi akan memiliki sepasang kunci, yaitu kunci publik dan kunci pribadi, dimana kunci publik di distribusikan kepada umum, sedangkan kunci pribadi disimpan untuk diri sendiri. Artinya bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca surat tersebut, ia perlu mendeskripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut.

Hash Functions

Fungsi Hash sering juga disebut fungsi enkripsi satu arah, atau disebut juga message diggest. Fungsi Hash digunakan untuk menjamin servis otentikasi dan integritas suatu pesan atau file. Suatu fungsi hash h memetakan bit-bit string dengan panjang sembarang ke sebuah string dengan panjang tertentu misal n. Dengan domain D dan range R maka: Proses hashing merupakan proses pemetaan suatu input string menjadi output disebut. Output dari fungsi Hash disebut nilai hash atau hasil Hash.

1. **MD5**

   MD5 ialah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit. Pada standard Internet (RFC 1321), MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan, dan MD5 juga umum digunkan untuk melakukan pengujian integritas sebuah file.

2. **Secure Hash Algorithm**

   Secure Hash Algorithm atau bisa disebut Algoritma Kemanan hash adalah cabang dari keluarga kriptografi untuk fungsi hashing yg dipublikasikan oleh National Institute of Standards and Technology (NIST) yang didalamnya termasuk :

- **SHA-0**
- **SHA-1**
- **SHA-2**
- **SHA-3**

Algoritma	Ukuran *message digest* (bit)	Ukuran blok pesan	Kolisi
MD2	128	128	Ya
MD4	128	512	Hampir
MD5	128	512	Ya
RIPEMD	128	512	Ya
RIPEMD-128/256	128/256	512	Tidak
RIPEMD-160/320	160/320	512	Tidak
SHA-0	160	512	Ya
SHA-1	160	512	Ada cacat
SHA-256/224	256/224	512	Tidak
SHA-512/384	512/384	1024	Tidak
WHIRLPOOL	512	512	Tidak

Cryptographic Attacks

- ***Brute force***
  - Mengungkap plainteks/kunci dengan mencoba semua kemungkinan kunci.
  - Asumsi: Kriptanalis mengetahui algoritma yang digunakan.
  - Waktu yang diperlukan untuk *exhaustive key search* :

Ukuran kunci	Jumlah kemungkinan kunci	Lama waktu untuk 10^6 percobaan per detik	Lama waktu untuk 10^{12} percobaan per detik
16 bit	$2^{16} = 65536$	32.7 milidetik	0.0327 mikrodetik
32 bit	$2^{32} = 4.3 \times 10^9$	35.8 menit	2.15 milidetik
56 bit	$2^{56} = 7.2 \times 10^{16}$	1142 tahun	10.01 jam
128 bit	$2^{128} = 4.3 \times 10^{38}$	5.4×10^{24} tahun	5.4×10^{18} tahun

  - Solusi: Kriptografer harus membuat kunci yang panjang dan tidak mudah ditebak
- ***Known Plaintext***
  - Menganalisis kelemahan algoritma kriptografi untuk mengurangi kemungkinan kunci yang tidak mungkin ada.
  - Asumsi: kriptanalis mengetahui algoritma kriptografi yang digunakan.
  - Caranya: memecahkan persamaan-persamaan matematika (yang diperoleh dari definisi suatu algoritma kriptografi) yang mengandung peubah-peubah yang merepresentasikan plainteks atau kunci.
  - Metode *analytical attack* biasanya lebih cepat menemukan kunci dibandingkan dengan *exhaustive attack.*
  - Solusi: kriptografer harus membuat algoritma kriptografi yang kompleks
  - Data yang digunakan untuk menyerang sistem kriptografi:
    1. *Chipertext only*.
    2. *Known plaintext* dan *corresponding chipertext.*
    3. *Chosen plaintext* dan *corresponding chipertext.*
    4. *Chosen chipertext* dan *corresponding plaintext*
- ***Chosen plaintext and adaptive-chosen palintext***
  Kriptanalis dapat memilih plainteks tertentu untuk dienkripsikan, yaitu plainteks-plainteks yang lebih mengarahkan penemuan kunci.
- ***Chosen ciphertext and adaptive-chosen ciphertext***
  Kriptanalis dapat memilih chiphertext tertentu untuk dienkripsikan, yaitu plainteks-plainteks yang lebih mengarahkan penemuan kunci.

Digital Siganuters

Digital signature itu signature, tanda, untuk menandai suatu data atau dokumen secara digital, bukan tanda tangan yang didigitalkan. Jadi begini, sekarang banyak kan dokumen penting yang dibuat dan dikirim secara digital. Siapa yang bisa menjamin keaslian dokumen itu, tidak ada halaman yang hilang, atau tidak ada perubahan terhadap isi dokumen itu setelah dikirim atau selama masa pengiriman.

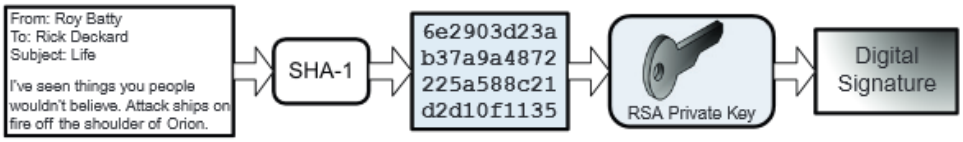


FIGURE 5.1

Creating a digital signature.[2]

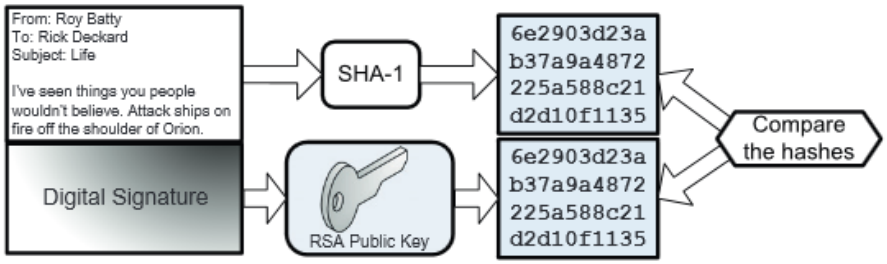


FIGURE 5.2

Dalam digital signature, suatu data/pesan akan dienkripsi dengan menggunakan kunci simetris yang diciptakan secara acak (randomly generated symmetric key). Kunci ini kemudian akan dienkripsi dengan menggunakan kunci publik dari calon penerima pesan. Hasil dari enkripsi ini kemudian dikenal/disebut sebagai "digital envelope" yang kemudian akan dikirimkan bersama pesan/data yang telah dienkripsi. Setelah menerima digital envelope penerima kemudian akan membuka/mendekripsi dengan menggunakkan kunci kunci prifatnya. Hasil yang ia dapatkan dari dekripsi tersebut adalah sebuah kunci simetris yang dapat digunakannya untuk membuka data/pesan tersebut.

Public Key Infrastructure

Dalam kriptografi, **Public Key Infrastructure** (**PKI**) adalah sebuah cara untuk otentikasi, pengamanan data dan perangkat anti sangkal. Secara teknis, PKI adalah implementasi dari berbagai teknik kriptografi yang bertujuan untuk mengamankan data, memastikan keaslian data maupun pengirimnya dan mencegah penyangkalan.

Teknik-teknik kriptografi yang digunakan antara lain: - fungsi hash, - algoritma enkripsi simetrik, dan - algoritma enkripsi asimetrik. Fungsi hash akan digunakan bersama dengan

algoritma enkripsi asimetrik dalam bentuk tanda tangan digital untuk memastikan integritas dan keaslian berita/data berikut pengirimnya. Algoritma enkripsi simetrik digunakan untuk mengamankan data dengan cara enkripsi. Dalam PKI penggunaan algoritma enkripsi simetrik tidak langsung didefinisikan tetapi telah diimplementasikan oleh berbagai perangat lunak. Secara garis besar PKI diwujudkan dalam bentuk kolaborasi antar komponen-komponennya.

SSL dan TLS

SSL(Secure Sockeet Layer) dan TLS (Transport Layer Security) adalah salah satu protokol pada jaringan komputer yang dapat menjaga kerahasiaan data yang dikirim oleh suatu *client* ke server ataupun juga sebaliknya sehingga *Third-party* (pihak ketiga) pada proses komunikasi tersebut tidak dapat menyadapnya.

IPsec

IPSec atau IP Security didesain untuk menyediakan interoperabilitas, kualitas yang baik, keamanan jaringan berbasis kriptografi untuk IPv4 dan IPv6. layanan yang disediakan meliputi kontrol akses, integritas hubungan, autentifikasi data asal, proteksi jawaban lawan, kerahasiaan (enkripsi), dan pembatasan aliran lalulintas kerahasiaan. Layanan-layanan ini tersedia dalam IP layer, memberi perlindungan pada IP dan lapisan protokol berikutnya. IP Security menyediakan sederet layanan untuk mengamankan komunikasi antar komputer dalam jaringan. Selain itu juga menambah integritas dan kerahasiaan, penerima jawaban optional (penyortiran jawaban) dan otentifikasi data asal (melalui manajemen kunci SA), IP Security juga menyediakan kontrol akses untuk lalulintas yang melaluinya. Tujuan-tujuan ini dipertemukan dengan dipertemukan melalui penggunaan dua protokol pengamanan lalulintas yaitu AH (Authentication Header) dan ESP (Encapsulating Security Payload) dan dengan penggunan prosedur dan protokol manajemen kunci kriptografi. Jika mekanisme ini diimplementasikan sebaiknya tidak merugikan pengguna, host dan komponen internet lainnya yang tidak mengguankan mekanisme ini untuk melindungi lalulintas data mereka. Mekanisme ini harus fleksibel dalam menggunakan algoritma keamanan, maksudnya yaitu modul ini dapat menggunakan algoritma sesuai dengan pilihan tanpa mempengaruhi komponen implementasi lainnya. Penggunaan algoritma defaultnya harus dapat memfasilitasi interoperabilitas dalam internet pada umumnya. Pengguanaan algoritma ini dalam hubungannya dengan proteksi lalulintas (IPSec traffic protection) dan protokol manajemen kunci (key managemen protocols), bertujuan memperbolehkan sistem dan pengembang aplikasi untuk meningkatkan kualitas yang tinggi, lapisan internet, teknologi keamanan berbasis kriptografi.

AH and ESP

protokol Authentication Header (AH): menawarkan autentikasi pengguna dan perlindungan dari beberapa serangan (umumnya serangan man in the middle), dan juga menyediakan fungsi autentikasi terhadap data serta integritas terhadap data. Protokol ini mengizinkan penerima untuk merasa yakin bahwa identitas si pengirim adalah benar adanya, dan data pun tidak dimodifikasi selama transmisi. Namun, protokol AH tidak menawarkan fungsi enkripsi terhadap data yang ditransmisikannya. Informasi AH dimasukkan ke dalam header paket IP yang dikirimkan dan dapat digunakan secara sendirian atau bersamaan dengan protokol Encapsulating Security Payload.

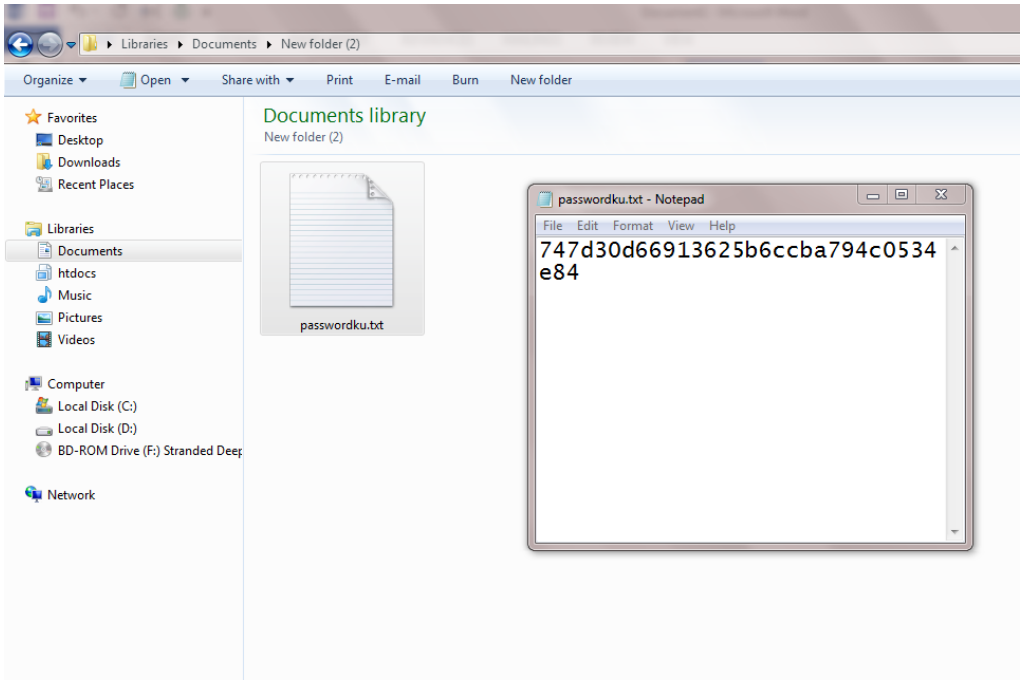
protokol Encapsulating Security Payload (ESP): Protokol ini melakukan enkapsulasi serta enkripsi terhadap data pengguna untuk meningkatkan kerahasiaan data. ESP juga dapat memiliki skema autentikasi dan perlindungan dari beberapa serangan dan dapat digunakan secara sendirian atau bersamaan dengan Authentication Header. Sama seperti halnya AH, informasi mengenai ESP juga dimasukkan ke dalam header paket IP yang dikirimkan.

Soal. 2

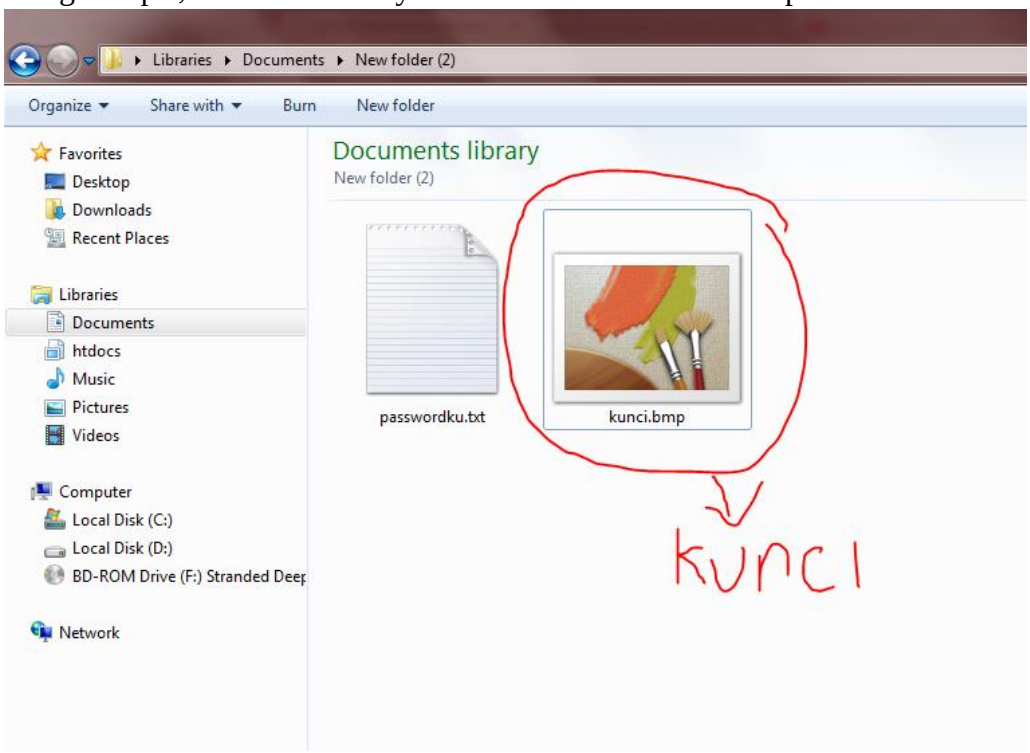
Cari software atau tools pendukung keamanan informasi kemudian cobalah fungsional software tersebut untuk menangani kasus tertentu. Buatlah step by step yang terdiri dari screenshot, keterangan gambar, dan analisis. Misalnya penggunaan wireshark dalam melakukan analisis paket data jaringan (pcap file), penggunaan ftk forensic untuk mengetahui file steganografi, dan lain sebagainya. Review software boleh sama, akan tetapi kasusnya harus berbeda dengan temen-temennya.

Mengamankan File dengan Axcrypt

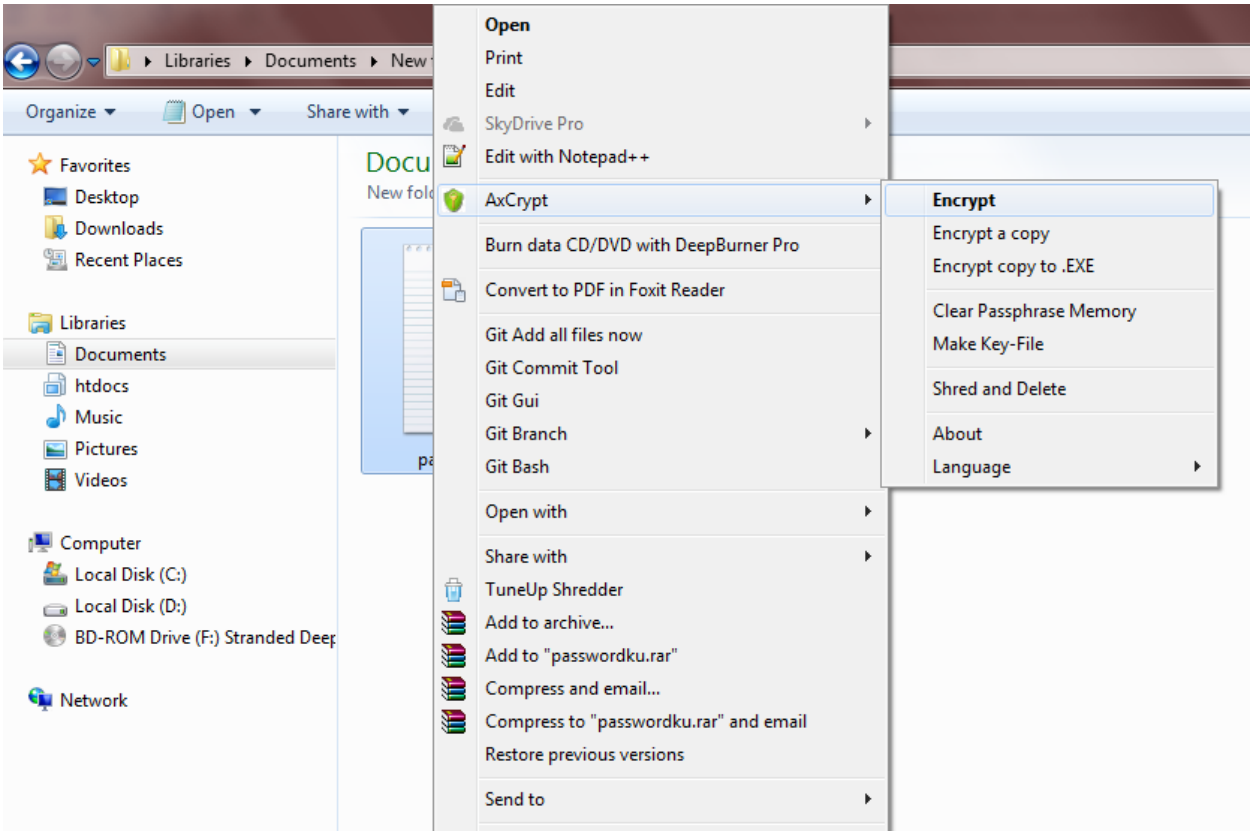
1. Langkah pertama saya akan membaut file password.txt yang akan berisi plaintext yang sudah di has ke MD5 yang nantinya file password.txt ini akan kita amankan



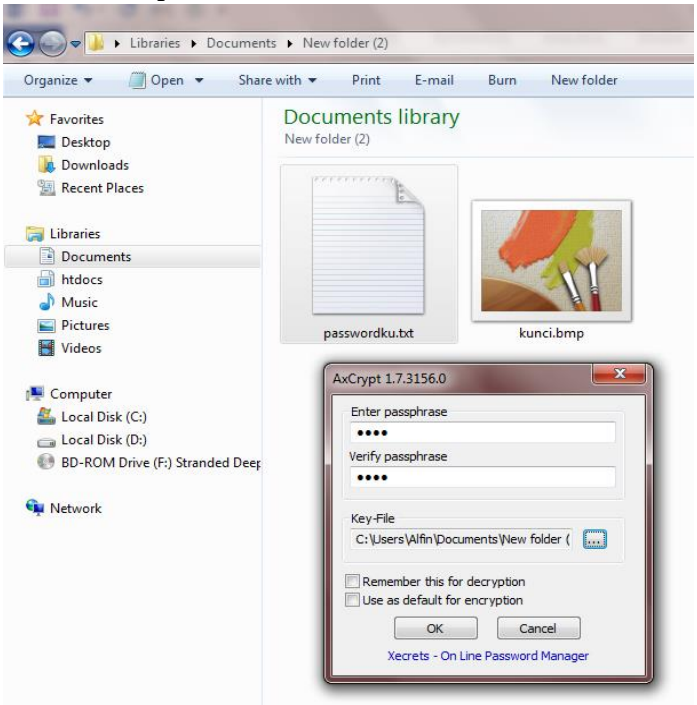
2. Setelah itu kita buat satu file lagi yang nantinya kita jadikan sebagai kunci untuk mengenkripsi, contoh disini saya buat file bernama kunci.bmp



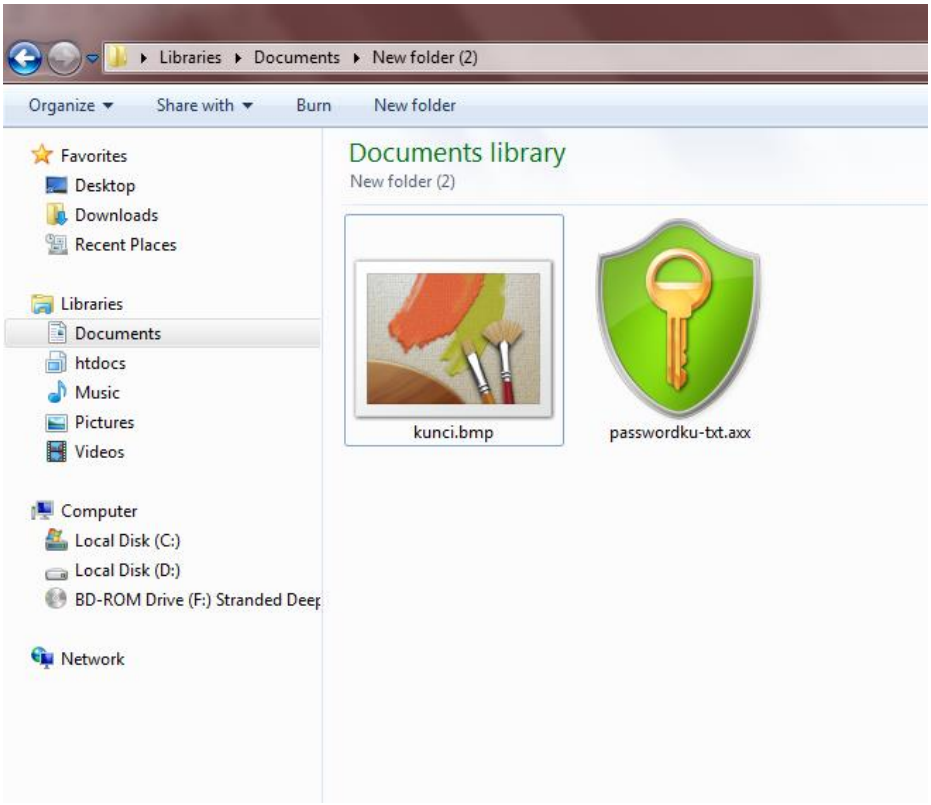
3. Setelah itu kita lakukan pengenkripsian terhadap file password.txt tersebut menggunakan Axcrypt, dengan cara klik kanan > Axcrypt > Encrypt



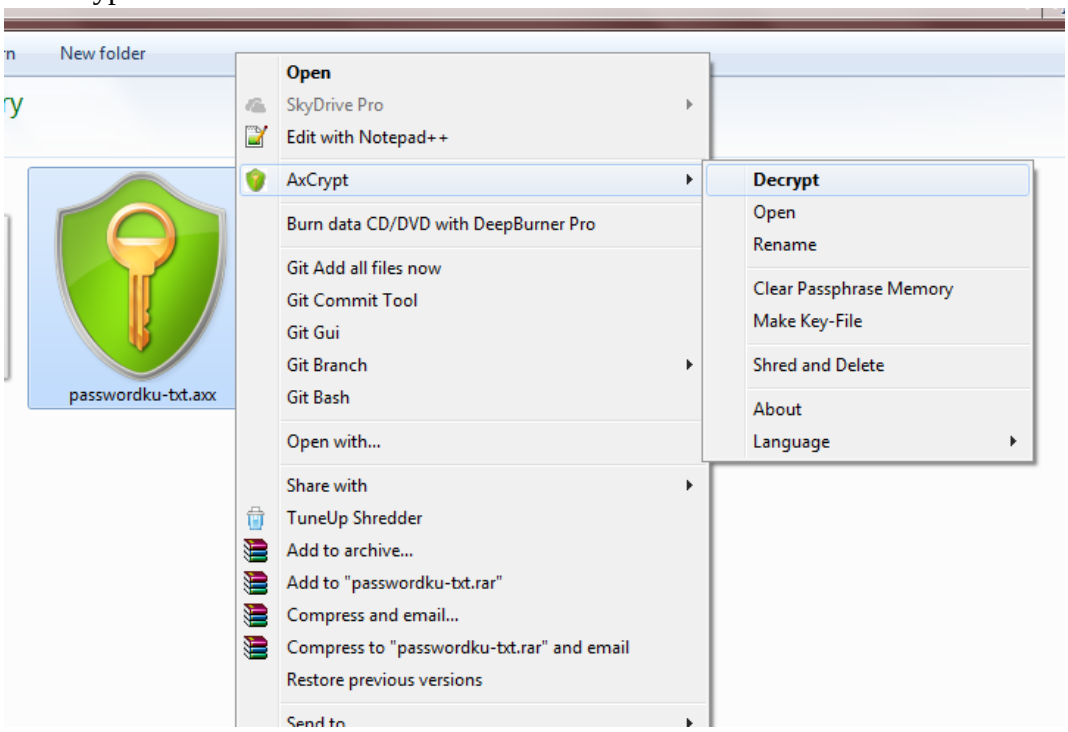
4. Setelah itu kita masukkan password untuk mengenkripsi file tersebut, dan key-filenya kita isikan dengan kunci.bmp, setelah itu klik OK



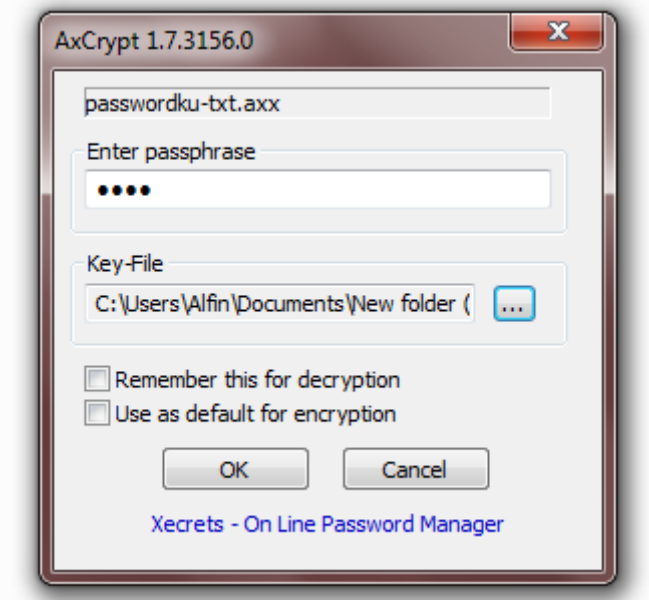
5. Setelah itu file password.txt akan berubah extensinya menjadi .axx yang telah dilindungi oleh aplikasi Axcrypt, dan ketika kita ingin membuka file tersebut akan dimintai password dan file kunci



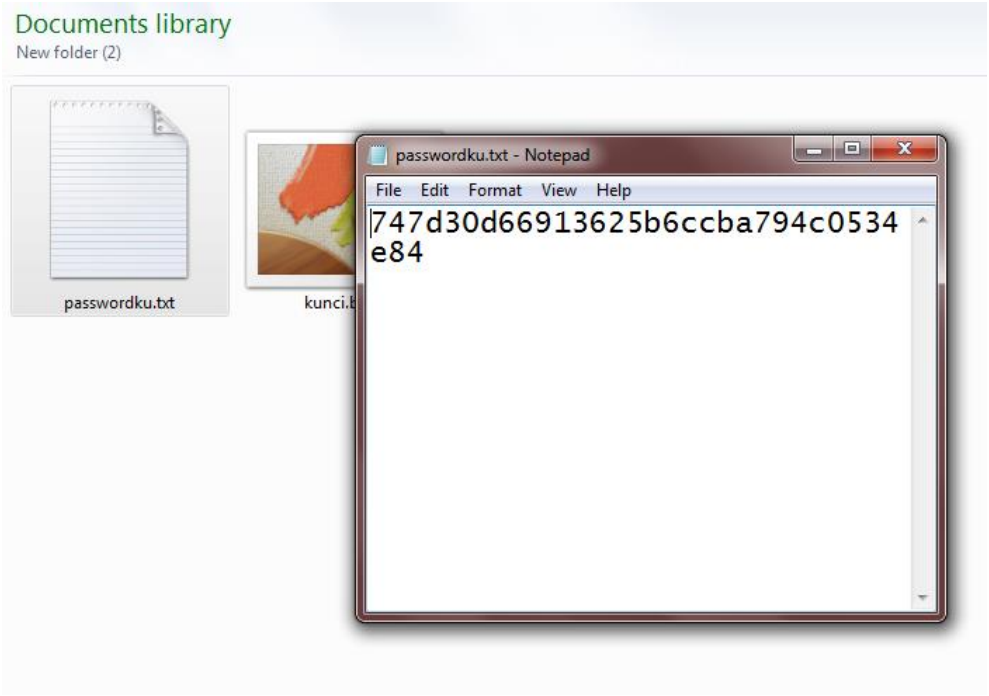
6. Untuk mendecrypt fle tersebut, klik kanan file passwordku-txt.axx lalu pilih Axcrypt > Decrypt



7. Lalu kita masukkan password yang tadinya dibuat melindungi file tersebut beserta kunci.bmp sebagai file kuncinya, lalu OK



8. Setelah itu kita sukses mengembalikan file tersebut kedalam bentuk aslinya, dan untuk mendecrypt plain text yang telah dienkripsi didalam file passwordku.txt kita bisa menggunakan beberapa md5 decrypt di website www.md5decrypt.org



9. Langkah terakhir kita buka website www.md5decrypt.org untuk mendecrypt kata2 tersebut, dan kita akan mendapatkan isi password tersebut.

Enter your Text Here

747d30d66913625b6ccba794c0534e84

MD5 Decrypt

search on 23+ websites

MD5 Encrypt

md4

crypt

sha1

More >

Get your Code Here

abdusajaaa