

|| SESI 21 CRYPTOGRAPHY

DATAFILES

- CrypTool 2.1
- Mailvelope

PERSIAPAN

- Instalasi aplikasi Cryptool 2.1
- Aplikasi Cryptool 2.1 berjalan pada OS Windows
- Siapkan akun email gmail

SCENARIO

Melakukan Enkripsi dan Dekripsi menggunakan Algoritma Kriptografi tertentu

PROSEDUR

|| SESI 1 – Classic Cryptography

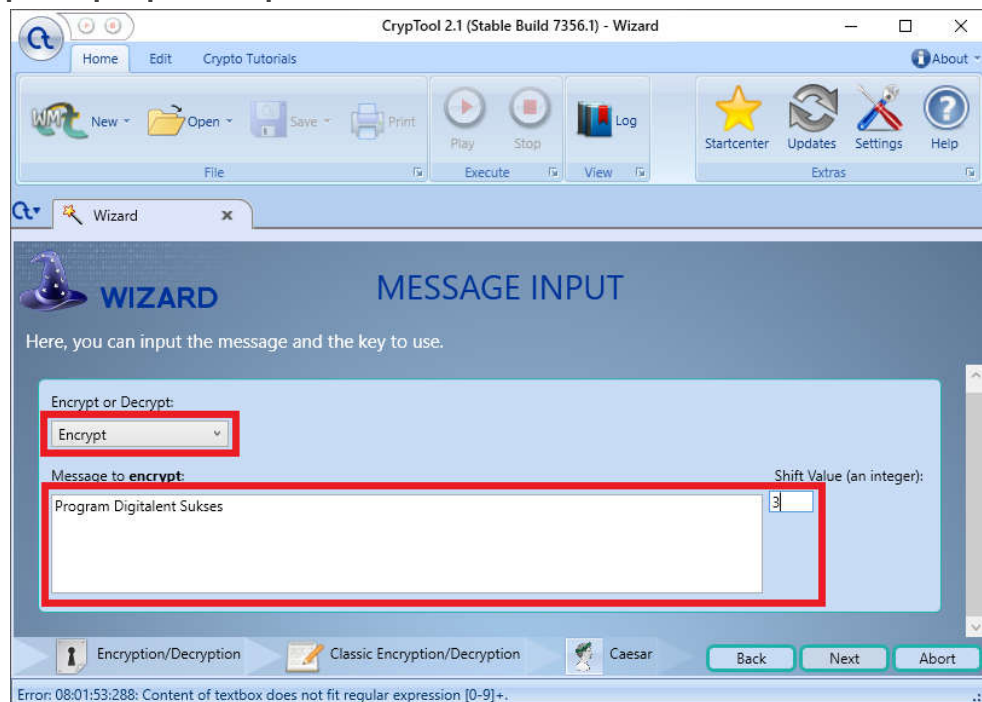
1. Caesar

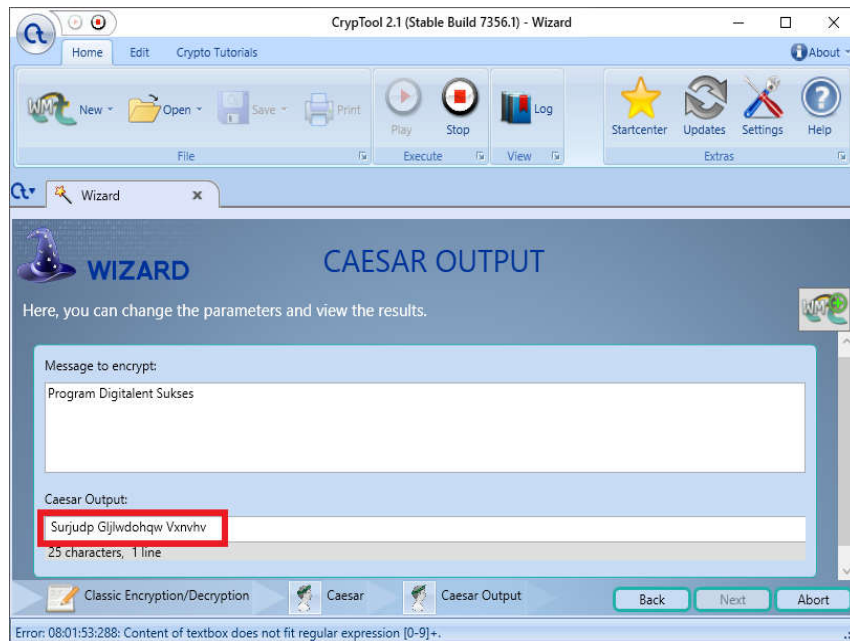
- **Encryption/Decryption > Classic > Caesar > Next**



- Langkah melakukan enkripsi pesan
 - Masukkan pesan yang akan dienkripsi
 - Tentukan kunci yang disepakati untuk mengenkripsi pesan

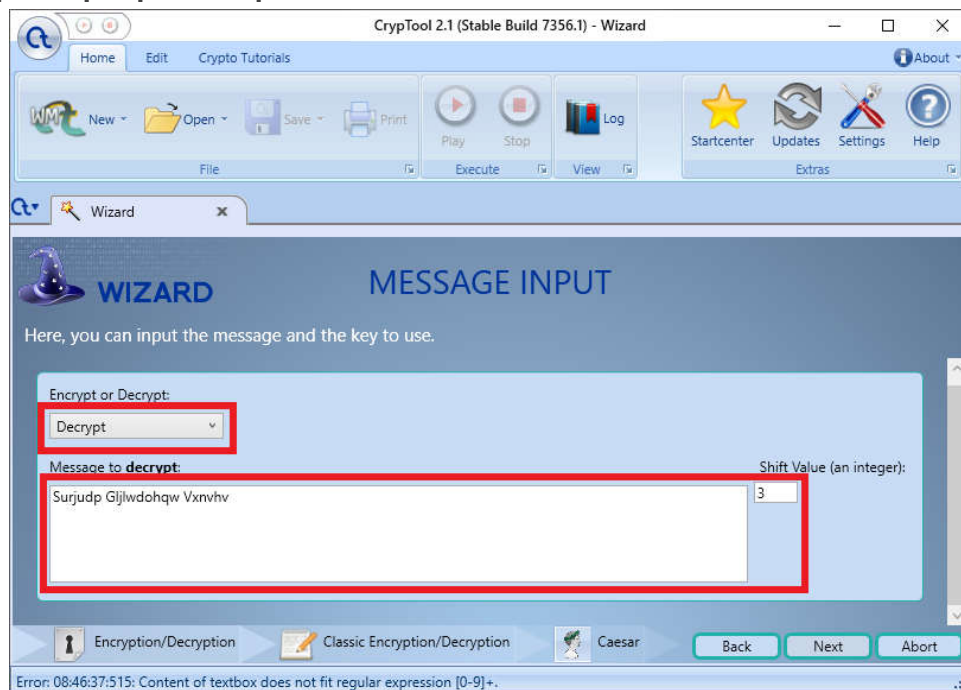
Encrypt > Input pesan > pilih shift value > Next

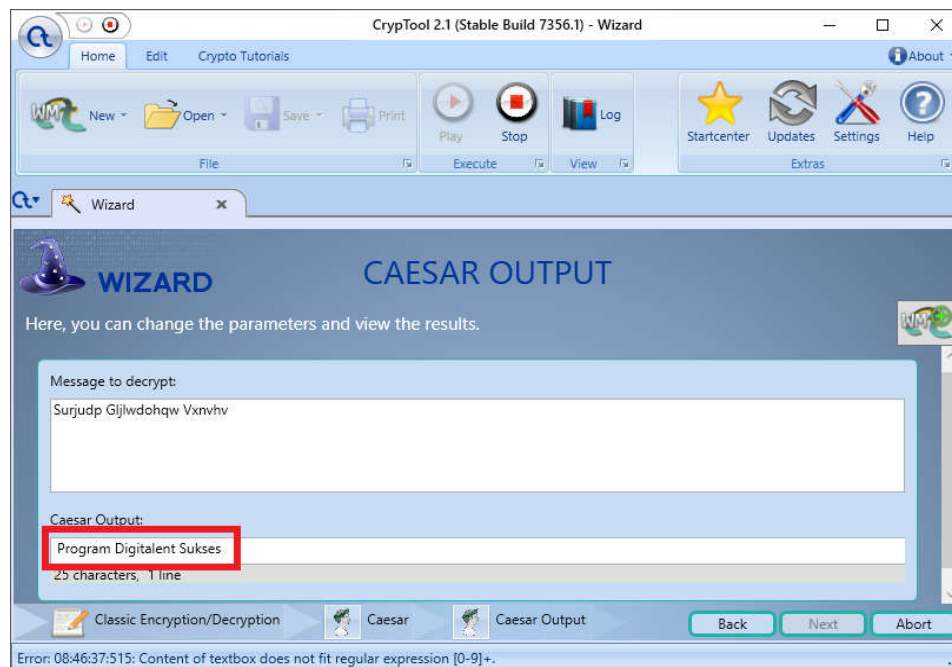




- Langkah melakukan dekripsi pesan
 - Input cipher teks yang diterima
 - Gunakan kunci yang telah disepakati untuk mendekripsi pesan

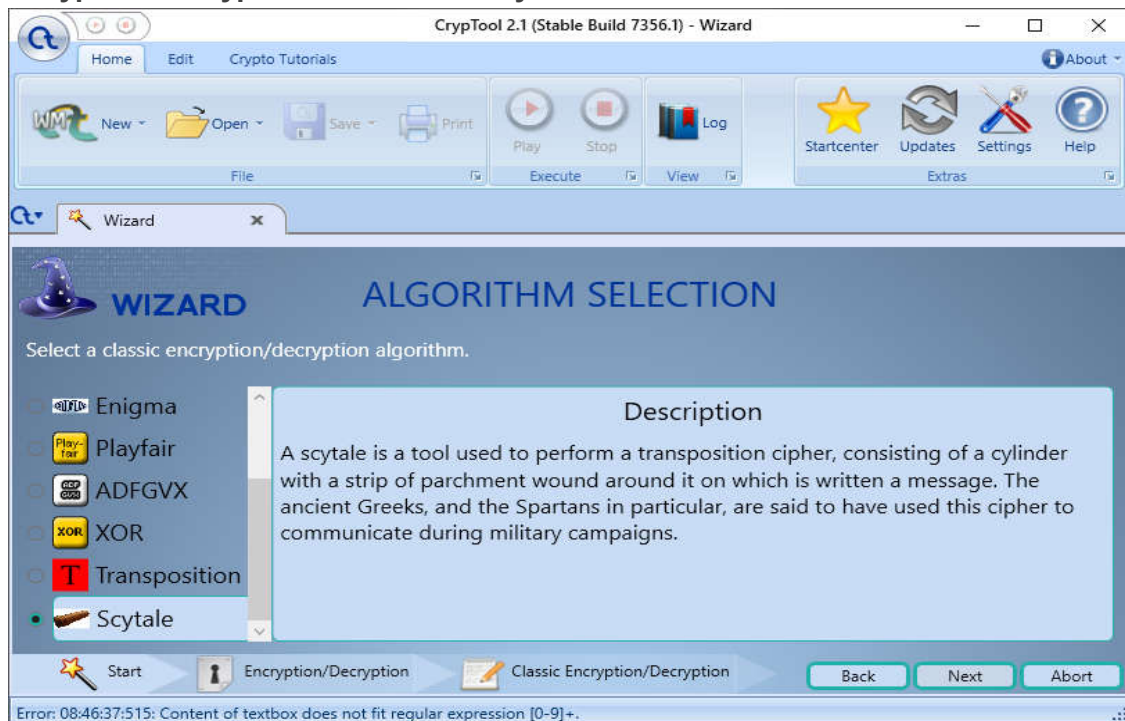
Decrypt > Input pesan > pilih shift value > Next





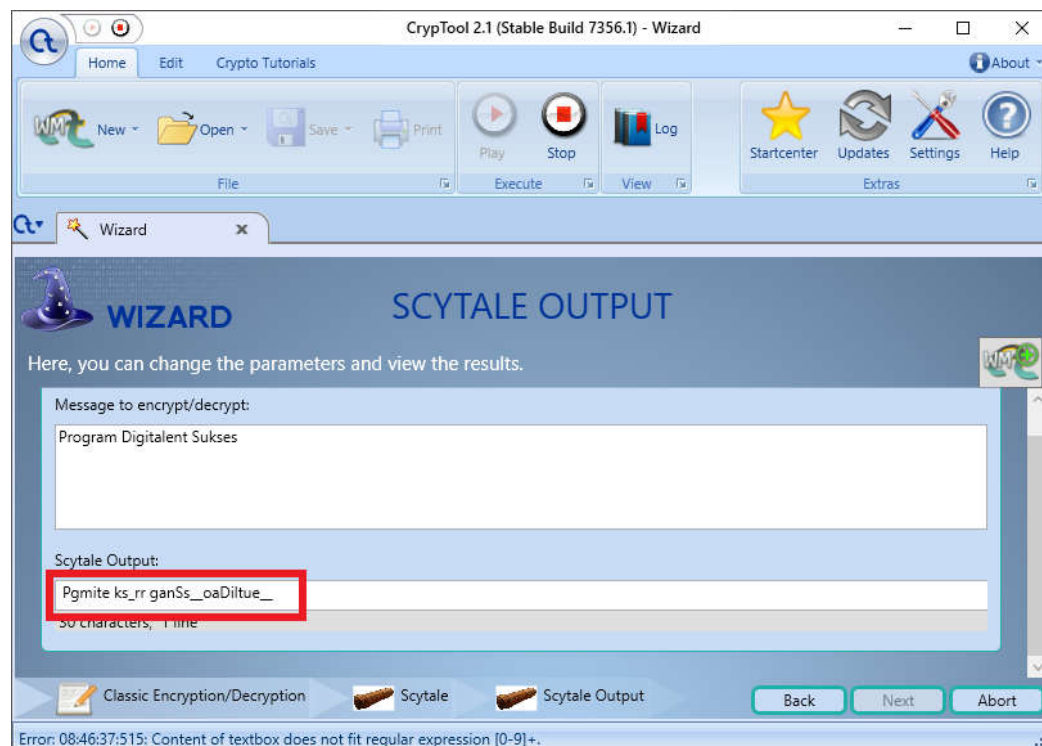
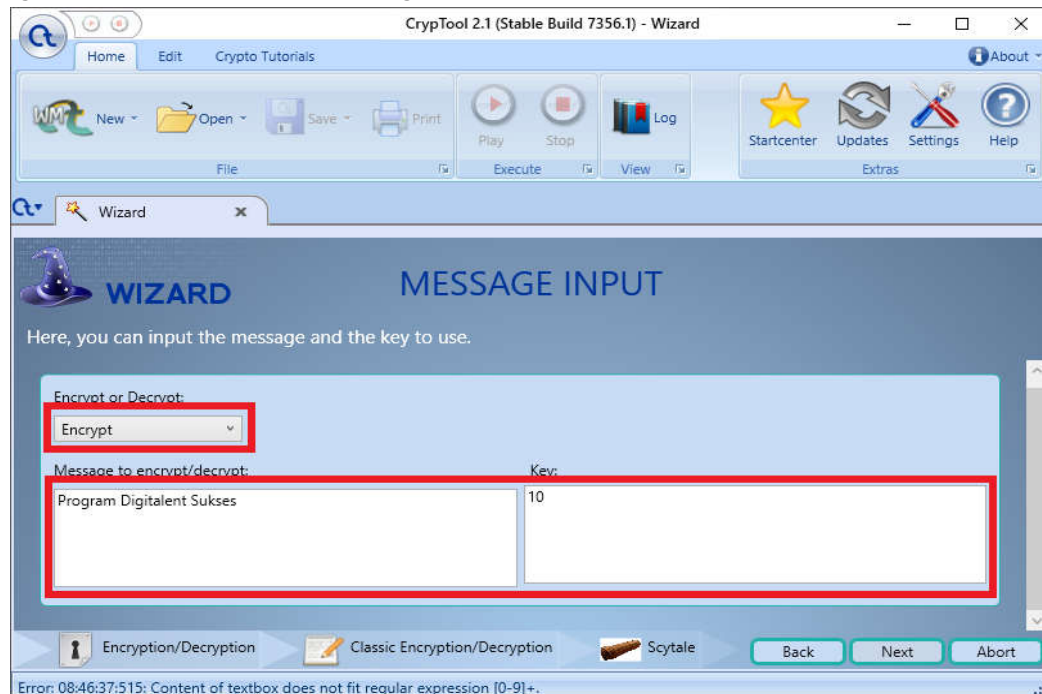
2. Scytale

- Encryption/Decryption > Classic > Skytale > Next



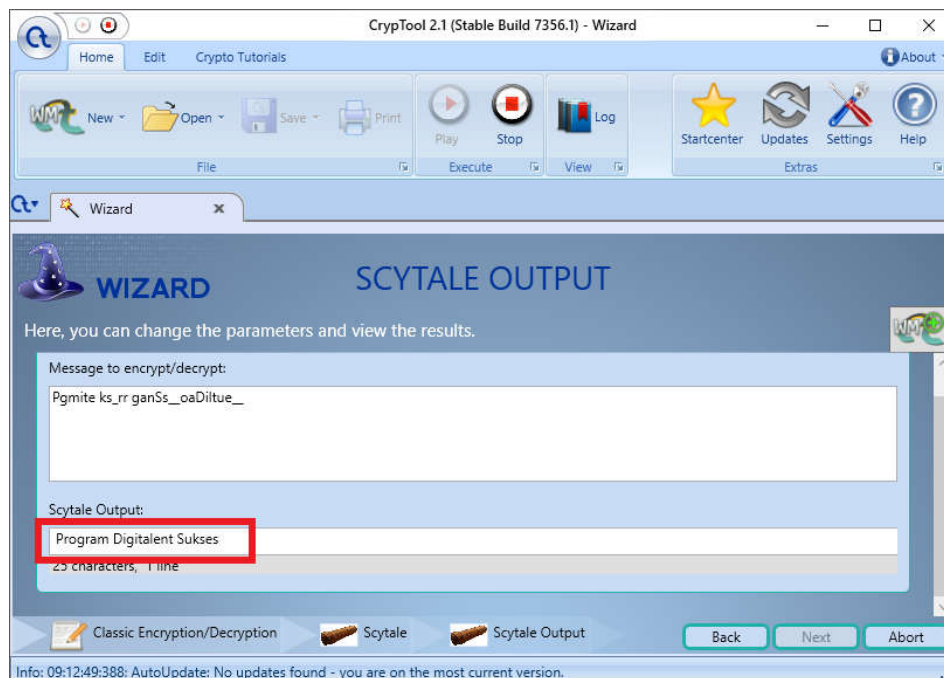
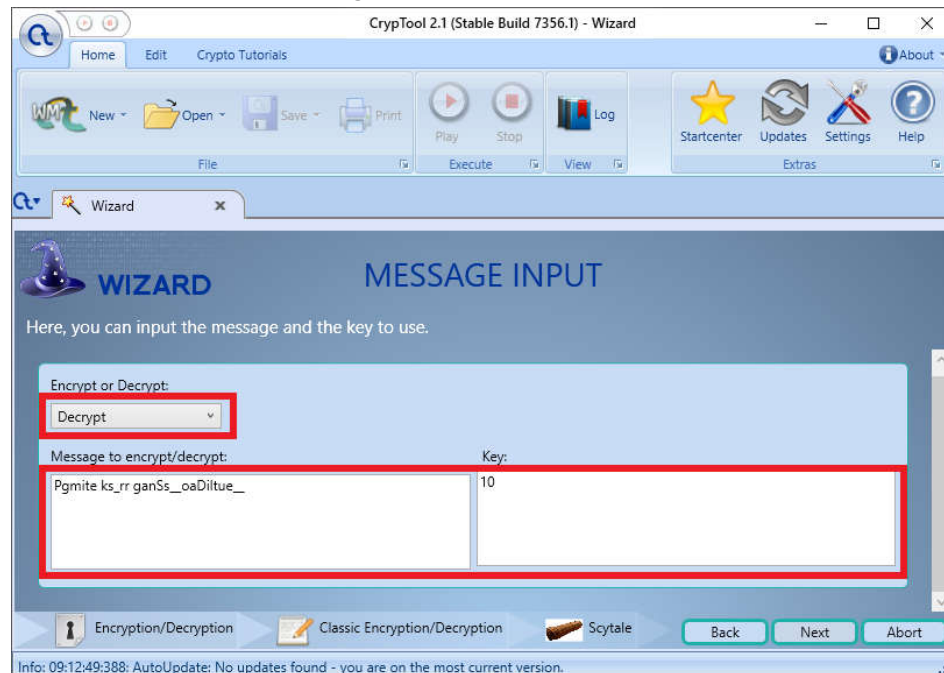
- Langkah melakukan enkripsi pesan
 - Masukkan pesan yang akan dienkripsi
 - Tentukan kunci (diameter silinder) yang disepakati untuk mengenkripsi pesan

Encrypt > Input pesan > pilih Key > Next



- Langkah melakukan dekripsi pesan
 - Masukkan cipherteks yang diterima
 - Gunakan kunci (diameter silinder) yang disepakati untuk mengenkripsi pesan

Decrypt > Input pesan > pilih Key > Next



3. Kesimpulan

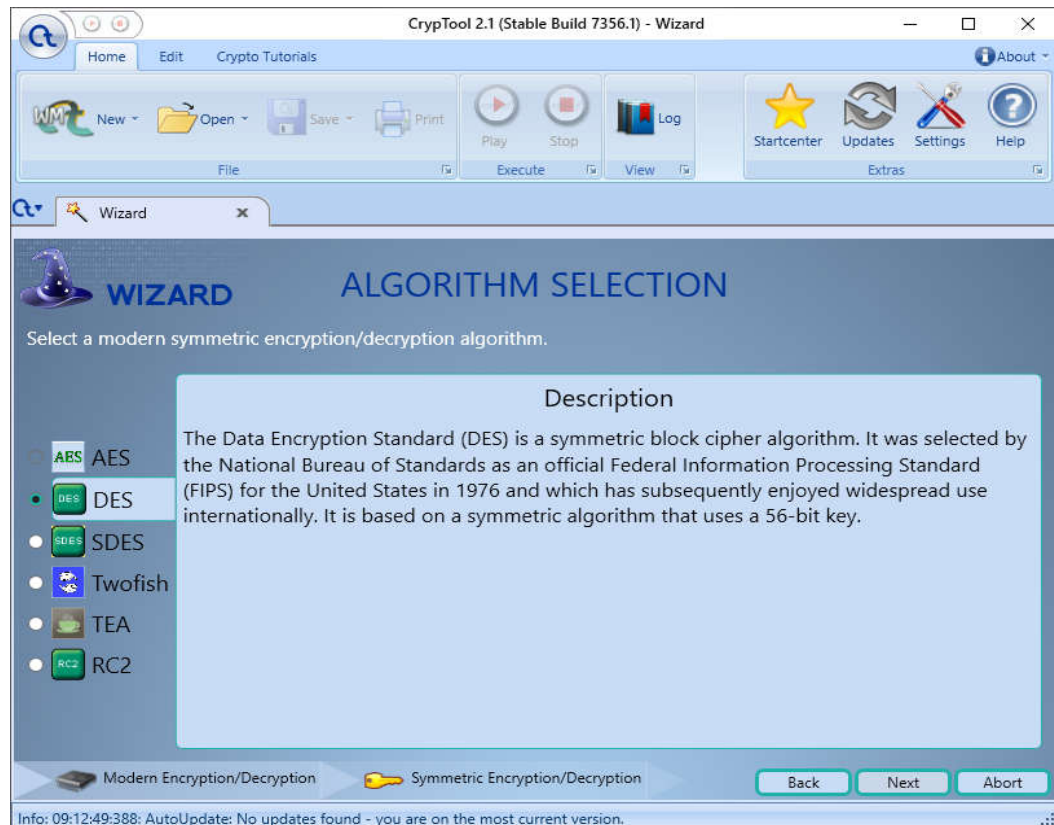
- Ilmu Kriptografi sudah ada sejak jaman dahulu
- Kriptografi digunakan untuk merahasiakan pesan
- Elemen utama dalam Kriptografi adalah **Kunci**

|| Sesi 2 – Modern Cryptography

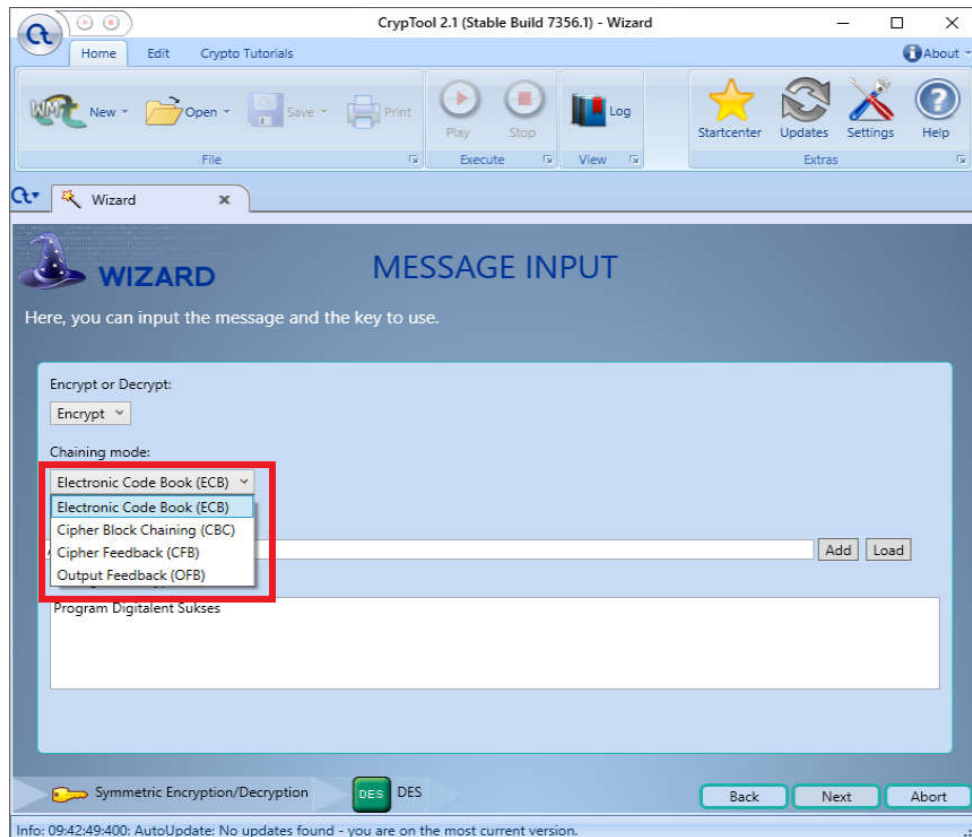
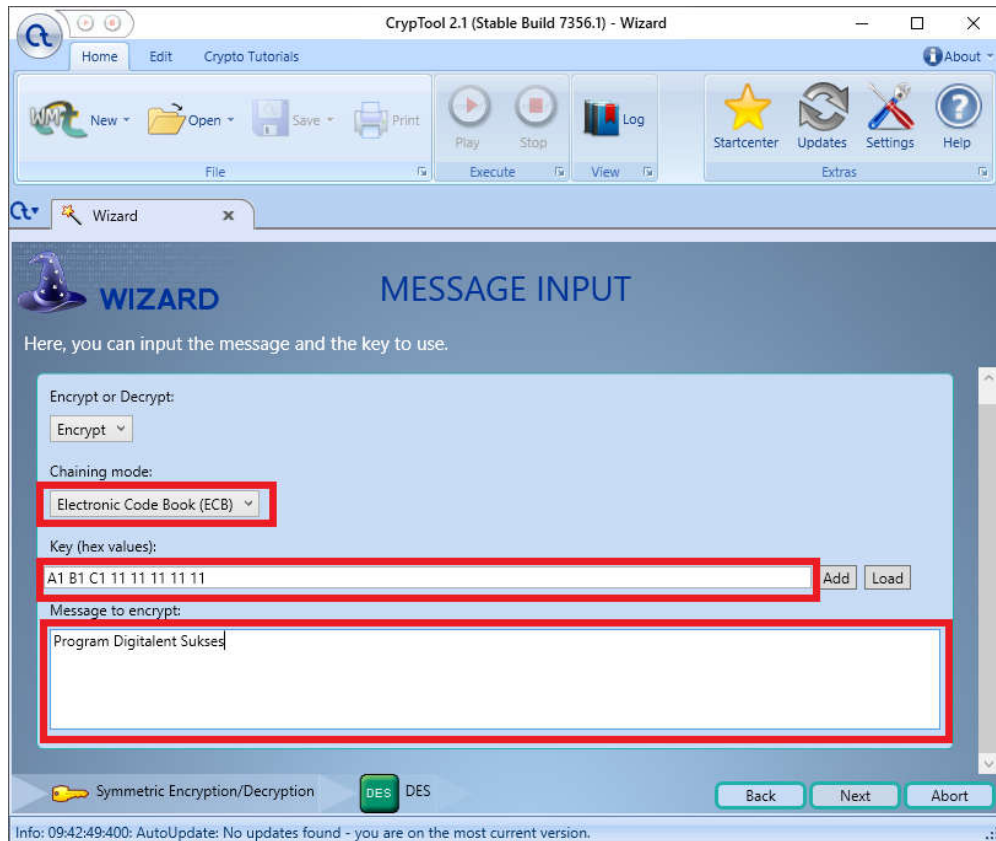
Symmetric Cryptography

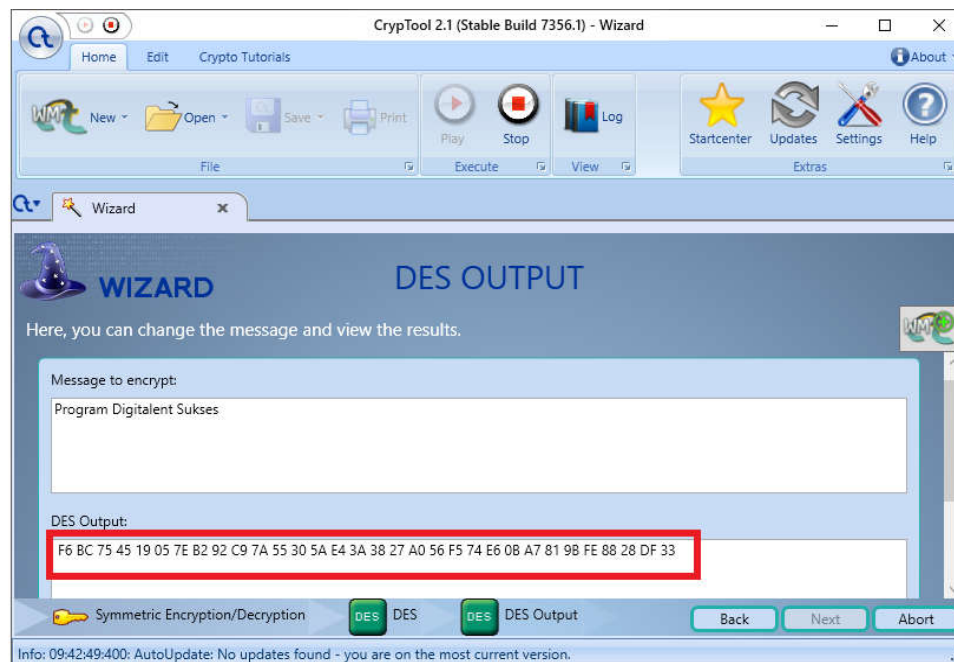
1. Data Encryption Standard (DES)

- Encryption/Decryption > Modern > Symetric > DES > Next

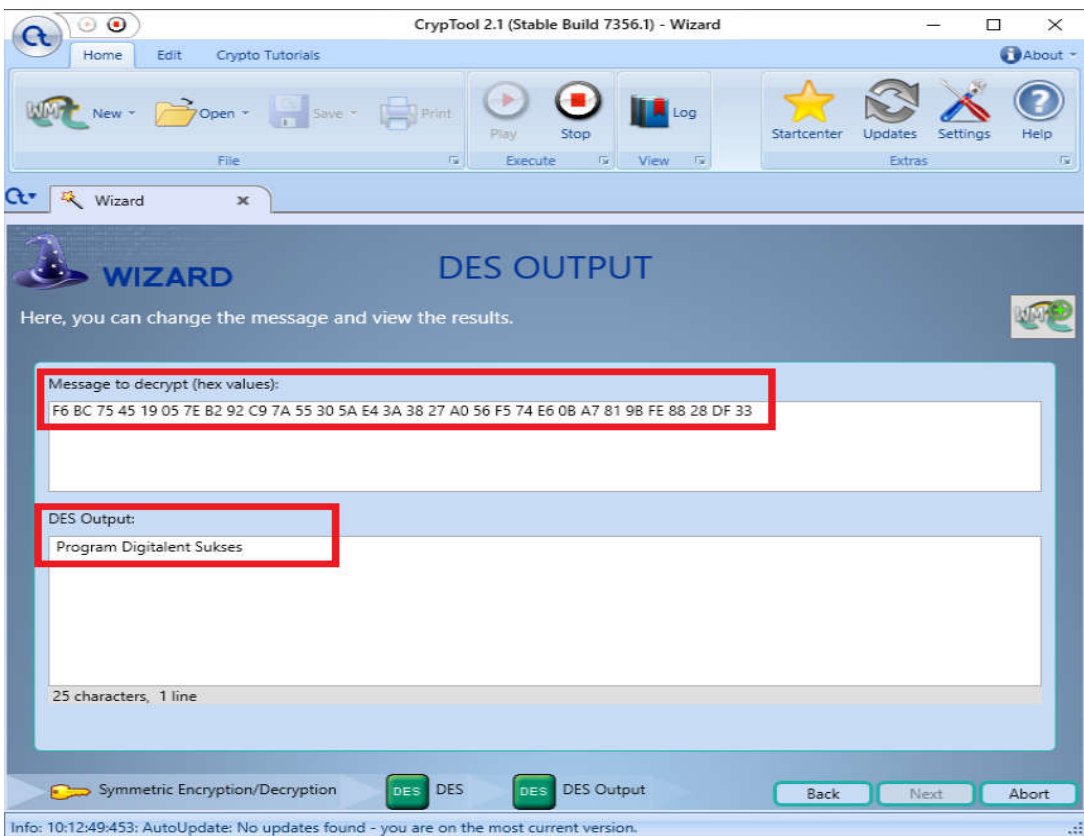
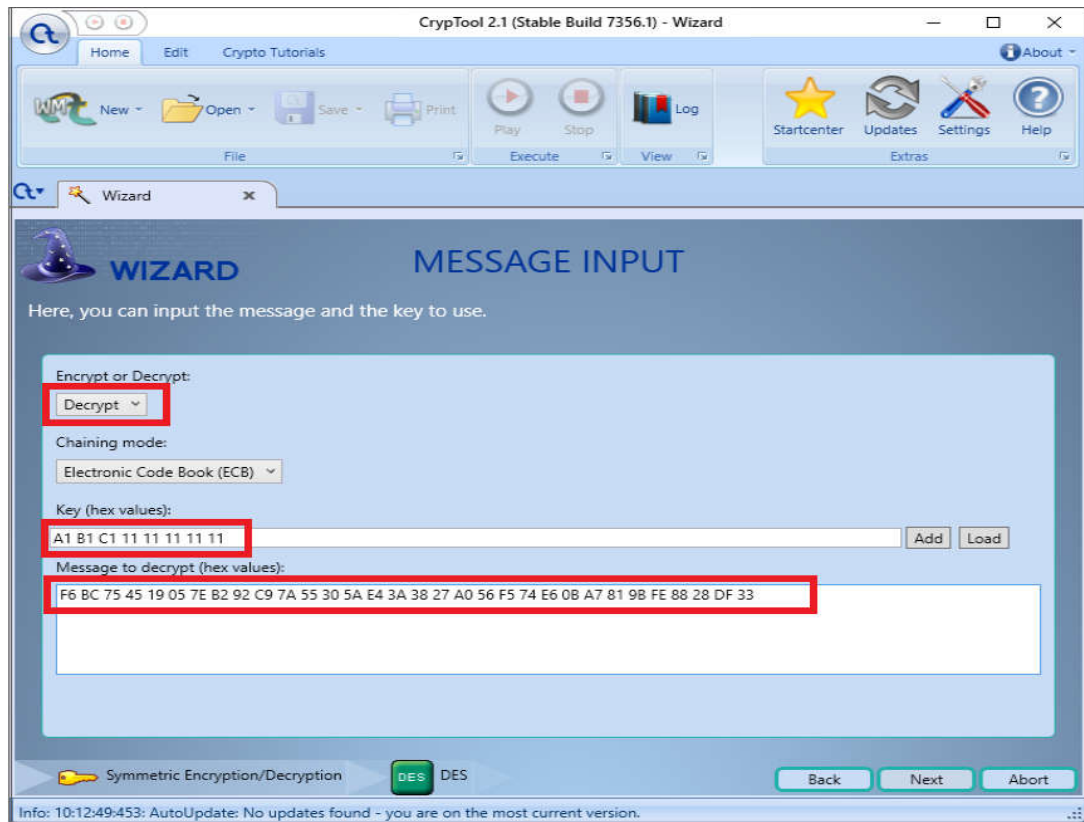


- Langkah melakukan enkripsi pesan
Dalam melakukan enkripsi menggunakan DES harus menentukan beberapa parameter yang digunakan yaitu:
 - Kunci dekripsi
Kunci enkripsi DES 64 bit (16 karakter heksa)
 - Mode operasi
Mode operasi **ECB, CBC, CFB, OFB****Kunci dan cipherteks** yang digunakan pada aplikasi cryptool dalam **format heksadesimal**



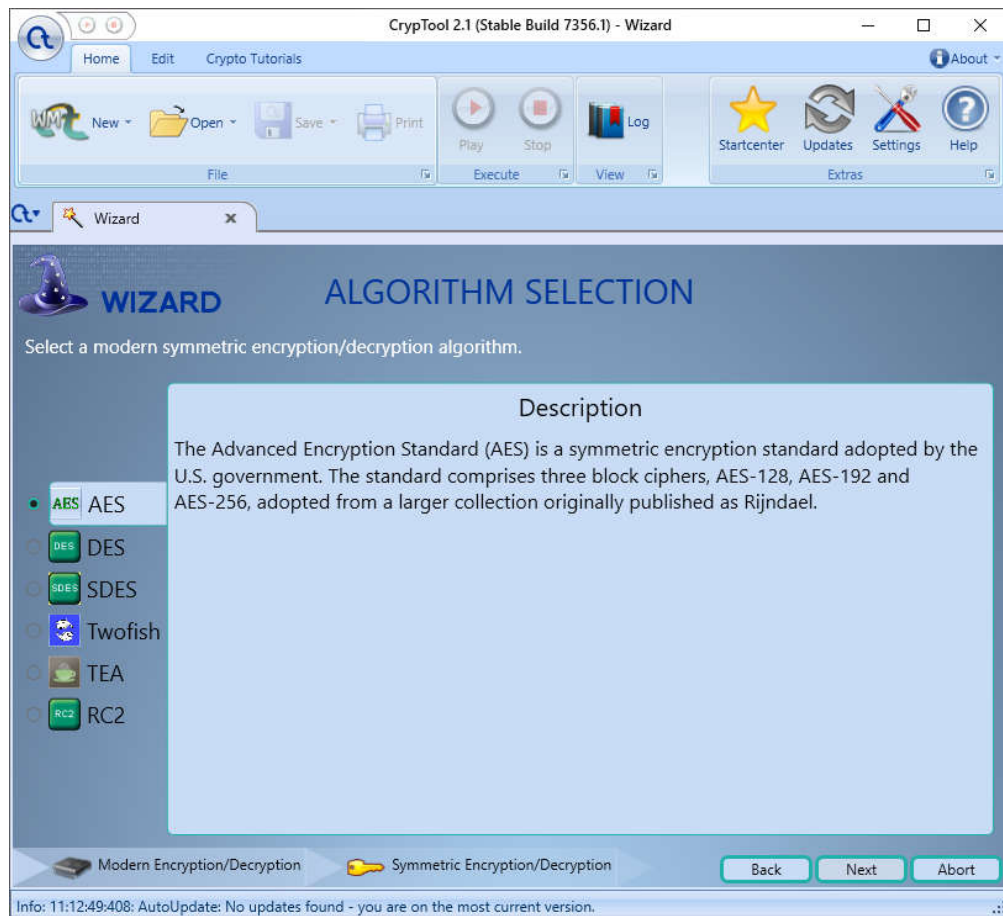


- Langkah melakukan dekripsi pesan
Dalam melakukan enkripsi menggunakan DES harus menentukan beberapa parameter yang digunakan yaitu:
 - Kunci dekripsi
Kunci dekripsi DES 64 bit
 - Mode operasi
Mode operasi **ECB, CBC, CFB, OFB**

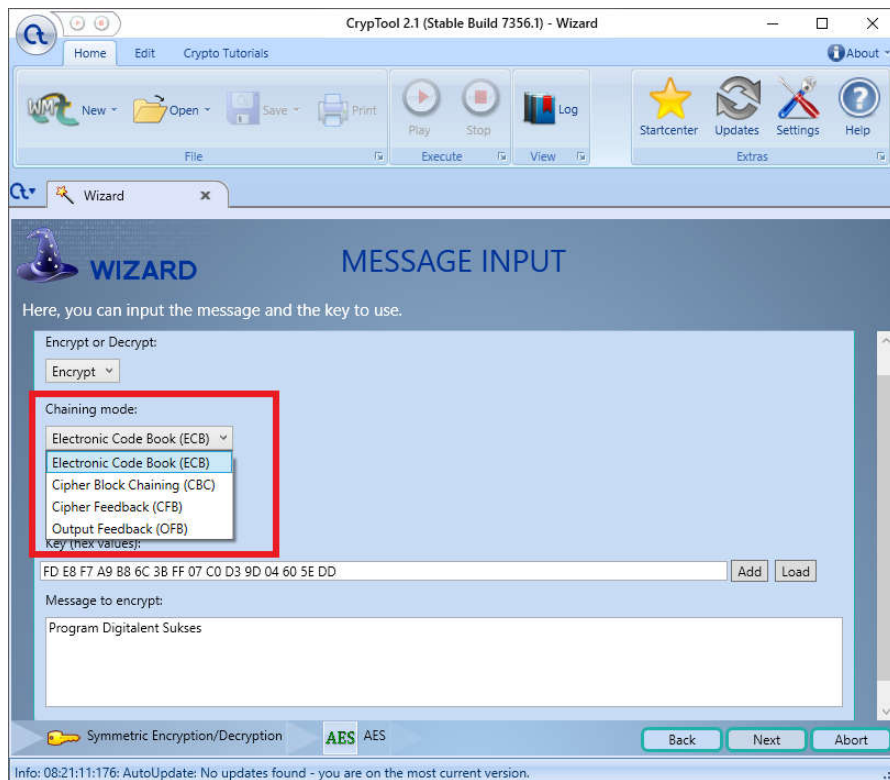
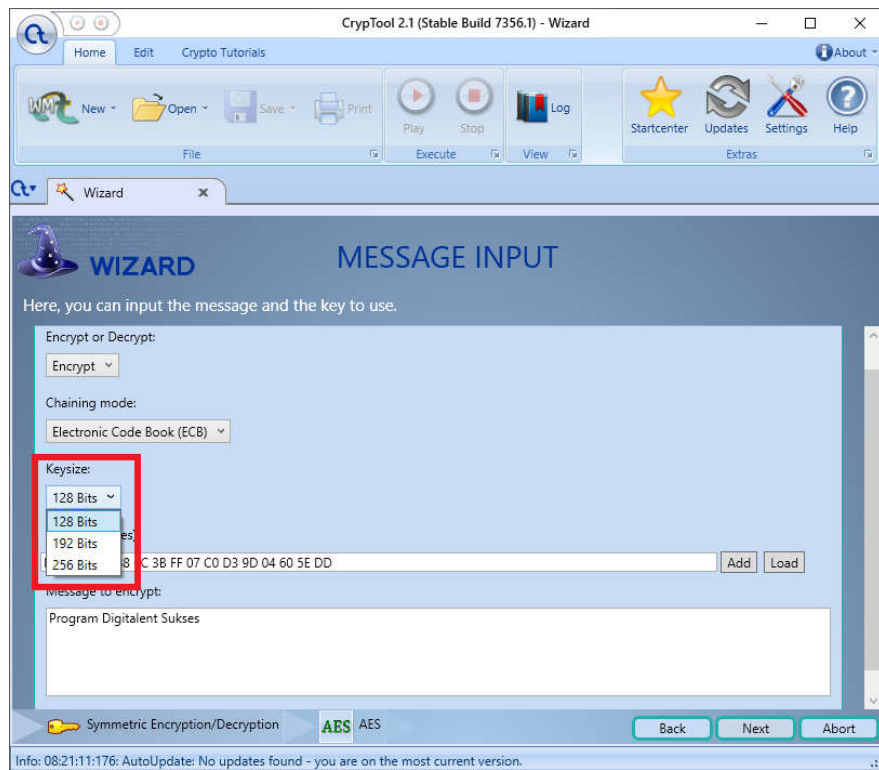


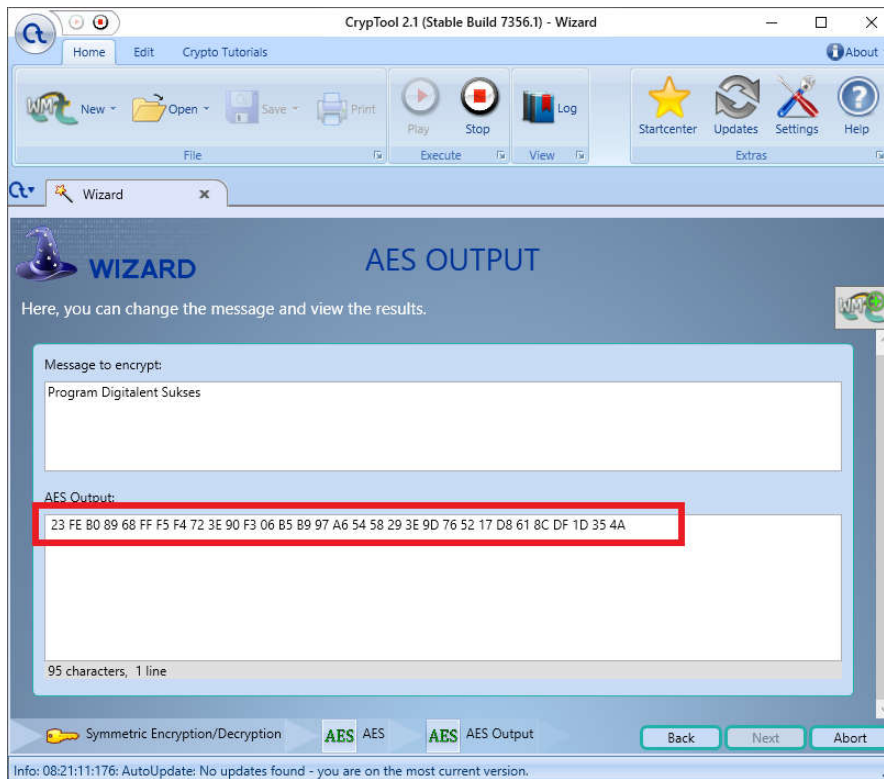
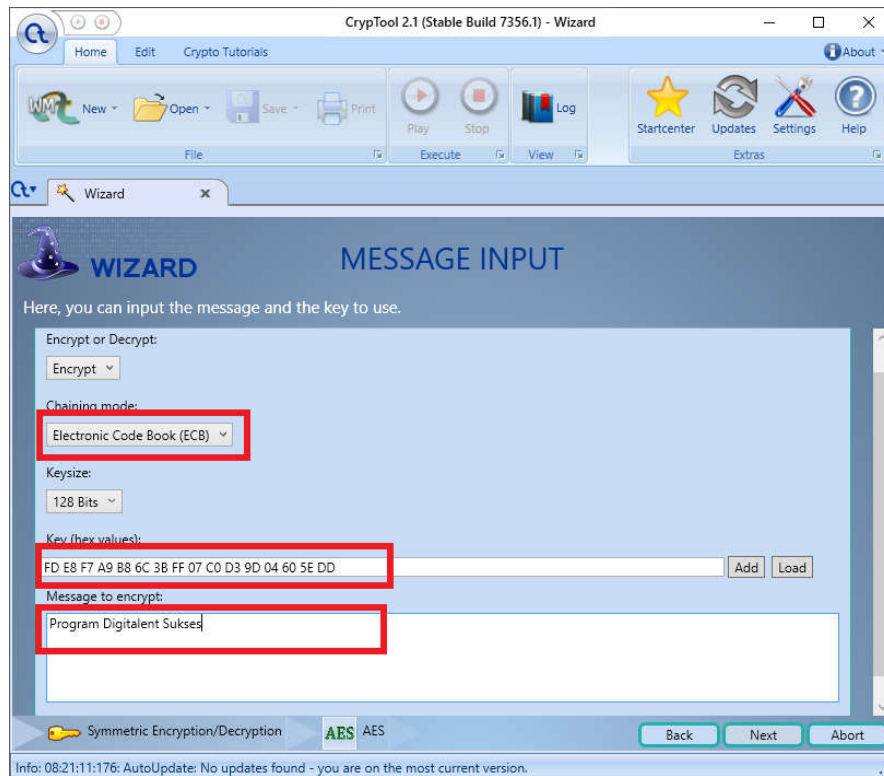
2. Advanced Encryption Standard (AES)

- Encryption/Decryption > Modern > Symetric > AES > Next

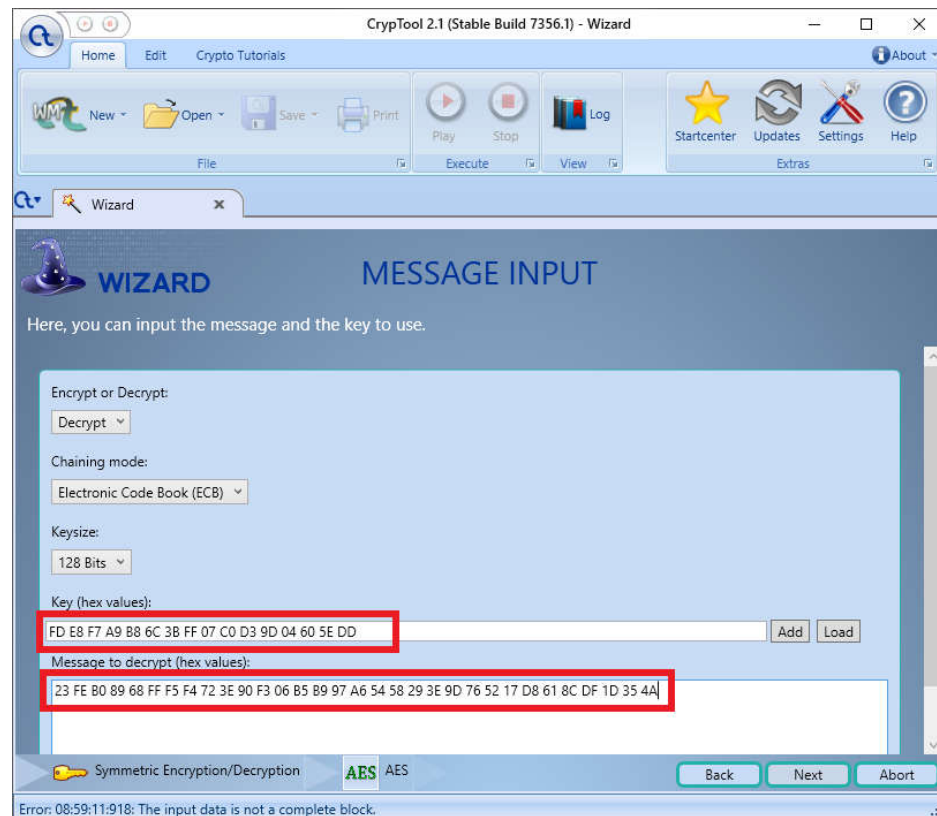


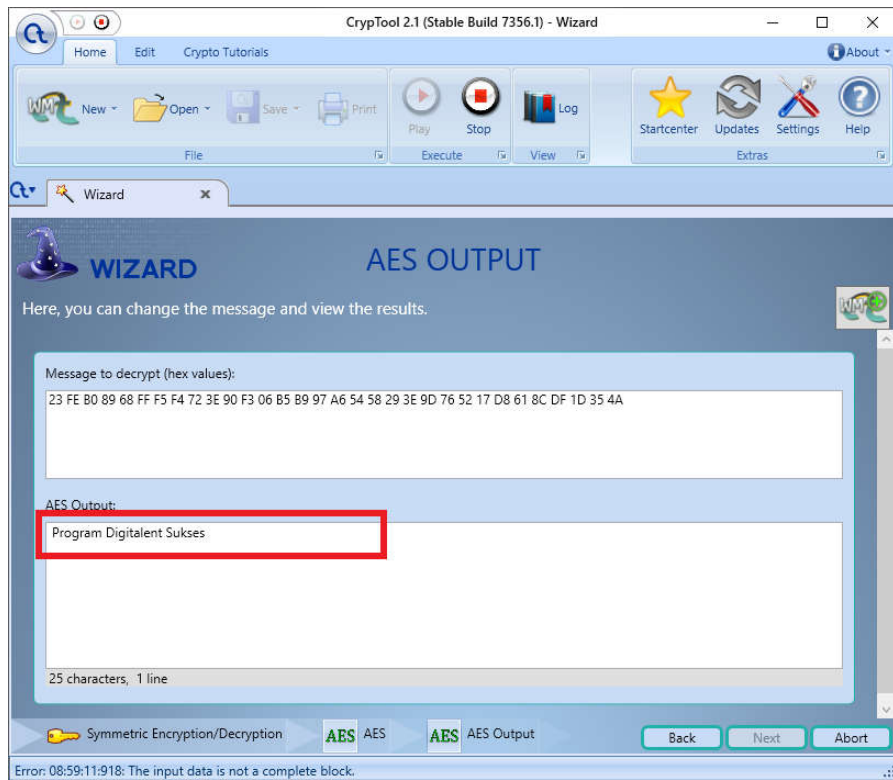
- Langkah melakukan enkripsi pesan
Dalam melakukan enkripsi menggunakan DES harus menentukan beberapa parameter yang digunakan yaitu:
 - Kunci enkripsi
Kunci enkripsi AES terdiri dari 3 variasi yaitu **128, 192, 256**
 - Mode operasi
Mode operasi **ECB, CBC, CFB, OFB****Kunci dan cipherteks** yang digunakan pada aplikasi cryptool dalam **format heksadesimal**





- Langkah melakukan dekripsi pesan
Dalam melakukan dekripsi menggunakan DES harus menentukan beberapa parameter yang digunakan yaitu:
 - Kunci dekripsi
Kunci dekripsi AES terdiri dari 3 variasi yaitu **128, 192, 256**
 - Mode operasi
Mode operasi **ECB, CBC, CFB, OFB**

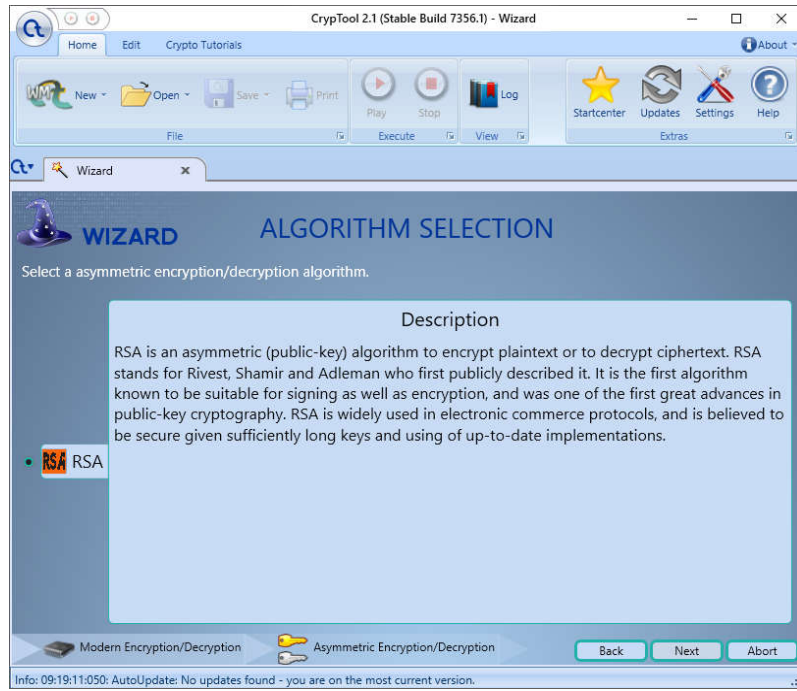




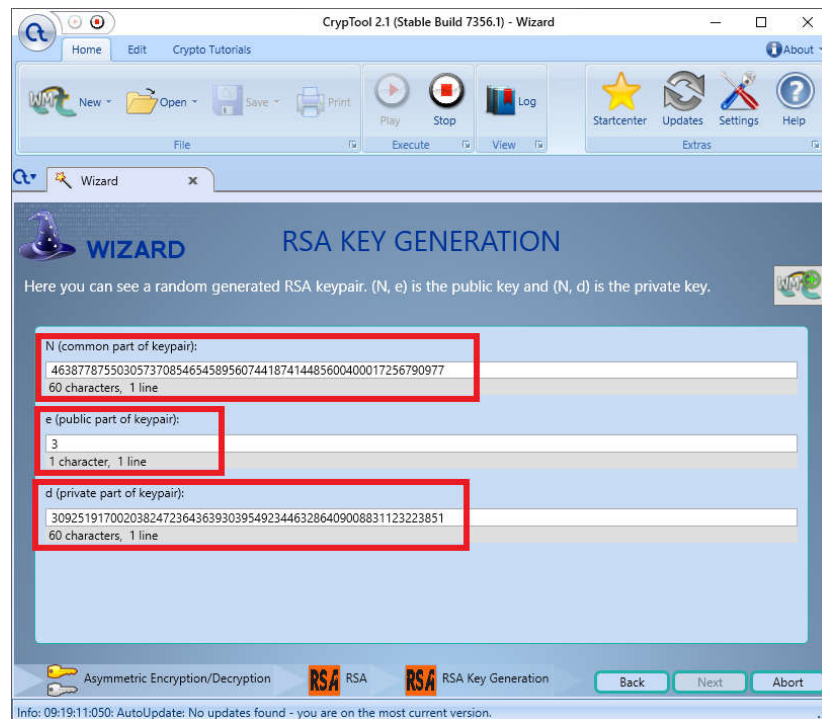
Sesi 3 – Asymmetric Cryptography

RSA (Rivest Shamir Adleman)

Encryption/Decryption > Modern > Asymmetric > RSA > Next

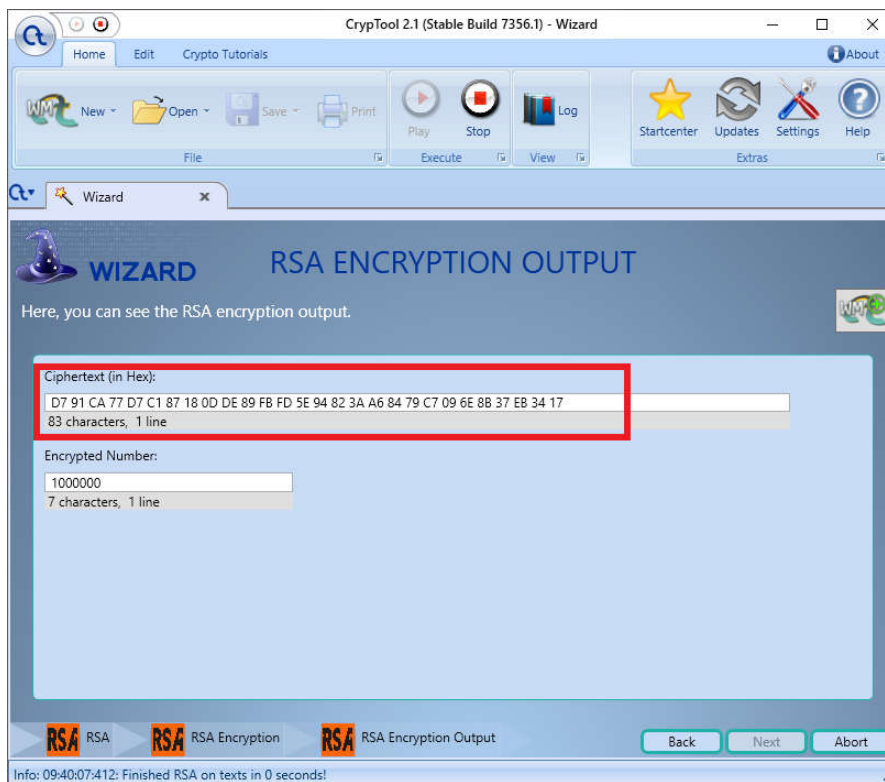
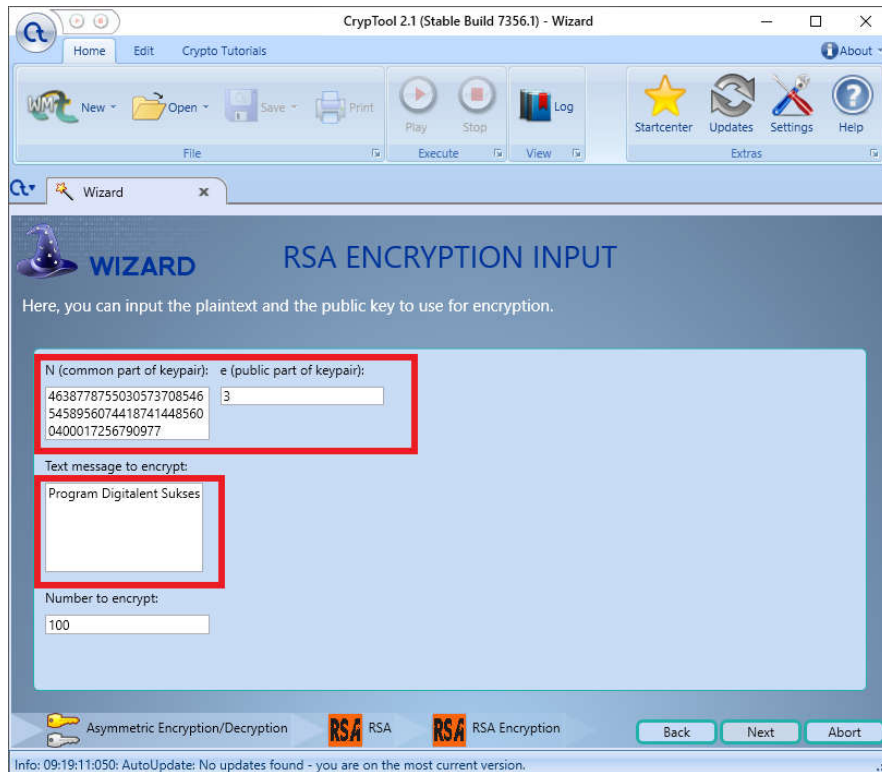


- Pembangkitan Kunci RSA

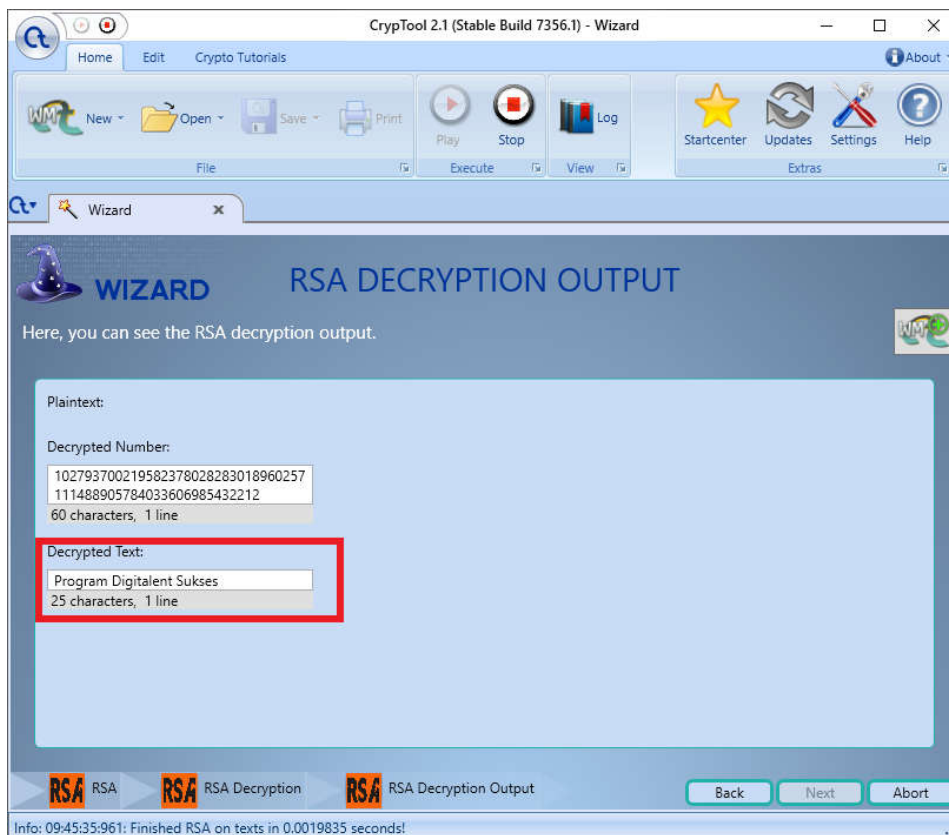
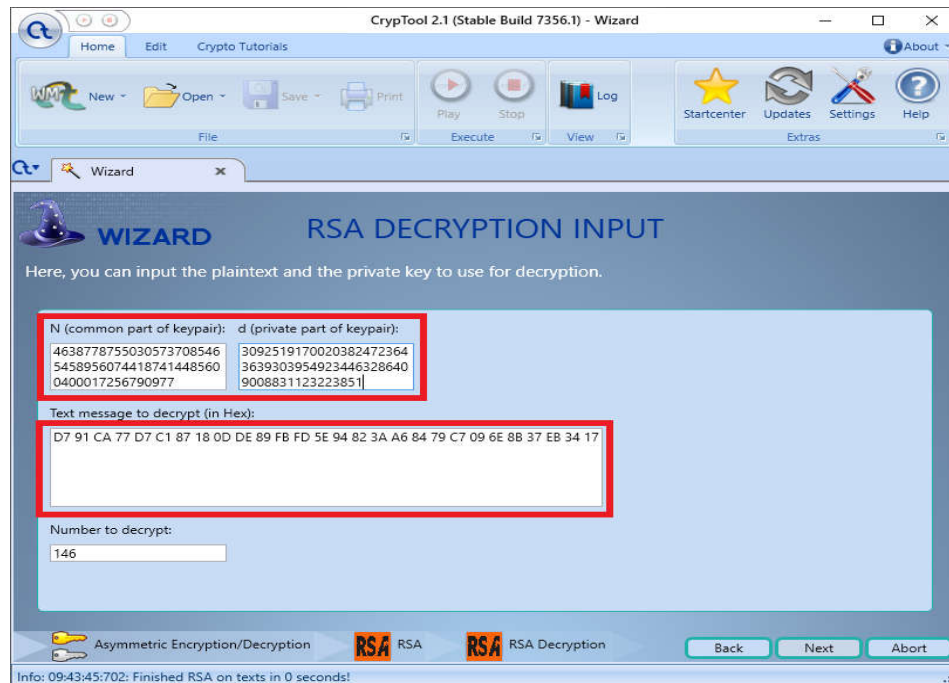


Simpan **privat key**, **publik key** dan **N**

- Langkah melakukan enkripsi
Enkripsi pesan menggunakan **kunci publik** dan **N**

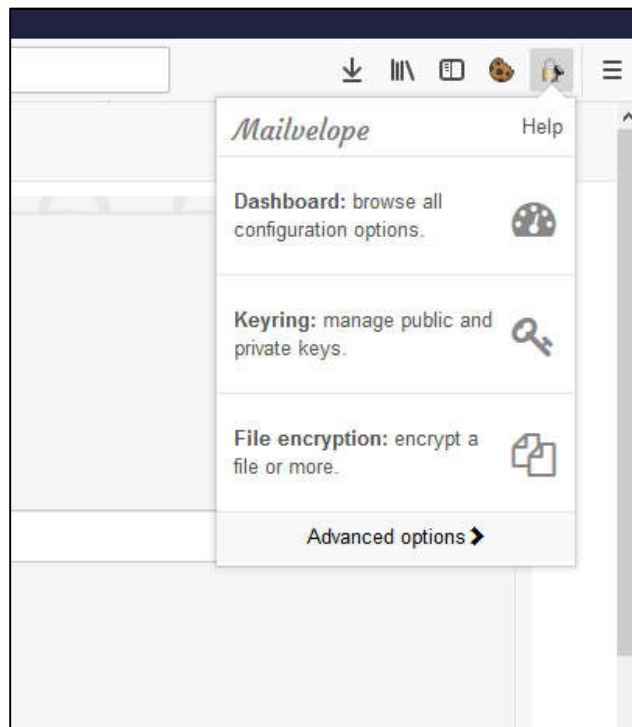


- Langkah melakukan dekripsi
Dekripsi pesan menggunakan **kunci privat** dan **N**



Sesi 4 – Secure Mail

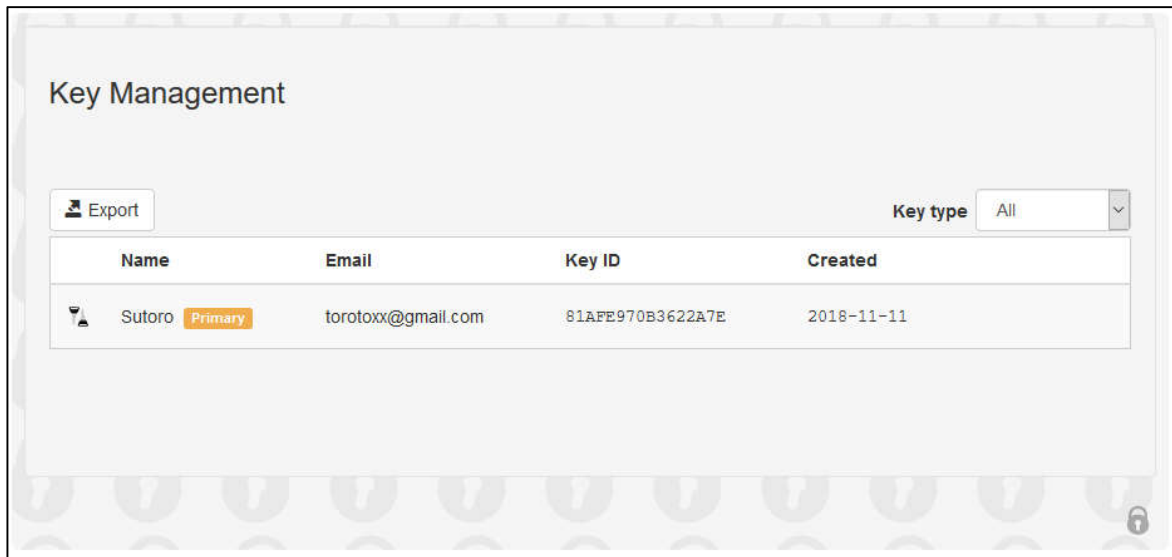
- Instal plugin **Mailvelope** pada browser



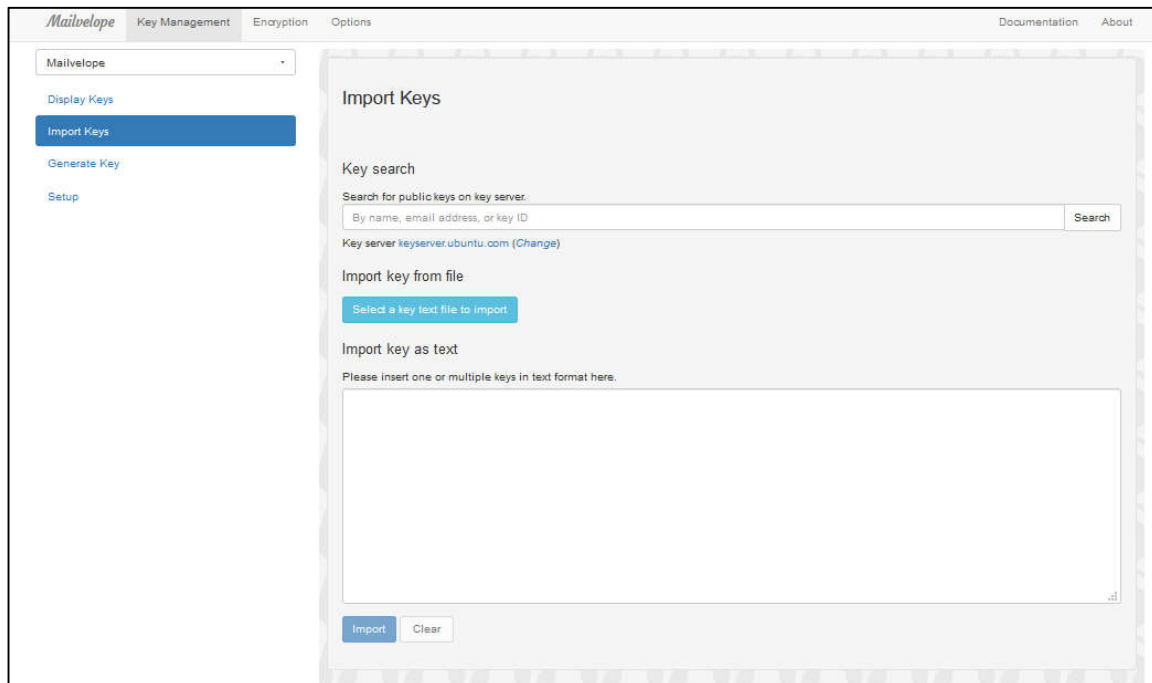
- Bangkitkan pasangan kunci publik dan privat

A screenshot of the Mailvelope web interface, specifically the 'Generate Key' page. The interface has a top navigation bar with 'Mailvelope', 'Key Management', 'Encryption', and 'Options'. On the left side, there is a sidebar with a dropdown menu set to 'Mailvelope' and several links: 'Display Keys', 'Import Keys', 'Generate Key' (highlighted with a blue button), and 'Setup'. The main content area is titled 'Generate Key' and contains several input fields: 'Name' (with a placeholder 'Full name of the key owner'), 'Email', and two password fields labeled 'Enter Password' and 'Re-enter Password'. A red error message 'Password field is empty' is visible below the first password field. There is an 'Advanced >>' button between the email and password fields. At the bottom, there is a checkbox labeled 'Upload public key to Mailvelope Key Server (can be deleted at any time). Learn more'.


- Setelah pasangan kunci dibangkitkan maka kita dapat share kunci publik milik kita dengan terlebih dahulu melakukan export pasangan kunci yang telah kita bangkitkan.

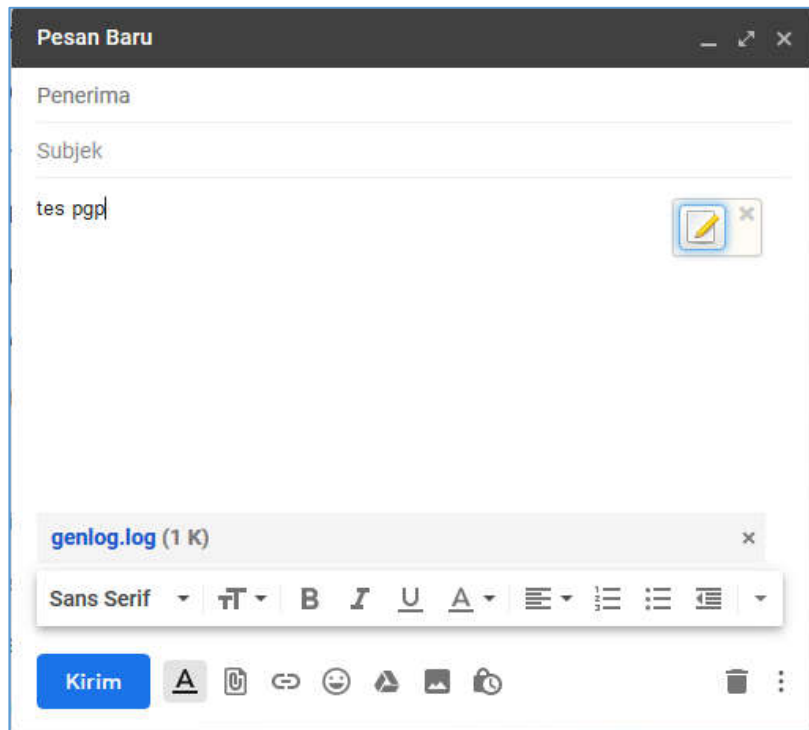


- Untuk melakukan Import kunci publik pihak lain dapat dilakukan dengan cara berikut ini

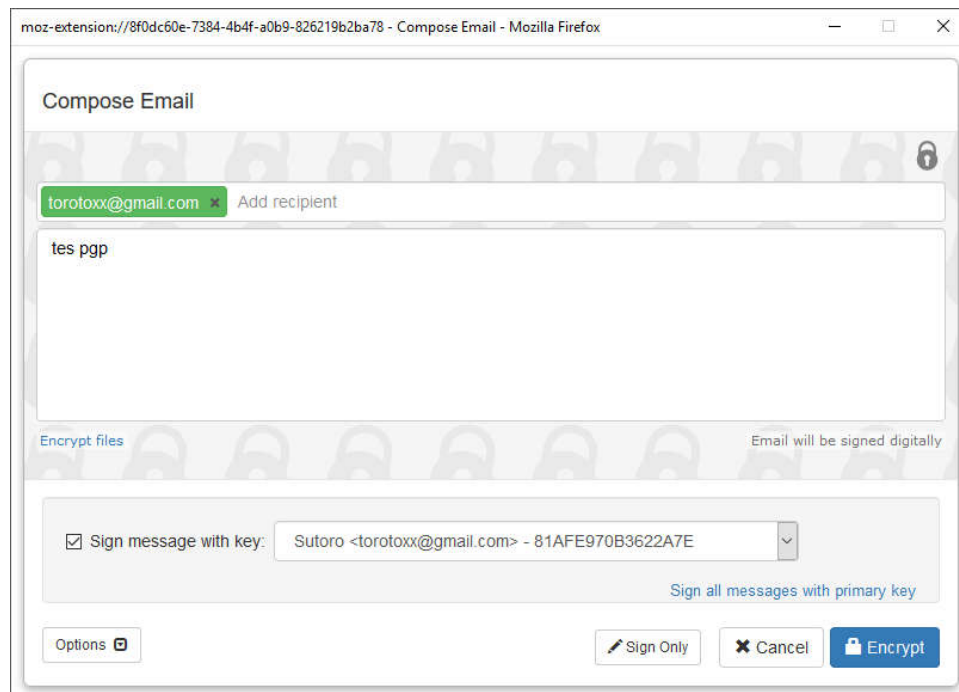


➤ Kirim terima email

- Pada halaman tulis email baru akan muncul ikon . Ikon tersebut merupakan ekstensi dari aplikasi mailvelope.

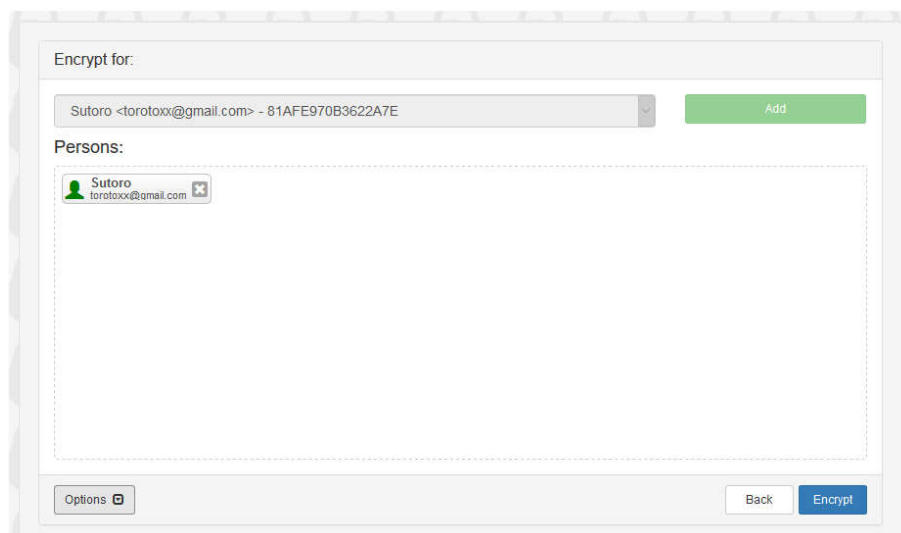
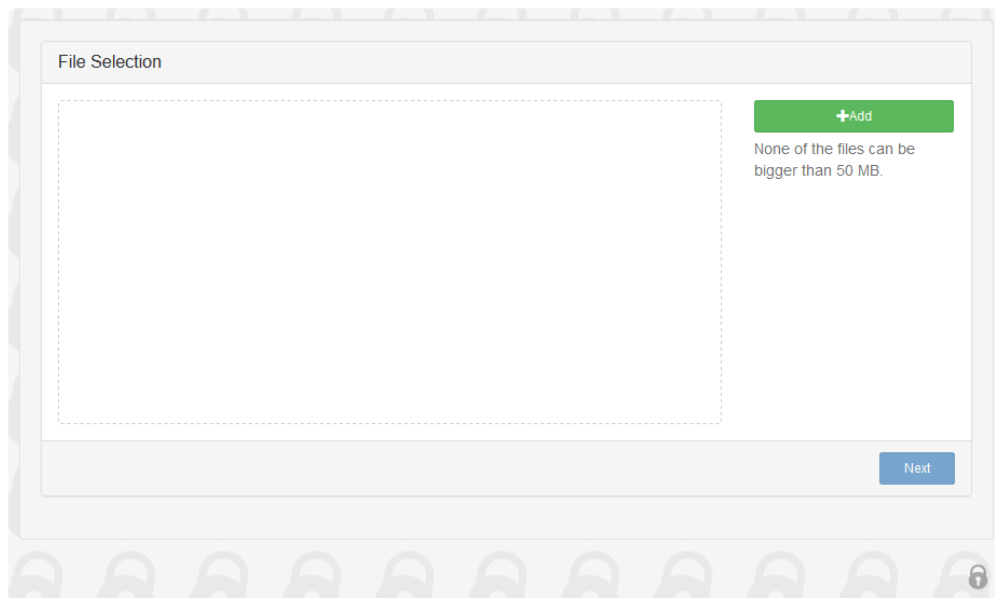


- Jika ikon  di-klik maka akan muncul halaman berikut ini.

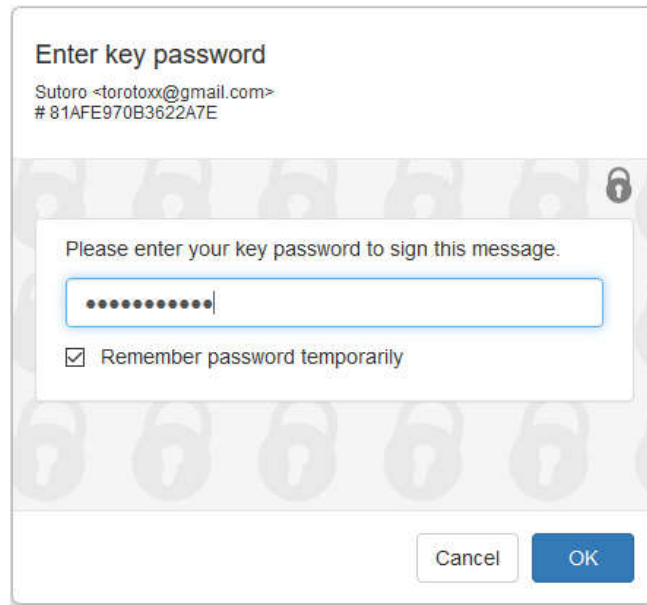


- Tentukan alamat email tujuan (yang sudah tersimpan public key-nya)

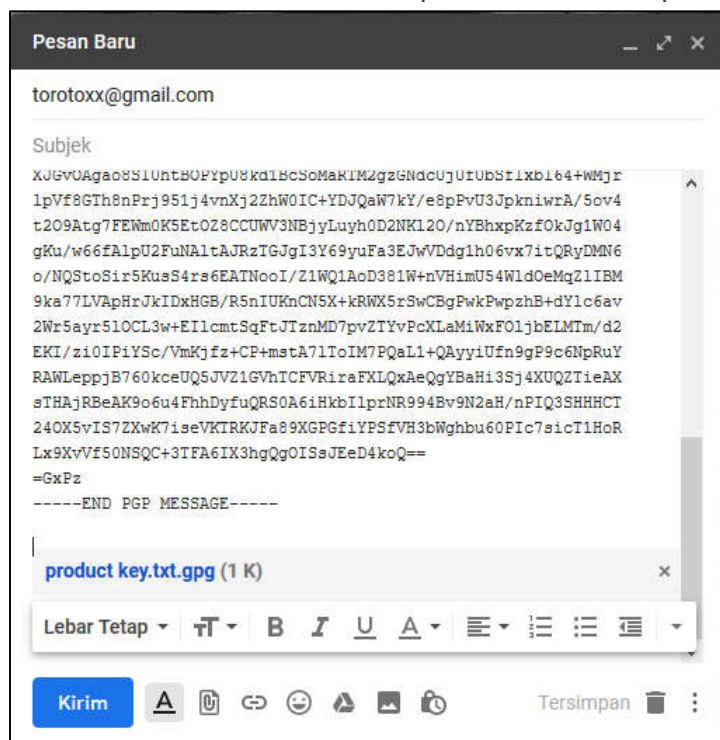
- Jika akan menambahkan file attachment terenkripsi maka dapat melakukan enkripsi terlebih dahulu dengan menekan ikon “Encrypt files” dan akan menuju halaman berikut ini.



- Kemudian file attachment yang telah dienkripsi dilampirkan pada email.
- Pada saat mengenkripsi pesan email akan muncul perintah untuk memasukkan password private key guna melakukan proses penandatanganan pesan email.



- Setelah pesan email dan file attachment dienkripsi maka email siap untuk dikirimkan.



- Pada sisi penerima pesan email dapat langsung didekripsi menggunakan private key.
- File attachment dapat didekripsi menggunakan aplikasi mailvelope file decryption.