1) telekomunikasi dan Keamanan jaringan

telekomunikasi dan keamanan jaringan pada saat ini adalah dasar bagi kehidupan manusia di era modern ini.

Banyak teknologi yang mengandalkan keamanan jaringan semisal seperti internet,online banking , e-mail dan lainnya. Karena semua ini berfokus pada satu kerahasiaan dan integritas, dan ketersediaan data dalam gerak.

Arsiteksur jaringan dan design

Dalam arsitektur jaringan dan desain yang di bahas adalah bagaimana jaringan itu harus di rancang dengantepat dan benar dengan mengandalakan keamanan dan menyediakan pendekatan dalam bentuk modular fungsional pada desain sebuah jaringan.

Konsep dasar jaringan.

Sebelum kita mulai membahas ytelekomunikasi secara spesifik kita perlu mengetahui bahwa di belakang mereka terdapat istilah seperti broadband yang sering di gunakan secara informal dan pada hal ini kita memerlukan pemahaman yang tepat dari terminology keamanan informasi.

Contohnya adalah

-Simplex, half-duplex, and full-duplex communication

-lan, wan , man

-internet, intranet, dan extranet

Model OSI

Model OSI adalah suatu dekripsi abstrak mengenai desain lapisan-lapisan komunikasi dan protokol jaringan komputer yang dikembangkan sebagai bagian dari inisiatif Open Systems Interconnection (OSI). Model ini disebut juga dengan model “Tujuh lapisan OSI” (OSI seven layer model).

Dalam osi model di bagi menjadi beberapa lapisan layer seperti berikut

1.lapisan fisik (physical layer)

2. lapisan koneksi data (data link layer)

3. lapisan jaringan (network layer)

4. lapisan transport (transport layer)

5. lapisan sesi (session layer)

6. lapisan presentasi (presentation layer)

7. lapisan aplikasi (application layer)

Model TCP/IP (transmission control protocol / internet protocol merupakan model jaringan yang di buat oleh AS Defense Advanced Research Projects Agency pada tahun 1970-an. Model dari TCP/IP lebih sederhana dari model OSI . TCP / IP sebenranya merupakan suite protocol termasuk UDP dan ICMP , di antara banyak lainnya seperti ;

1. Network acces layer
2. Internet layer
3. Host-to-host transpot layer
4. Appkication layer

MAC Address *(Media Access Control Address)* adalah sebuah alamat jaringan yang diimplementasikan pada lapisan data-link dalam tujuh lapisan model OSI, yang merepresentasikan sebuah node tertentu dalam jaringan. Dalam sebuah jaringan berbasis Ethernet, **MAC address** merupakan alamat yang unik yang memiliki panjang 48-bit (6 byte) yang mengidentifikasikan sebuah komputer, interface dalam sebuah router, atau node lainnya dalam jaringan. **MAC Address** juga sering disebut sebagai *Ethernet address, physical address, atau hardware address.*

PERANGKAT DAN PROTOKOL JARINGAN

Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya. Pada tingkatan yang terendah, protokol mendefinisikan koneksi perangkat keras. Protocol digunakan untuk menentukan jenis layanan yang akan dilakukan pada internet.

Protokol TCP/IP dikembangkan pada akhir dekade 1970-an hingga awal 1980-an sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas (WAN). TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme transport jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (IP Address) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di Internet. Protokol ini juga bersifat routable yang berarti protokol ini cocok untuk menghubungkan sistem-sistem berbeda (seperti Microsoft Windows dan keluarga UNIX) untuk membentuk jaringan yang heterogen.

Domain Name System (DNS) adalah distribute database system yang digunakan untuk pencarian nama komputer (name resolution) di jaringan yang mengunakan TCP/IP (Transmission Control Protocol/Internet Protocol)
Point-to-Point Protocol (sering disingkat menjadi PPP) adalah sebuah protokol enkapsulasi paket jaringan yang banyak digunakan pada wide area network (WAN).

ICMP berbeda tujuan dengan TCP dan UDP dalam hal ICMP tidak digunakan secara langsung oleh aplikasi jaringan milik pengguna. salah satu pengecualian adalah aplikasi ping yang mengirim pesan ICMP Echo Request (dan menerima Echo Reply) untuk menentukan apakah komputer tujuan dapat dijangkau dan berapa lama paket yang dikirimkan dibalas oleh komputer tujuan.

HTTP (Hypertext Transfer Protocol) suatu protokol yang digunakan oleh WWW (World Wide Web). HTTP mendefinisikan bagaimana suatu pesan bisa diformat dan dikirimkan dari server ke client. HTTP juga mengatur aksi-aksi apa saja yang harus dilakukan oleh web server dan juga web browser sebagai respon atas perintah-perintah yang ada pada protokol HTTP ini.

HTTPS adalah versi aman dari HTTP, protokol komunikasi dari World Wide Web. Ditemukan oleh Netscape Communications Corporation untuk menyediakan autentikasi dan komunikasi tersandi dan penggunaan dalam komersi elektris. Selain menggunakan komunikasi plain text, HTTPS menyandikan data sesi menggunakan protokol SSL (Secure Socket layer) atau protokol TLS (Transport

Layer Security). Kedua protokol tersebut memberikan perlindungan yang memadai dari serangan eavesdroppers, dan man in the middle attacks.

SSH adalah protocol jaringan yang memungkinkan pertukaran data secara aman antara dua komputer. SSH dapat digunakan untuk mengendalikan komputer dari jarak jauh mengirim file, membuat Tunnel yang terrenkripsi dan lain-lain. Protocol ini mempunyai kelebihan disbanding protocol yang sejenis seperti Telnet, FTP, Danrsh, karena SSH memiliki system Otentikasi,Otorisasi, dan ekripsinya sendiri.

Telnet Adalah sebuah protokol jaringan yang digunakan di koneksi Internet atau Local Area Network. TELNET dikembangkan pada 1969 dan distandarisasi sebagai IETF STD 8, salah satu standar Internet pertama. TELNET memiliki beberapa keterbatasan yang dianggap sebagai risiko keamanan.

SSL (Secure Socket Layer) adalah arguably internet yang paling banyak digunakan untuk enkripsi. Ditambah lagi, SSL sigunakan tidak hanya keamanan koneksi web, tetapi untuk berbagai aplikasi yang memerlukan enkripsi jaringan end-to-end.

Nama : MOHAMMAD MAWARDI
NIM: 1310651175

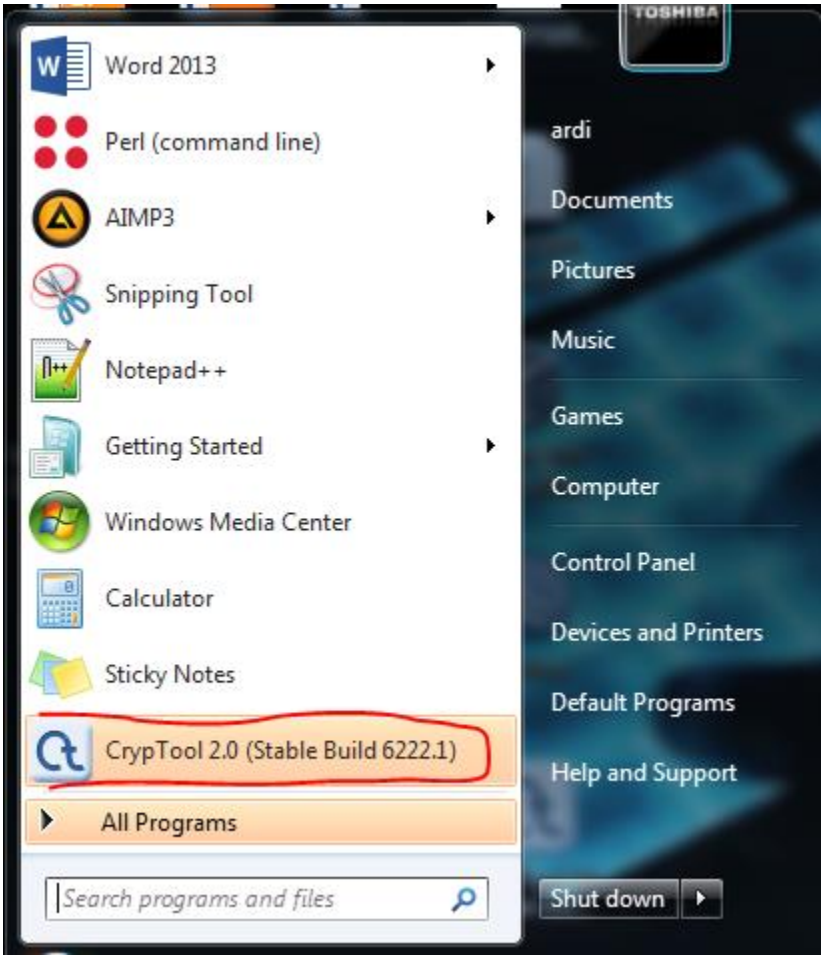
2) Cara mengaplikasikan CrypTool

Di sini saya akan memberitahu bagaimana cara merubah suatu kata sehingga menjadi kode rahasia semacam morse menggunakan aplikasi cryptool.

Mula mula kita harus menginstall aplikasi cryptoll terlebih dahulu.kita ikuti langkah penginstalan step by step sesuai apa yang di instruksikan.

Setelah terinstall kita buka aplikasi cryptoll

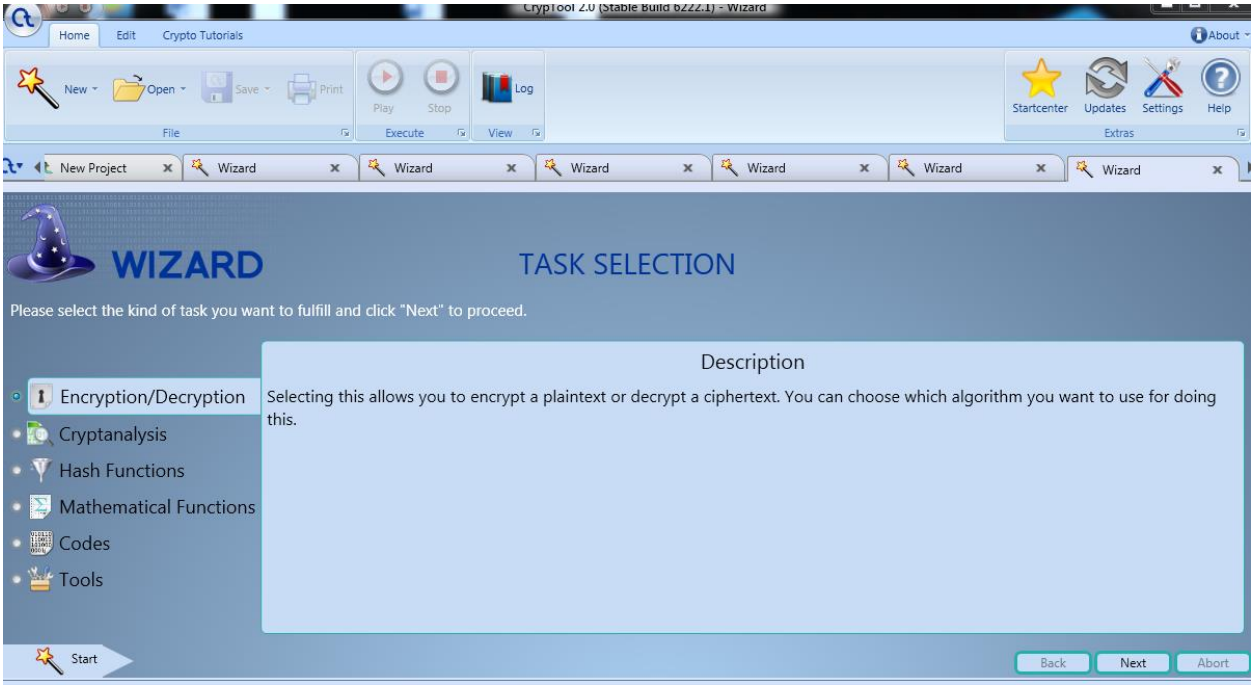
Klik tombol windows pada keyboard lalu klik aplikasi cryptoll



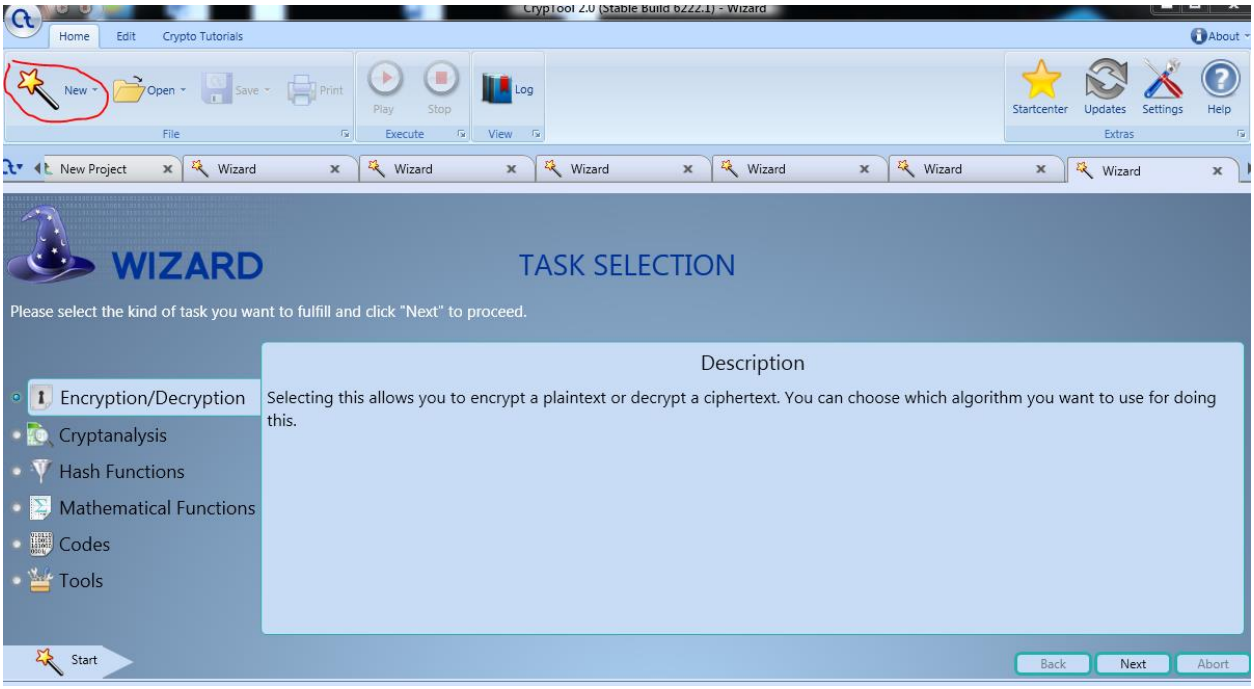
Nama : MOHAMMAD MAWARDI
NIM: 1310651175

KELAS : A
KEAMANAN INFORMASI

Setelah kita klik maka akan tampil seperti di bawah ini



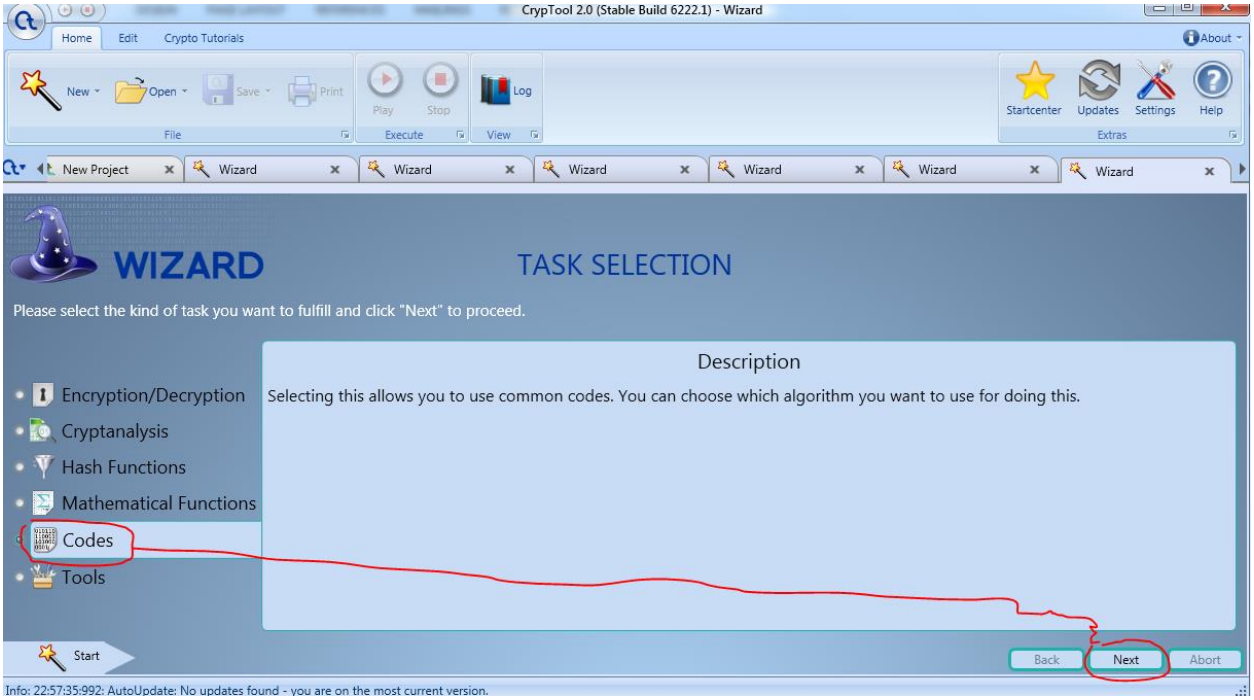
Setelah itu klik NEW seperti pada gambar di bawah



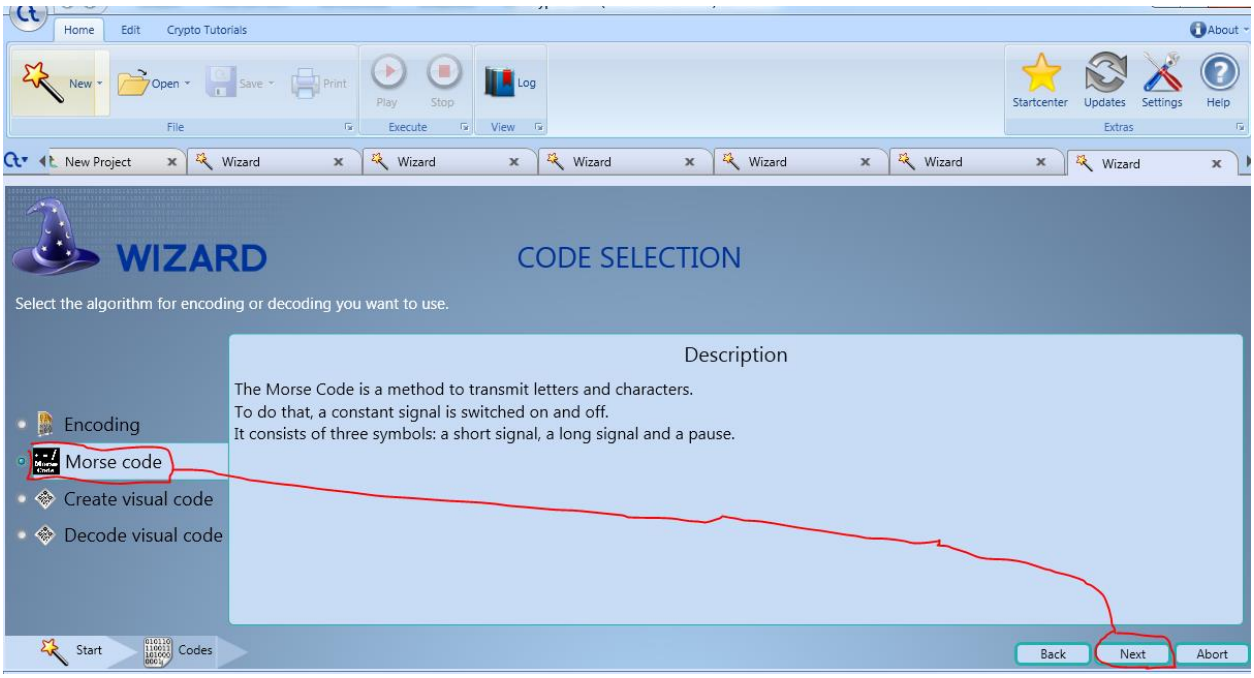
Nama : MOHAMMAD MAWARDI
NIM: 1310651175

KELAS : A
KEAMANAN INFORMASI

Setelah itu kita klik codes dan kemudian klik next seperti pada gambar



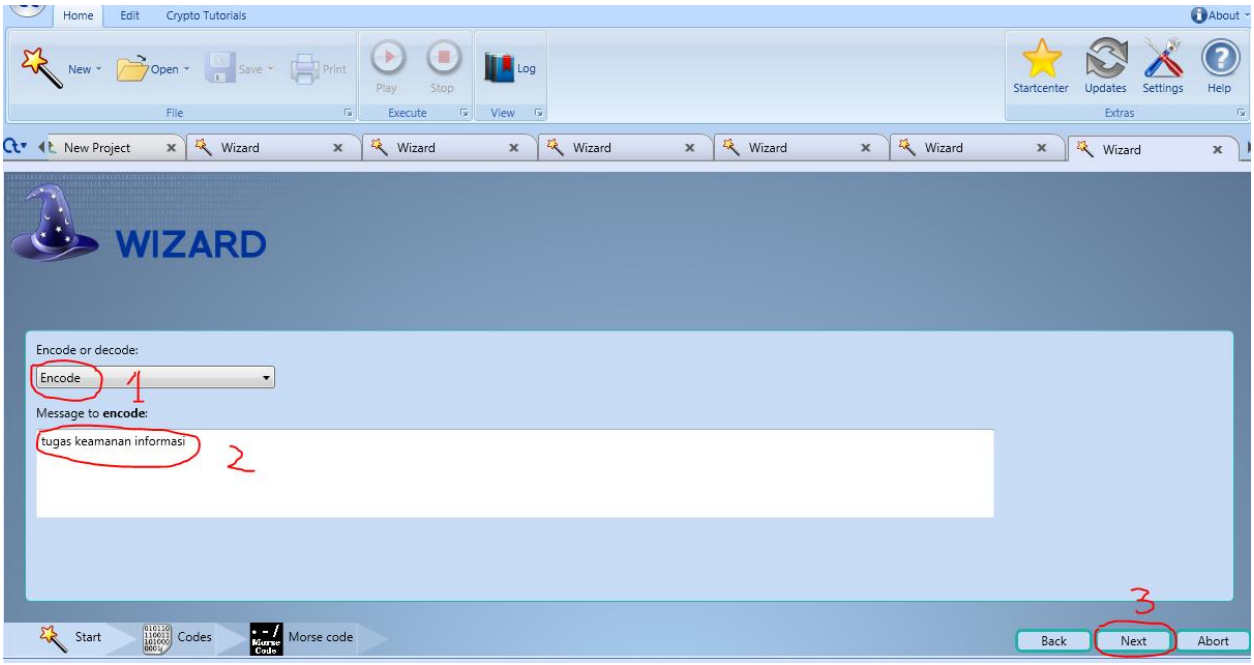
Setelah itu kita klik morse code kemudian klik next seperti pada gambar



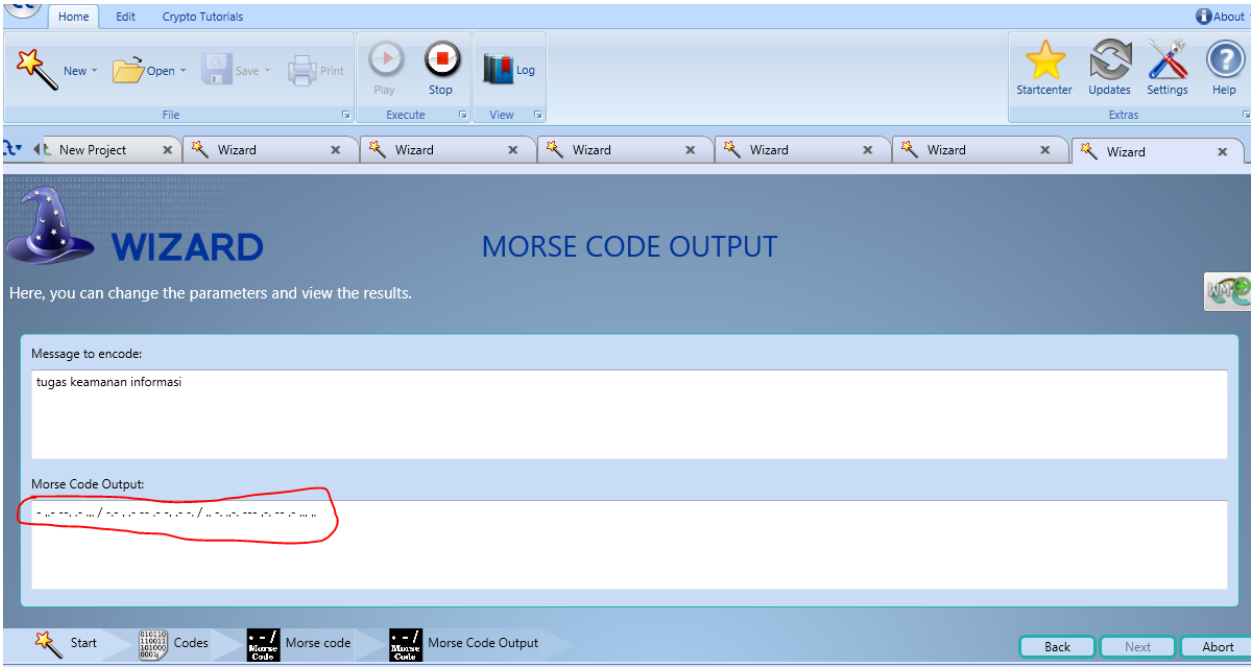
Nama : MOHAMMAD MAWARDI
NIM: 1310651175

KELAS : A
KEAMANAN INFORMASI

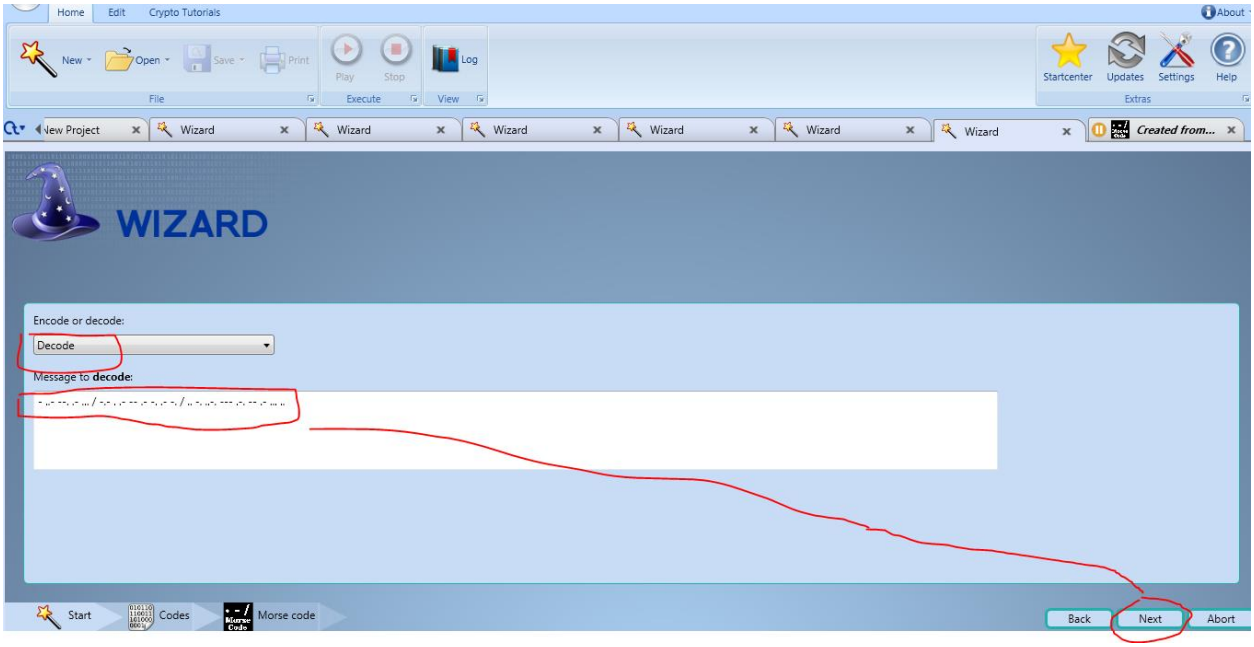
Kemudian 1.kita pilih encode dan ke 2. Kita masukkan kalimat yang akan kita rubah contoh " tugas keamanan informasi" dan ke 3. Kita klik next



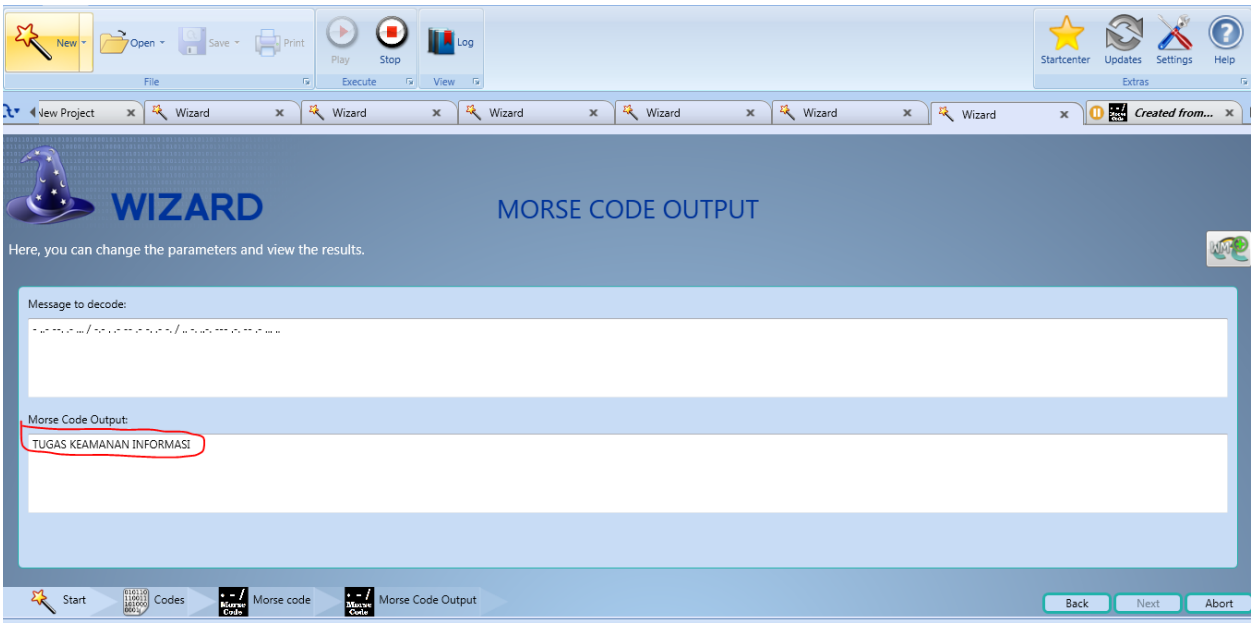
Maka setelah kita melakukan langkah di atas maka kalimat tugas keamanan informasi akan berubah menjadi code morse seperti pada gambar di bawah ini



Dan apabila kita menemukan suatu masalah yang mana menggunakan morse code maka jika kita ingin mengerti apa maksud dari morse code kita cukup memasukkan morse tersebut dan mengganti yang awalnya encode menjadi decode kemudian klik next



Maka akan muncul kalimat tugas keamanan informasi



SELESAI