CRYPTOR

Autor: SINAPSA Infocomplex® S. R. L.

Manualul de utilizare

CRYPTOR este o aplicaţie *software* (ori "program") care vă oferă posibilitatea de a efectua operaţiuni de criptografie precum criptarea unor fişiere şi texte şi ascunderea unui text într-o imagine.

După ce un fişier sau un text este criptat va putea fi decriptat, adică descifrat numai de către cei care au cheia cu care informaţia respectivă a fost criptată. Astfel, chiar dacă persoane sau entităţi neavenite obţin în orice fel informaţiile criptate, nu le vor putea descifra decât după un timp relativ lung (chiar ani întregi, luni, sau în cel mai rău caz săptămâni). Aceasta este valabil şi pentru un text (ori mesaj) criptat ascuns într-o imagine: cei care vor obţine imaginea respectivă nu vor putea citi acel text decât dacă vor şti că imaginea conţine un mesaj şi dacă vor avea cheia de criptare a acestuia.

Fişierele şi textele pot fi "semnate" pentru a le verifica integritatea şi pot fi identificate prin calcularea aşa-numitei semnături de tip *hash*. Aceste operaţiuni ajută la identificarea informaţiei provenite din anumite surse, prin semnalarea modificărilor informaţiei originale.

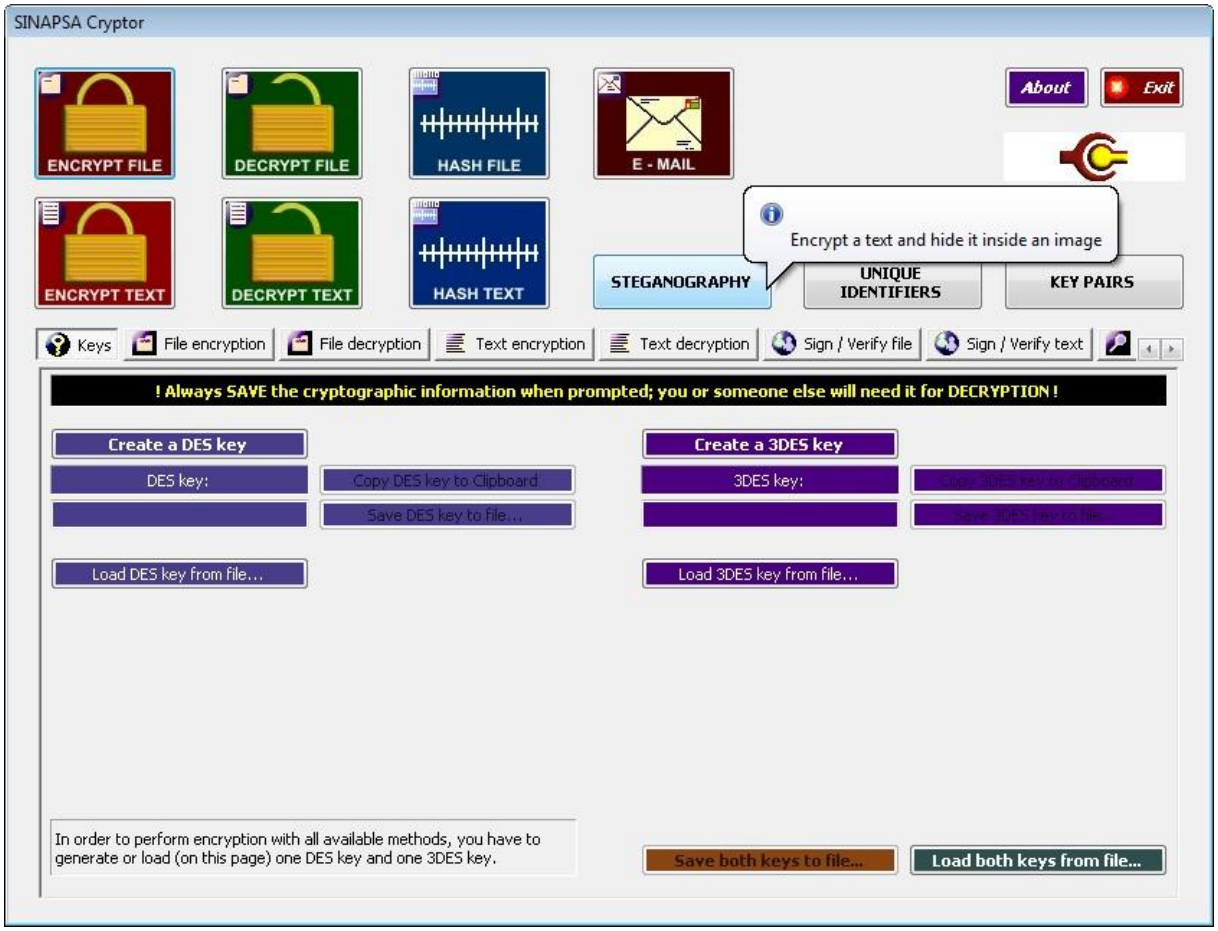
Acest manual se referă la versiunile 2.x ale CRYPTOR-ului; astfel, unele dintre funcţiile prezentate aici pot lipsi din versiunea pe care o folosiţi, care poate fi mai veche sau ulterioară uneia din acestea.

Interfaţa este elaborată în limba engleză, însă explicaţiile şi sfaturile detaliate sunt prezentate în cuvinte des folosite.

INTERFAŢA PROGRAMULUI

Interfaţa CRYPTOR-ului este alcătuită din mai multe "pagini", anume:

1) "Keys" ("Chei")
2) "File encryption" ("Criptarea unui fişier")
3) "File decryption" ("Decriptarea unui fişier")
4) "Text encryption" ("Criptarea unui text")
5) "Text decryption" (Decriptarea unui text")
6) "Sign / Verify file" ("Semnarea / Verificarea unui fişier")
7) "Sign / Verify text" ("Semnarea / Verificarea unui text")
8) "Steganography" ("Steganografie")
9) "Hash a file" ("Calcularea *hash*-ului unui fişier")
10) "Hash a text" ("Calcularea *hash*-ului unui text")
11) "E-mail" ("Poştă electronică")
12) "Password generator" ("Creator de parole")
13) "Identifiers" ("Identificatori")
14) "Key pairs" ("Perechi de chei")
15) "Info" ("Informaţii")


SINAPSA Cryptor
ENCRYPT FILE
DECRYPT FILE
HASH FILE
E - MAIL
About
Exit
ENCRYPT TEXT
DECRYPT TEXT
HASH TEXT
Encrypt a text and hide it inside an image
STEGANOGRAPHY
UNIQUE IDENTIFIERS
KEY PAIRS
Keys
File encryption
File decryption
Text encryption
Text decryption
Sign / Verify file
Sign / Verify text
! Always SAVE the cryptographic information when prompted; you or someone else will need it for DECRYPTION !
Create a DES key
DES key:
Copy DES key to Clipboard
Save DES key to file...
Load DES key from file...
Create a 3DES key
3DES key:
Load 3DES key from file...
In order to perform encryption with all available methods, you have to generate or load (on this page) one DES key and one 3DES key.
Save both keys to file...
Load both keys from file...

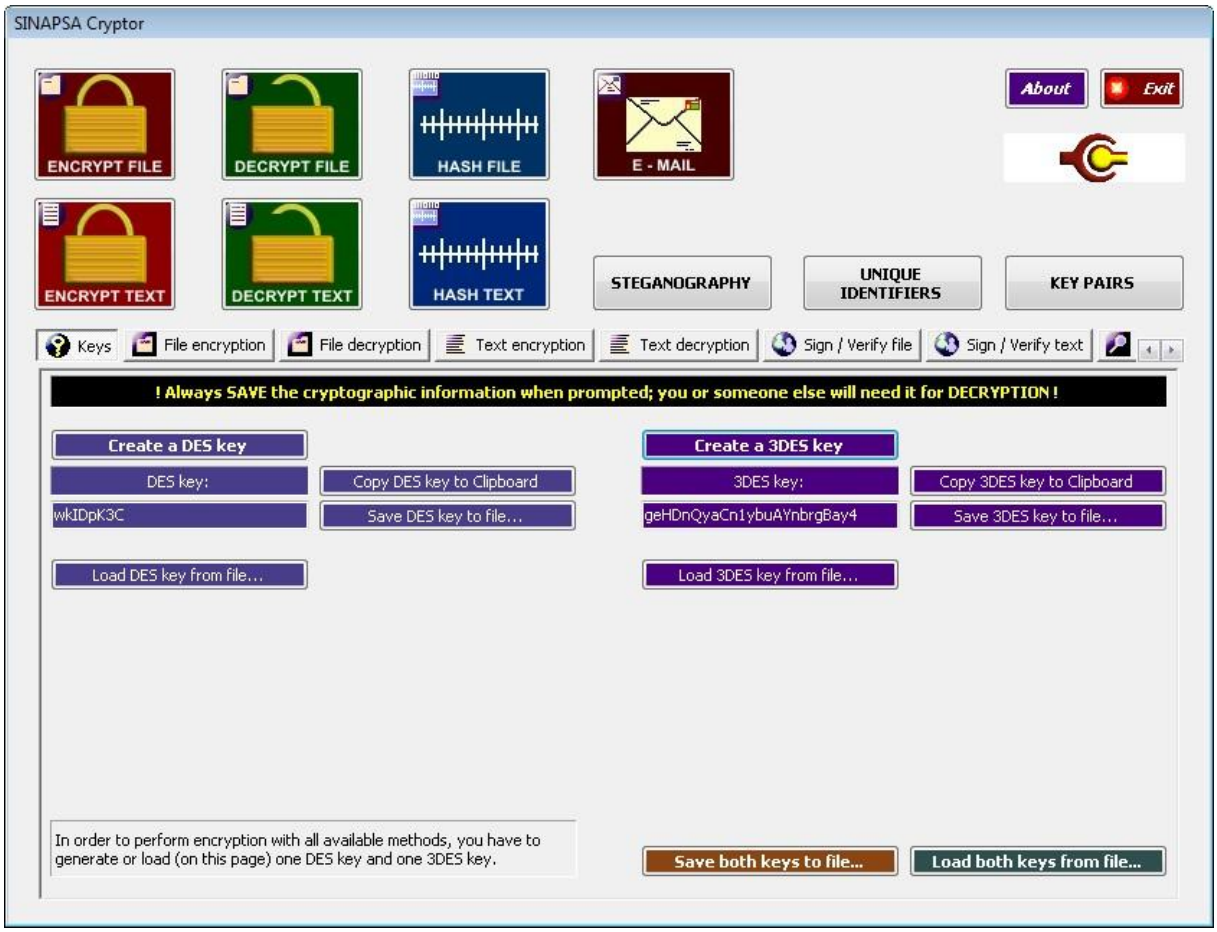
1. PAGINA "Keys" ("Chei")

Pe această pagină pot fi create aşa-numite chei de criptare şi decriptare.
Cheia cu care o informaţie a fost criptată poate fi folosită pentru decriptarea aceleiaşi informaţii.

Altă cheie decât cea care a criptat o informaţie nu va putea decripta acea informaţie.
O cheie nu poate decripta decât informaţia pe care a criptat-o.

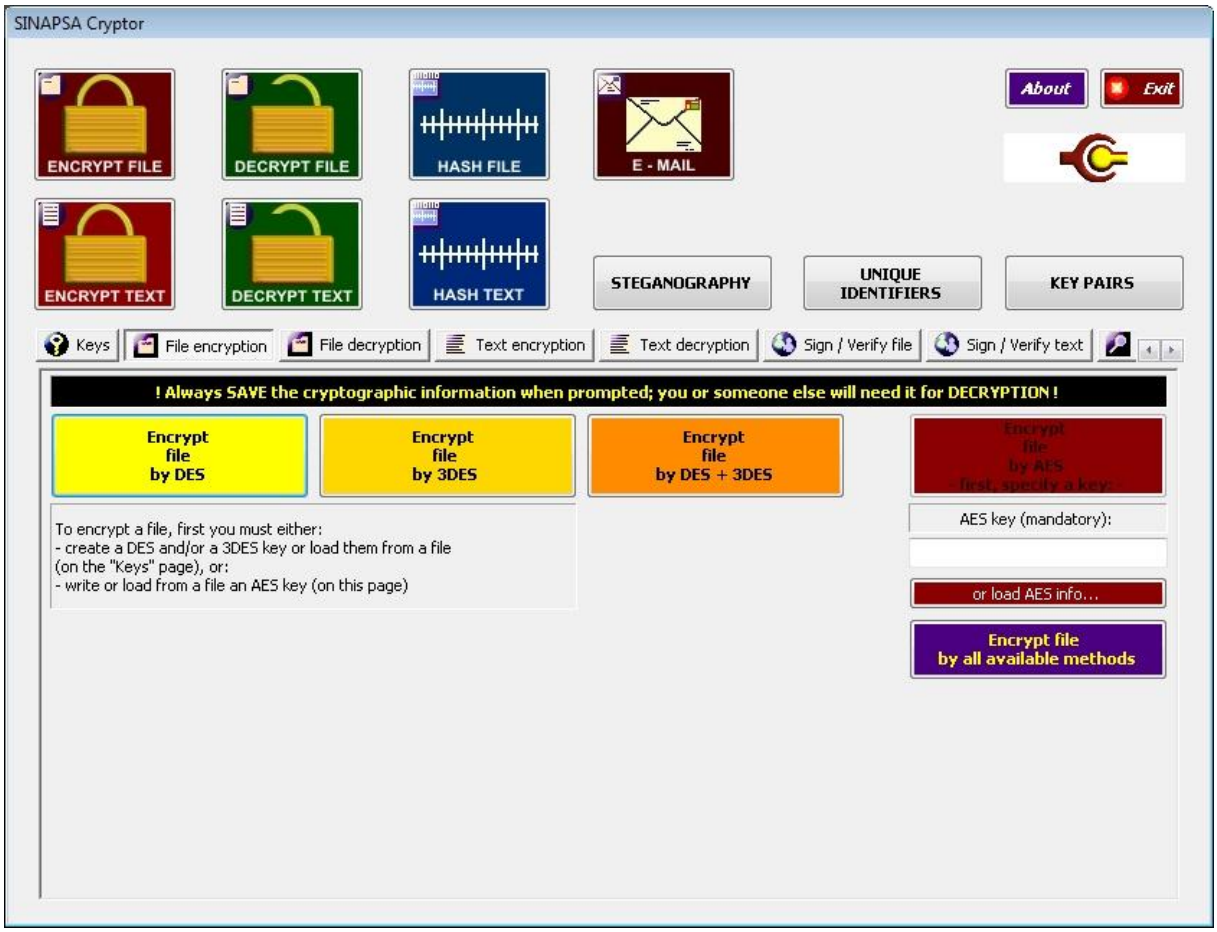
Aici puteţi crea chei de criptare prin metodele DES şi TripleDES (sau "3DES").
Puteţi şi salva în fişiere cheile create:
- pe rând, acţionând butoanele "Save DES/3DES key to file..."
- împreună, acţionând butonul "Save both keys to file...")
De asemenea, puteţi încărca astfel de chei din fişierele în care le-aţi salvat:
- pe rând, acţionând butoanele "Load DES/3DES key from file..."
- împreună, acţionând butonul "Load both keys from file...")
În plus, puteţi copia în memoria computerului (Clipboard) cheile create:
- cheia DES poate fi copiată în Clipboard acţionând butonul "Copy DES key to Clipboard"
- cheia 3DES poate fi copiată în Clipboard acţionând butonul "Copy 3DES key to Clipboard"

Butoanele corespunzătoare unei chei vor fi active numai când fie cheia a fost creată, fie a fost încărcată dintr-un fişier în care fusese salvată anterior.



2. PAGINA "File encryption" ("Criptarea unui fişier")

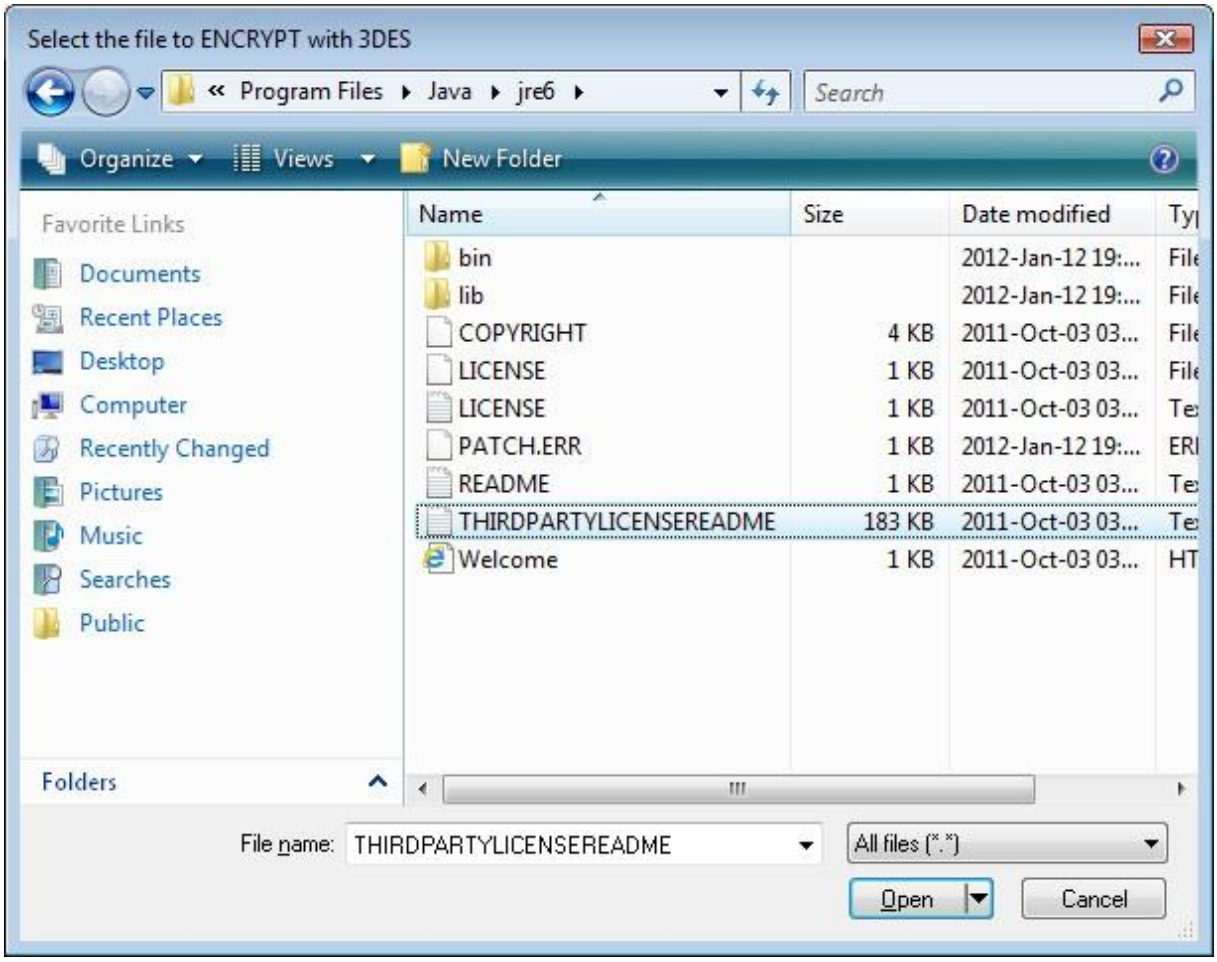
Pe această pagină poate fi criptat un fişier, astfel încât deşi îşi va păstra denumirea (de exemplu, "fisiertext.txt") fie nu va putea fi deschis cu programul asociat, fie va fi deschis dar va fi indescifrabil fiindcă formatul şi conţinutul său vor fi dezorganizate şi distruse prin criptare, încât numai cei care deţin cheia cu care a fost criptat să îl poată accesa şi descifra.



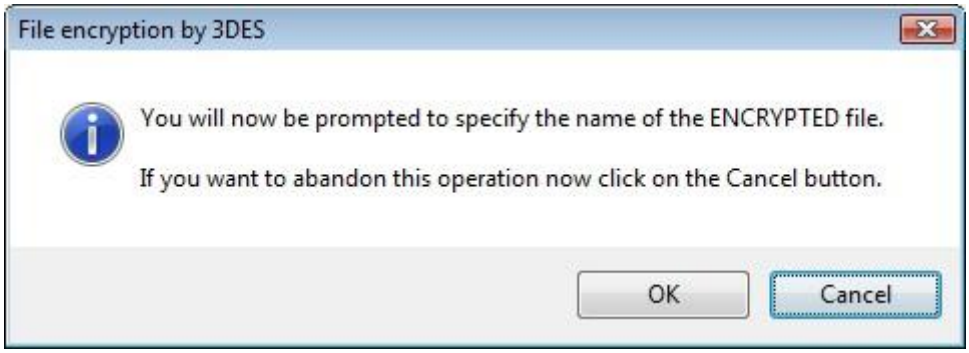
Puteţi cripta un fişier prin patru metode:
1) DES. Aceasta este disponibilă numai dacă este cunoscută o cheie DES.
2) 3DES. Aceasta este disponibilă numai dacă este cunoscută o cheie 3DES.
3) DES şi 3DES. Aceasta este disponibilă numai dacă sunt cunoscute o cheie DES şi o cheie 3DES.
4) prin metoda AES.

Butoanele pentru metodele DES/3DES vor fi active numai dacă sunt cunoscute astfel de chei.
Butonul pentru metoda AES va deveni activ după ce scrieţi manual un text-cheie AES sau încărcaţi informaţie AES dintr-un fişier în care o salvaseţi anterior, acţionând butonul "or load AES info...".

În acest exemplu se foloseşte metoda 3DES.
După ce apăsaţi unul din butoanele "Encrypt file by..." (în acest exemplu, 3DES) va fi prezentat un dialog în care veţi putea alege fişierul ce va fi criptat:

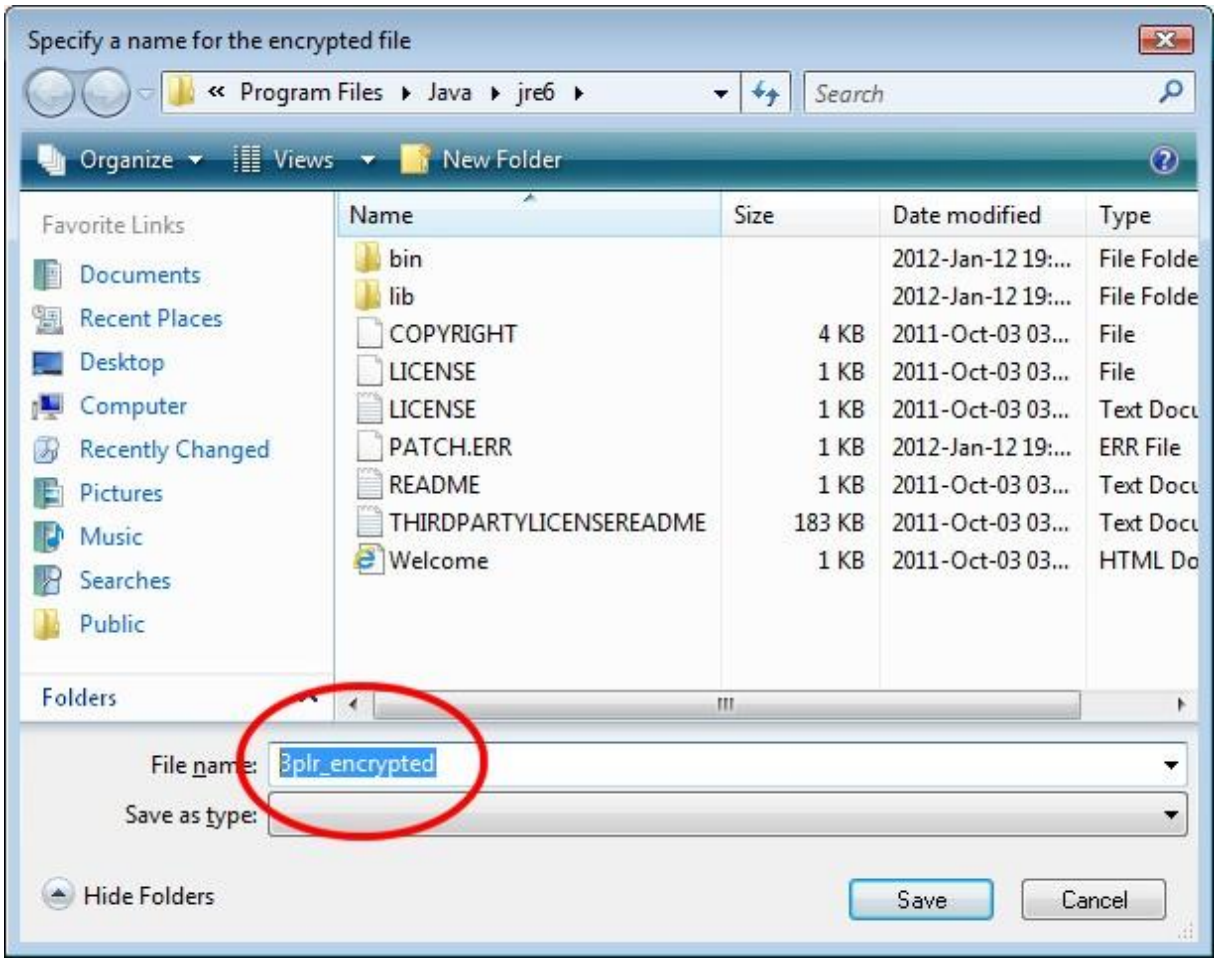


După ce alegeţi fişierul pe care îl veţi cripta şi apăsaţi butonul "Open" sau similar al dialogului vi se va solicita confirmarea continuării operaţiunii de criptare a fişierului; dacă vreţi să continuaţi apăsaţi butonul "OK" sau similar:

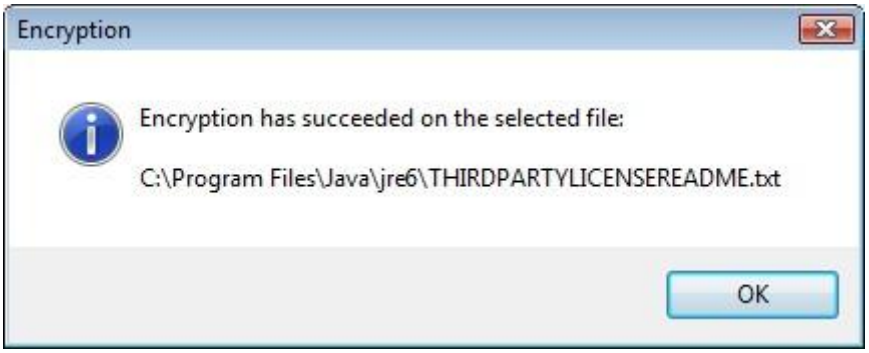


După criptare fişierul original va continua să existe împreună cu forma sa criptată.

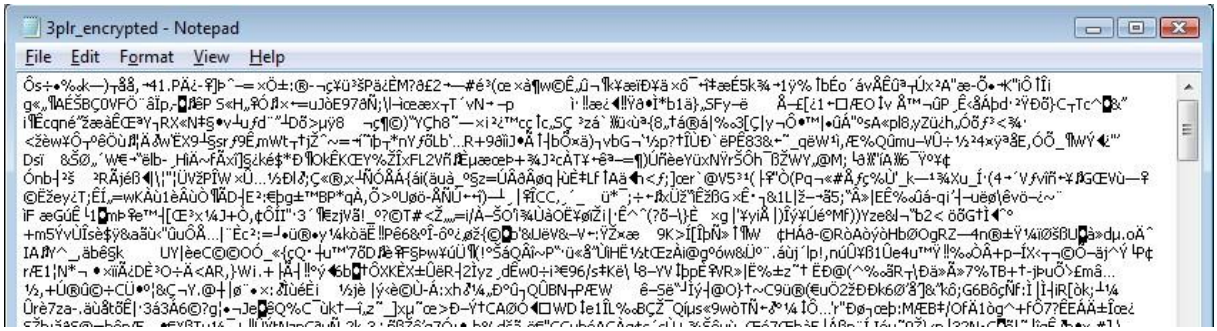
Dacă apăsaţi butonul "OK" sau similar vi se va solicita denumirea fişierului criptat:



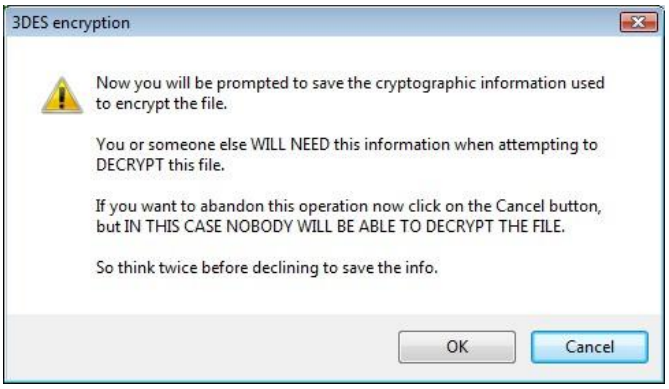
Odată ce specifcaţi destinaţia şi denumirea fişierului criptat apăsaţi butonul "Save" sau similar al acestui dialog. Un mesaj va anunţa succesul sau eşecul operaţiunii de criptare:



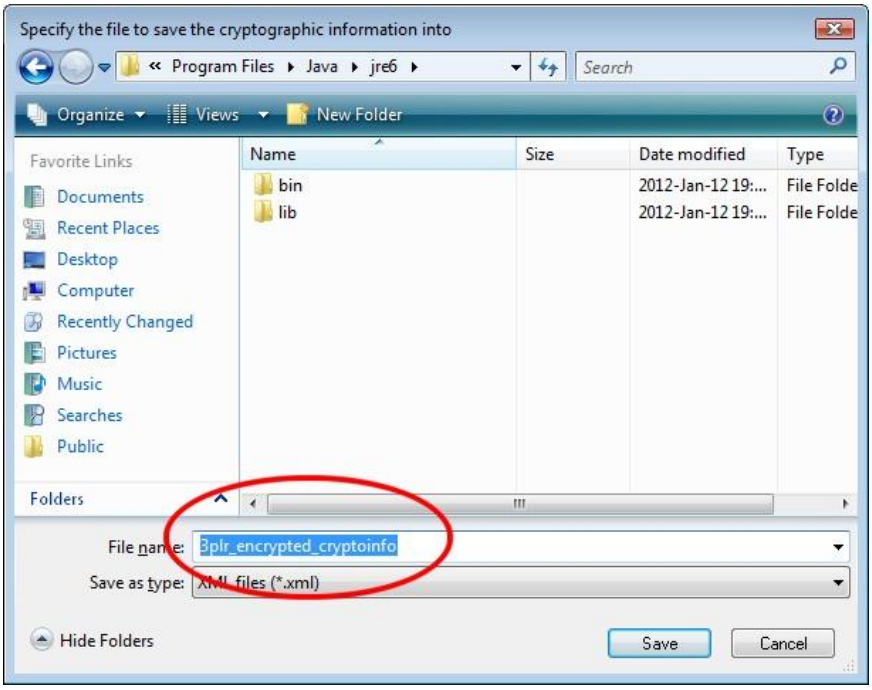
Pentru a verifica reuşita criptării încercaţi să deschideţi fişierul criptat – în exemplul de mai sus, acesta se numeşte "3plr_encrypted.txt". Dacă programul asociat acelui tip de fişier (în acest caz, de tip text, cu extensia .txt) îl poate deschide veţi vedea conţinutul fişierului criptat, însă nu îl veţi putea descifra:



După criptare va apărea un mesaj de avertizare prin care se va recomanda să salvaţi cheia de criptare a fişierului, pentru ca mai târziu să îl decriptaţi:



Pentru a salva respectiva informaţie criptografică apăsaţi butonul "OK" sau similar al acestui dialog. Ca mai înainte, specificaţi numele fişierului care va conţine această informaţie:



!!! Salvaţi informaţia criptografică de fiecare dată când vi se recomandă !!!
!!! Altfel nu veţi putea decripta ceea ce aţi criptat !!!

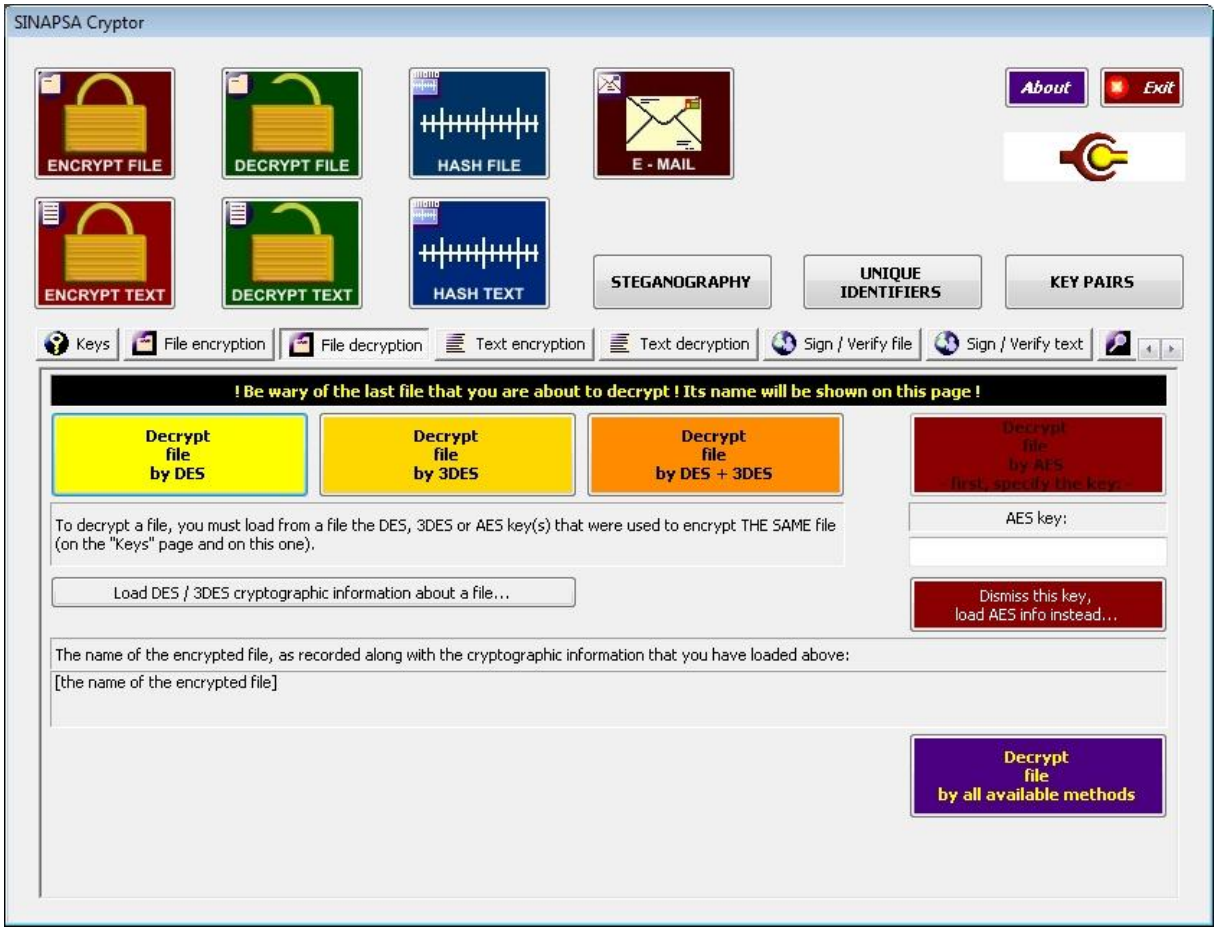
Un dialog va anunţa reuşita sau eşecul operaţiunii de salvare a informaţiei criptografice corespunzătoare fişierului criptat:



Informaţia criptografică pe care o salvaţi după ce criptaţi un fişier sau un text va putea fi folosită pentru decriptarea acelui fişier sau text.

3. PAGINA "File decryption" ("Decriptarea unui fişier")

Pe această pagină poate fi decriptat un fişier prin aceeaşi metodă şi folosind aceeaşi informaţie criptografică folosită la criptarea sa.



Aici puteţi decripta un fişier prin metodele disponibile pentru criptare (DES, 3DES, DES+3DES şi AES).

Butoanele corespunzătoare metodelor vor fi active numai dacă sunt cnoscute cheile respective sau informaţia criptografică respectivă.

În cazul metodelor DES / 3DES puteţi fie:

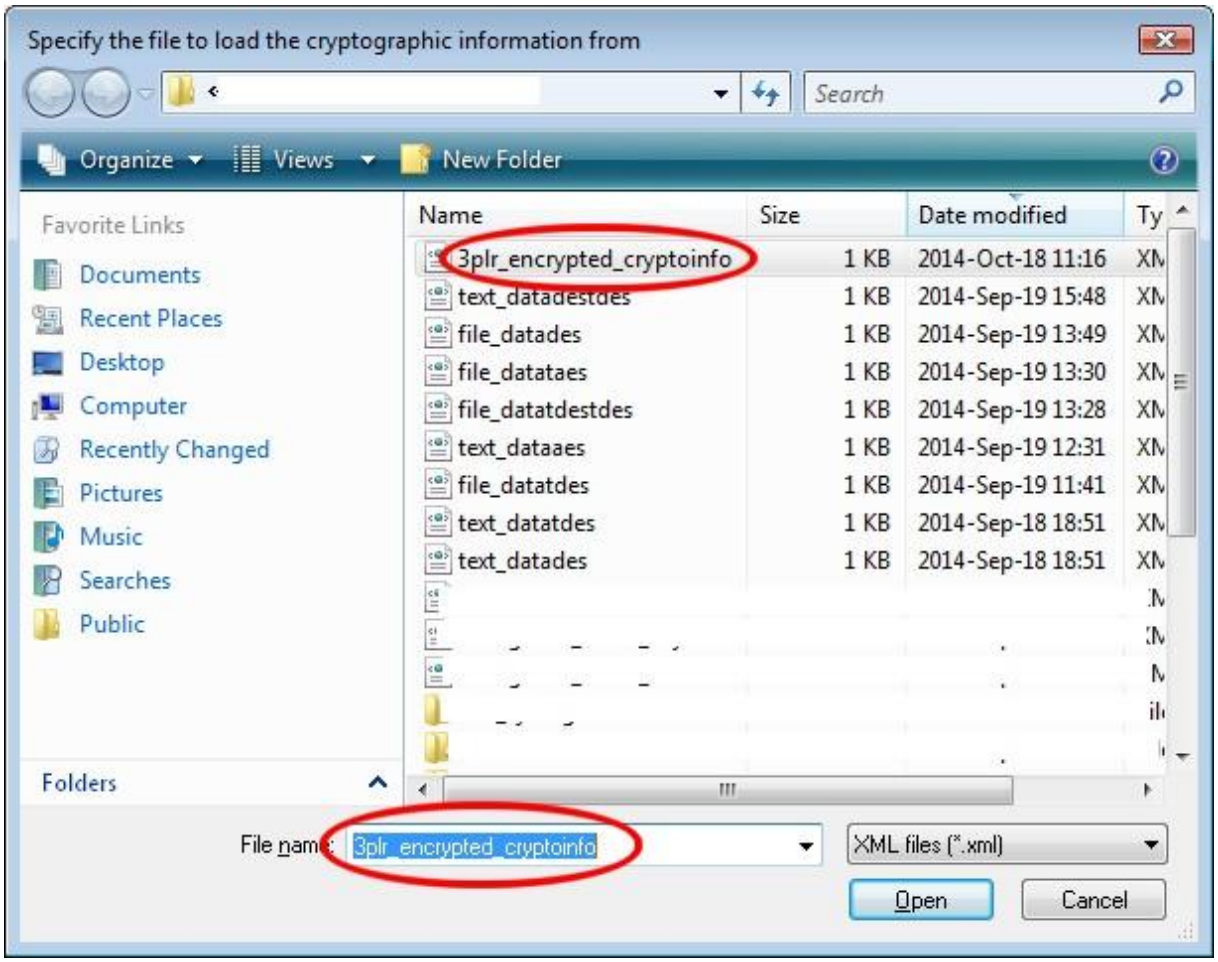
- folosi pagina "Keys" pentru a încărca astfel de chei din fişiere în care le-aţi salvat anterior
- apăsa butonul "Load DES / 3DES cryptographic information about a file..." pentru a încărca informaţie criptografică DES / 3DES referitoare explicit la un fişier criptat anterior.

În cazul metodei AES puteţi fie:

- scrie manual cheia AES de decriptare în caseta de editare de sub eticheta marcată "AES key:"
- apăsa butonul "Dismiss this key, load AES info instead..." pentru a ignora cheia scrisă aici (dacă există vreuna) şi a încărca informaţie criptografică AES / 3DES referitoare explicit la un fişier criptat anterior.

În acest exemplu se va prezenta decriptarea fişierului criptat anterior prin metoda 3DES.

1) Întrucât ştim că într-un fişier dedicat există informaţia criptografică referitoare la un fişier criptat, apăsăm butonul "Load DES / 3DES cryptographic information about a file...":



Un mesaj va anunţa reuşita sau eşecul încărcării informaţiei criptografice din fişierul selectat:

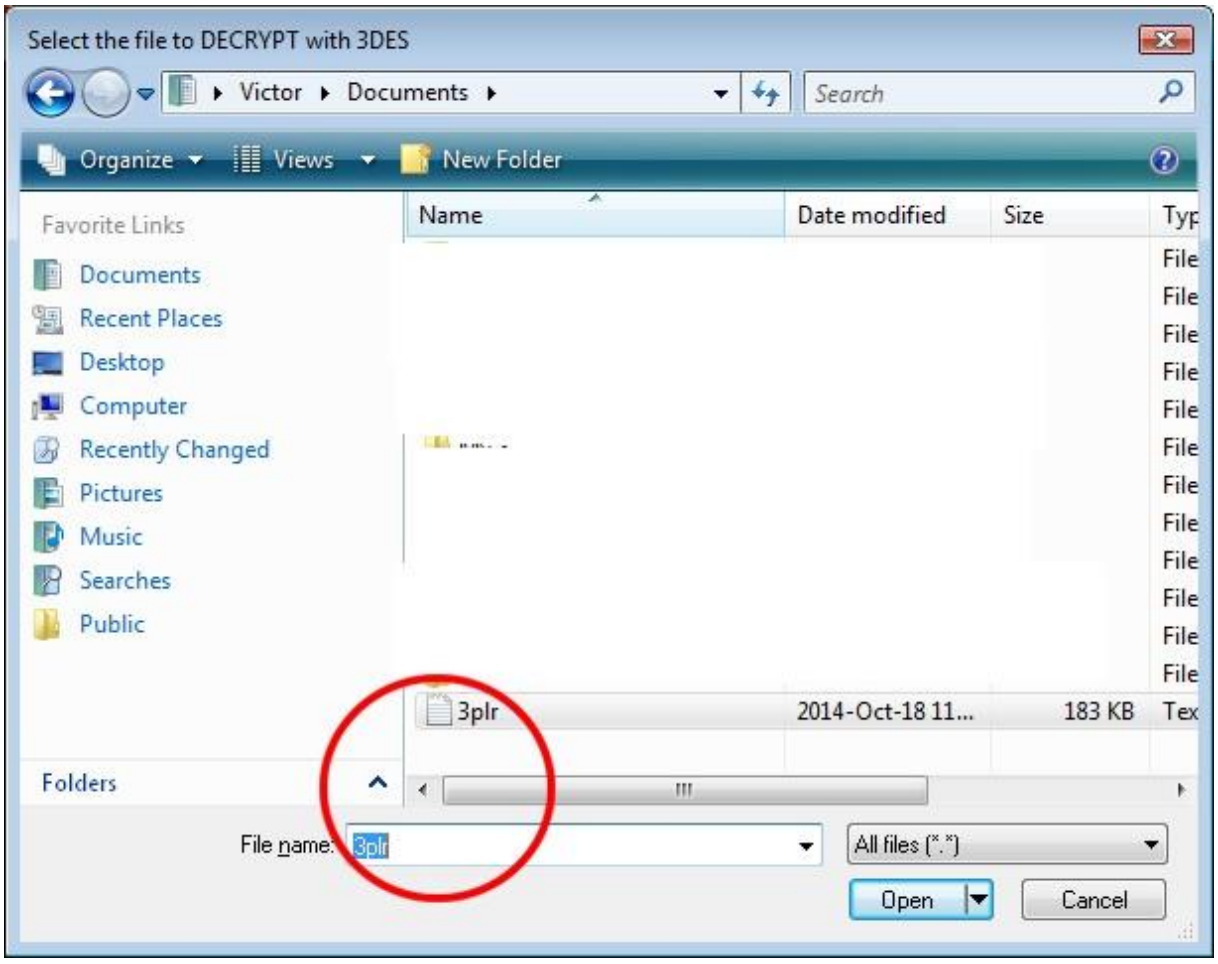


Suntem anunţaţi şi că denumirea fişierului criptat este afişată pe această pagină.

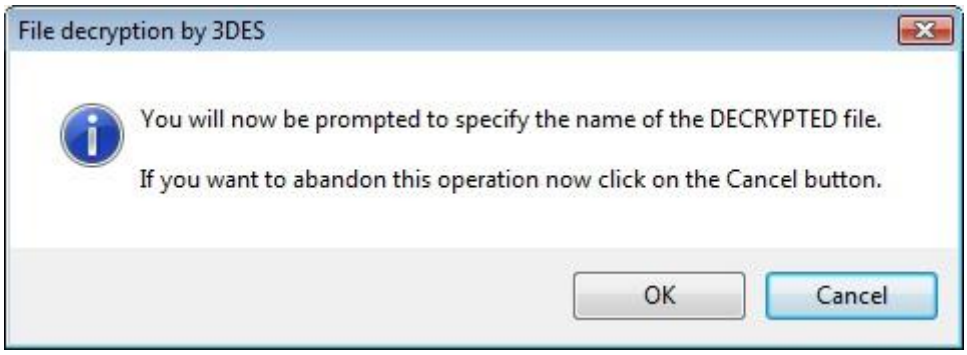
În dialogul următor suntem anunţaţi că se va încerca decriptarea fişierului a cărui denumire a fost cunoscută după încărcarea informaţiei criptografice:

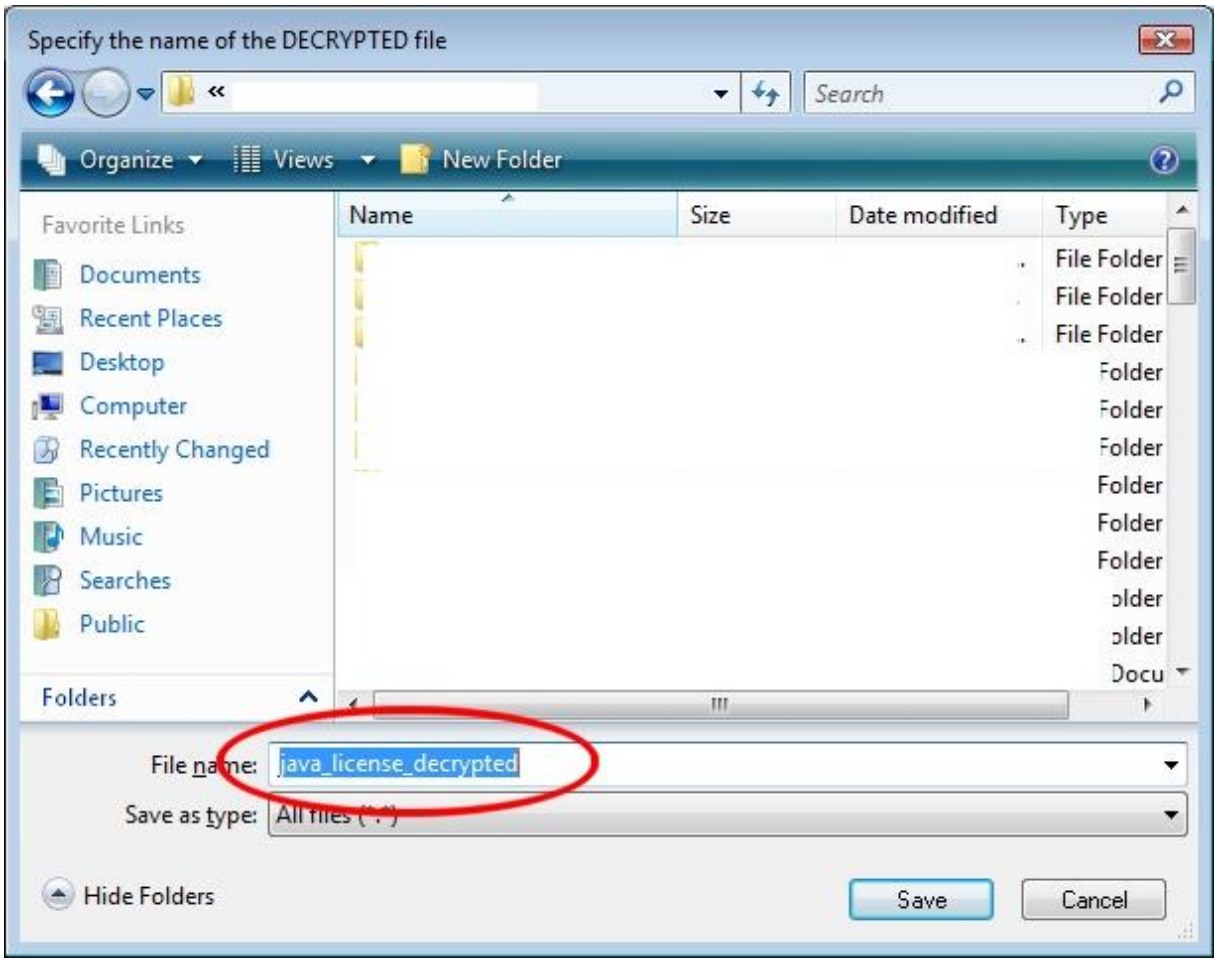


2) Pentru a continua cu decriptarea fişierului apăsăm butonul "OK", după care ni se va solicita să selectăm fişierul CRIPTAT:

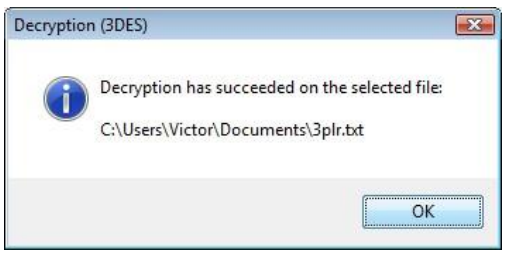


3) După ce alegem fişierul ce fusese criptat ni se va solicita denumirea fişierului DECRIPTAT:

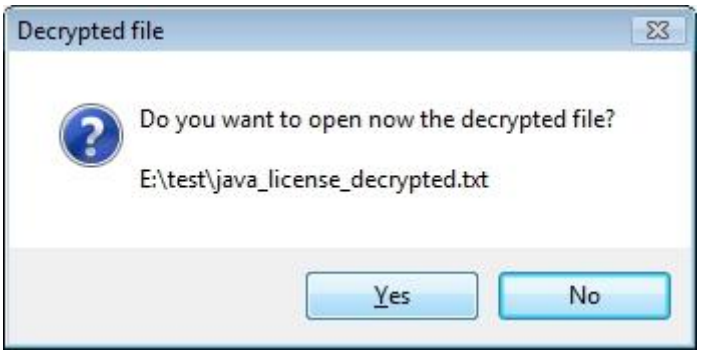




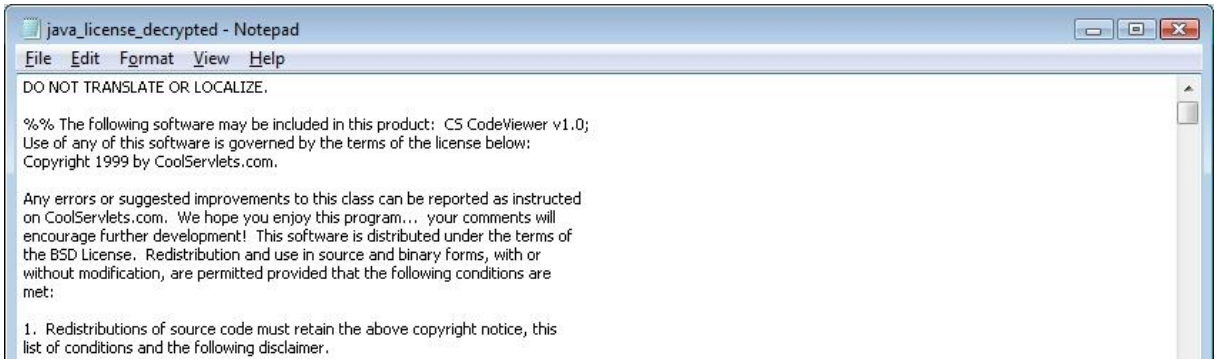
4) După ce apăsăm butonul "Save" sau similar fişierul va fi decriptat folosind informaţia criptografică încărcată şi va fi salvat sub denumirea tocmai specificată. Un mesaj va anunţa reuşita sau eşecul operaţiunii de decriptare a fişierului:



5) Dacă decriptarea reuşeşte ni se va oferi posibilitatea de a deschide fişierul decriptat:

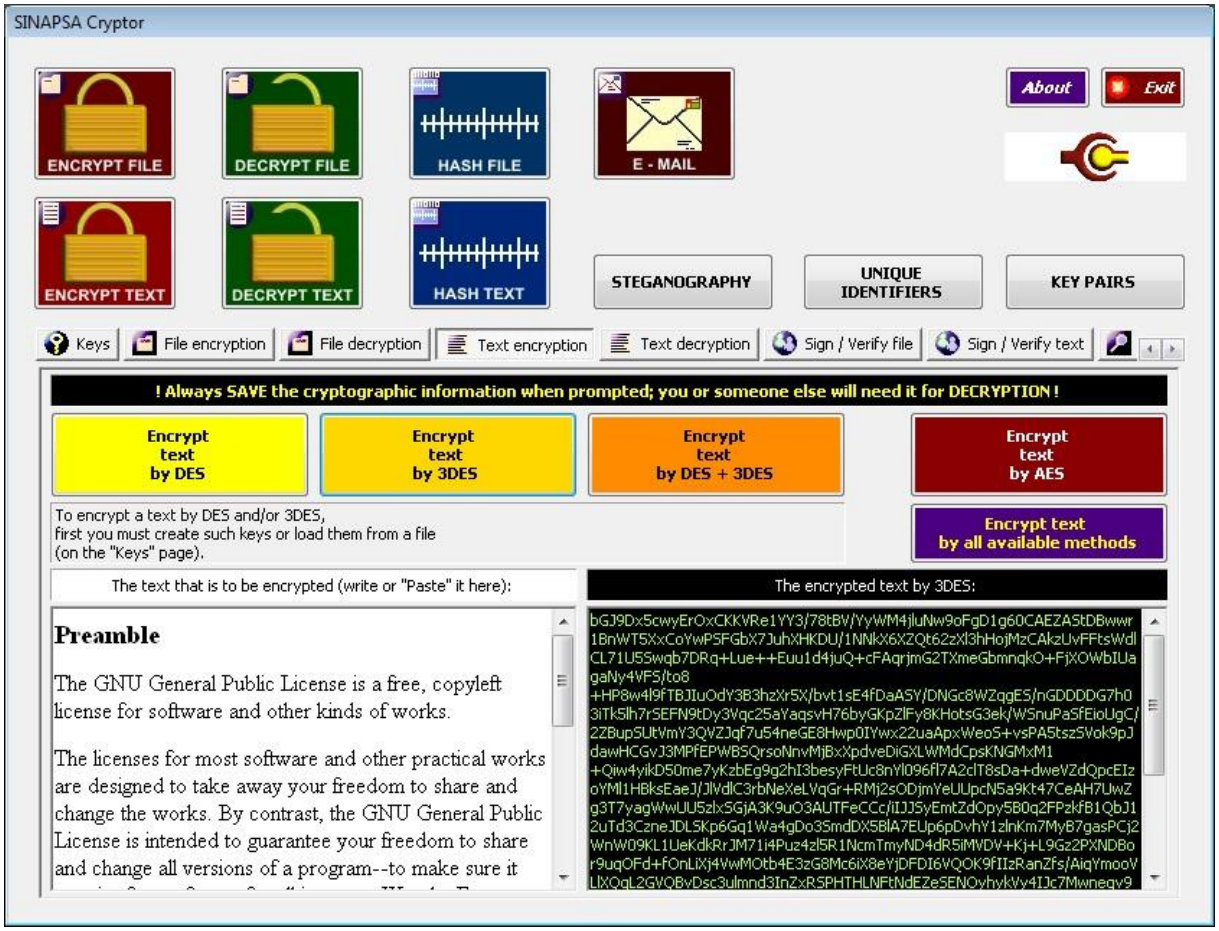


Dacă apăsăm butonul "Yes" sau similar fişierul decriptat va fi deschis cu programul implicit ce îi corespunde şi astfel îi vom putea accesa conţinutul:



4. PAGINA "Text encryption" ("Criptarea unui text")

Pe această pagină poate fi criptat un text, astfel încât va fi indescifrabil fiindcă va fi dezorganizat şi distrus prin criptare, încât numai cei care deţin cheia cu care a fost criptat să îl poată accesa şi descifra.



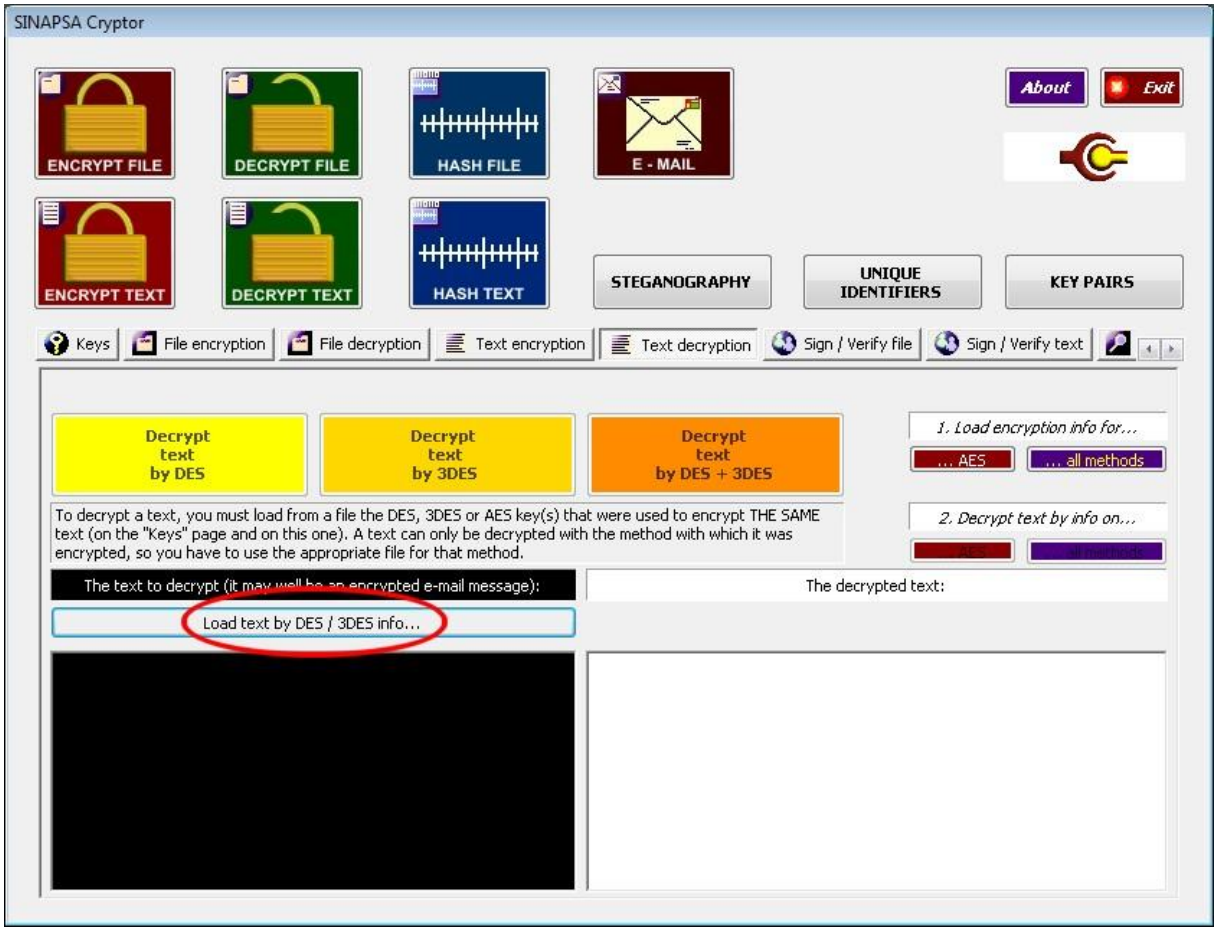
1) În caseta din stânga scrieţi sau preluaţi din Clipboard textul pe care îl veţi cripta.

2) Apoi apăsaţi unul dintre butoanele corespunzătoare metodelor de criptare (DES, 3DES, DES+3DES şi AES). În cazul metodelor DES, fiecare dintre acele butoane va fi activ numai dacă este cunoscută o astfel de cheie; butonul pentru criptarea prin metoda AES este activ permanent.

După ce operaţiunea de criptare reuşeşte vi se va solicita salvarea informaţiei criptografice, pentru ca mai târziu să fie folosită pentru decriptarea aceluiaşi text. Puteţi folosi acea informaţie în pagina "Text decryption" ("Decriptarea unui text").

5. PAGINA "Text decryption" ("Decriptarea unui text")

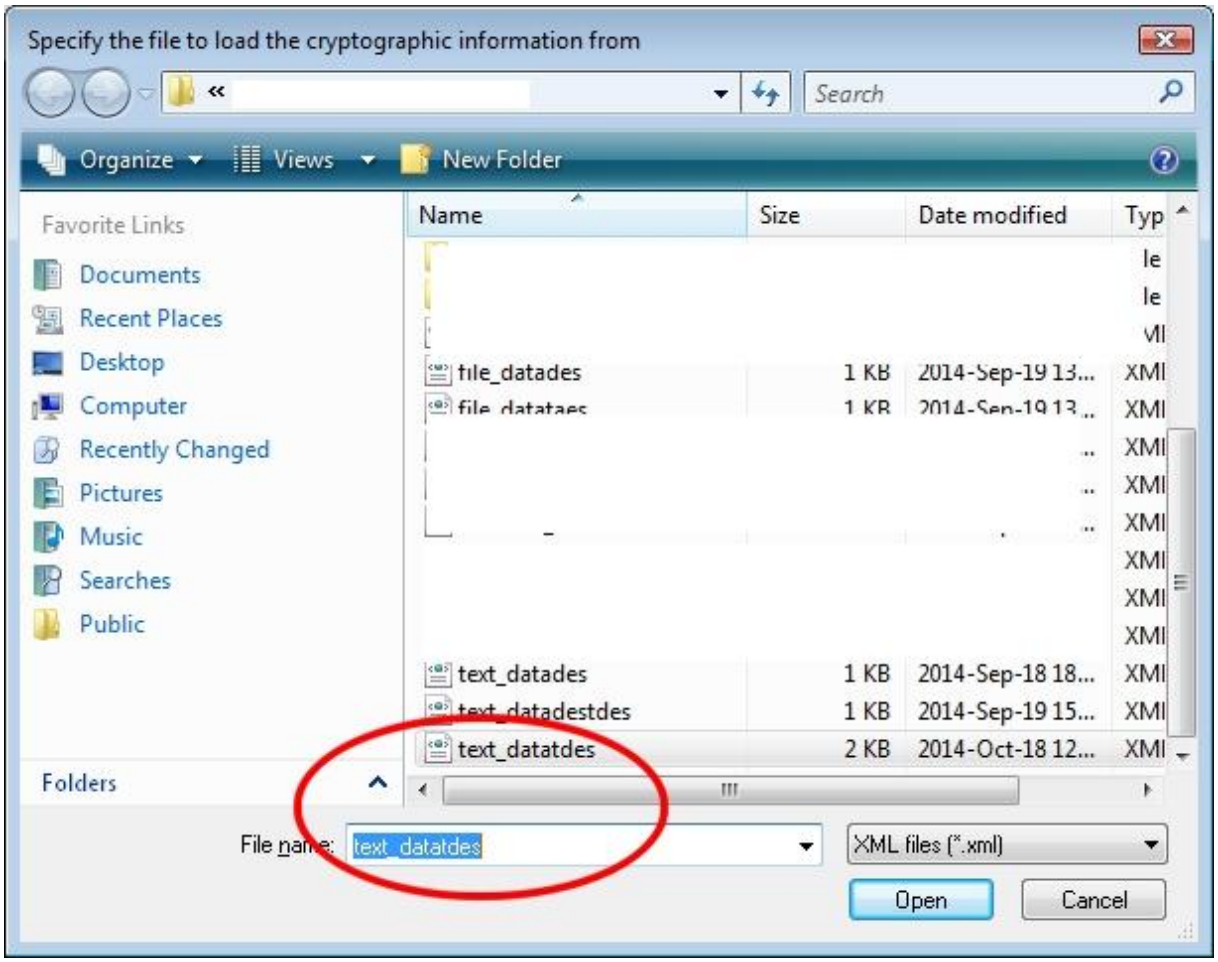
Pe această pagină poate fi decriptat un text prin aceeaşi metodă şi folosind aceeaşi informaţie criptografică folosită la criptarea sa.



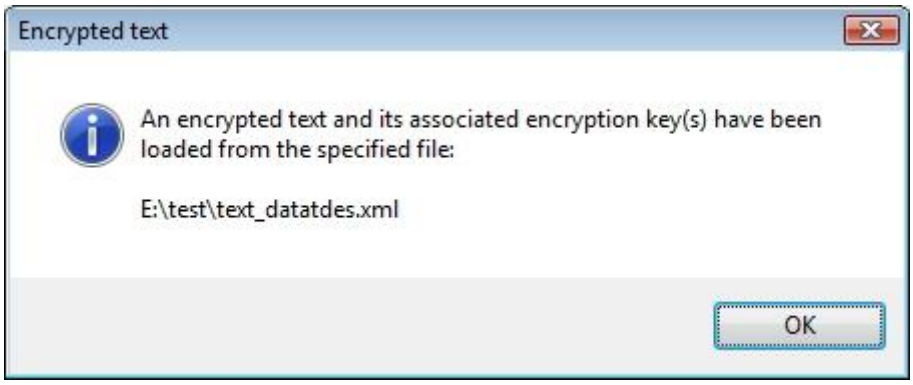
Pentru a decripta un text este neapărat nevoie de încărcarea informaţiei criptografice folosite la criptarea sa; altfel textul nu va putea fi decriptat.

Informaţia respectivă poate fi încărcată din fişiere salvate în cursul criptării textului, apăsând butonul "Load text by DES / 3DES info..." sau butonul "Load AES info about an encrypted text".

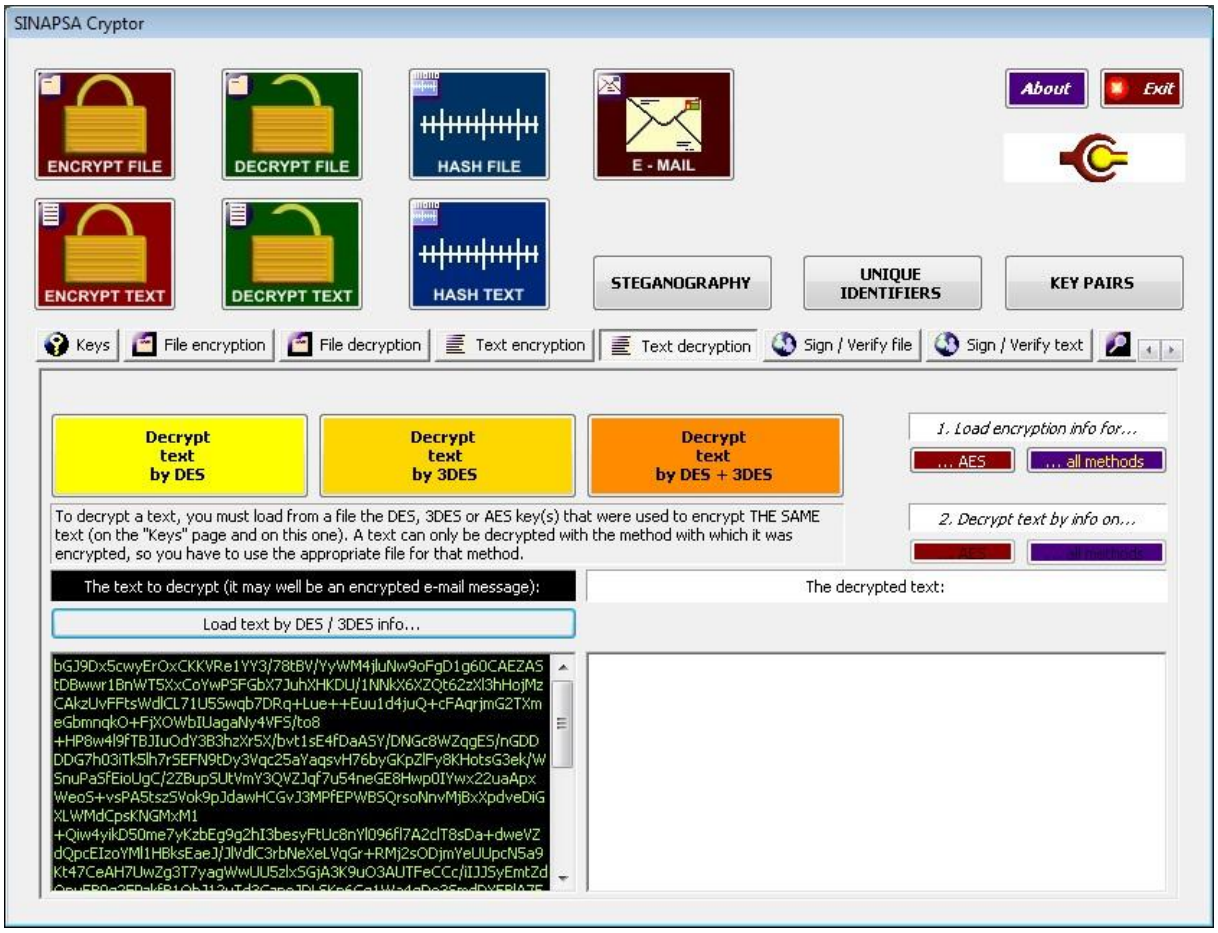
În dialogul care va apărea după ce apăsaţi acel buton vi se va solicita să selectaţi fişierul care conţine informaţia criptografică respectivă. Acel fişier conţine textul criptat şi cheia cu care a fost criptat.



Dacă informaţia criptografică referitoare la decriptarea unui text va putea fi încărcată din fişierul selectat va fi afişat un mesaj care va anunţa aceasta:



În caseta de editare din stânga paginii va fi afişat textul criptat:



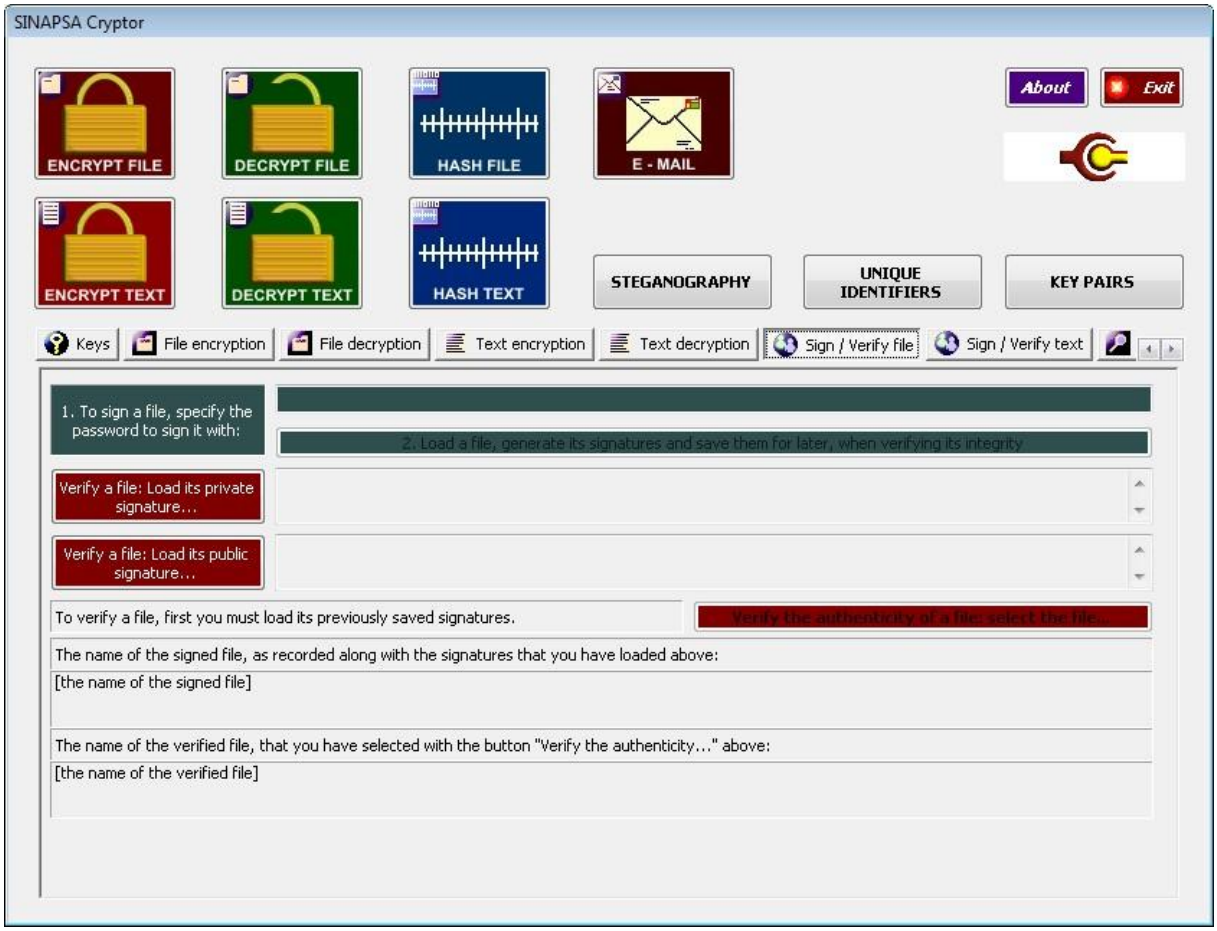
Observaţi cum, deoarece în fişierul cu informaţie criptografică se specificase că textul a fost criptat prin metoda 3DES, butonul "Decrypt text by 3DES" s-a activat. Aşadar, pentru a decripta textul puteţi apăsa acest buton; puteaţi decripta textul şi fără a apăsa butonul, imediat după încărcarea informaţiei criptografice.

Dacă operaţiunea de decriptare reuşeşte, textul decriptat va fi afişat în caseta de editare din dreapta acestei pagini:



6. PAGINA "Sign / Verify file" ("Semnarea / Verificarea unui fişier")

Pe această pagină poate fi folosită metoda de verificare a autenticităţii unui fişier prin metoda "semnăturilor publică şi privată".

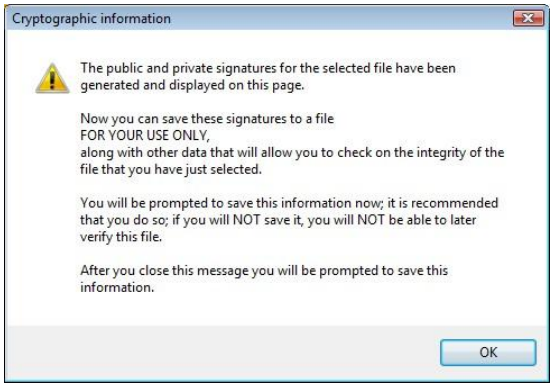


Pentru a determina semnăturile unui fişier procedaţi astfel:

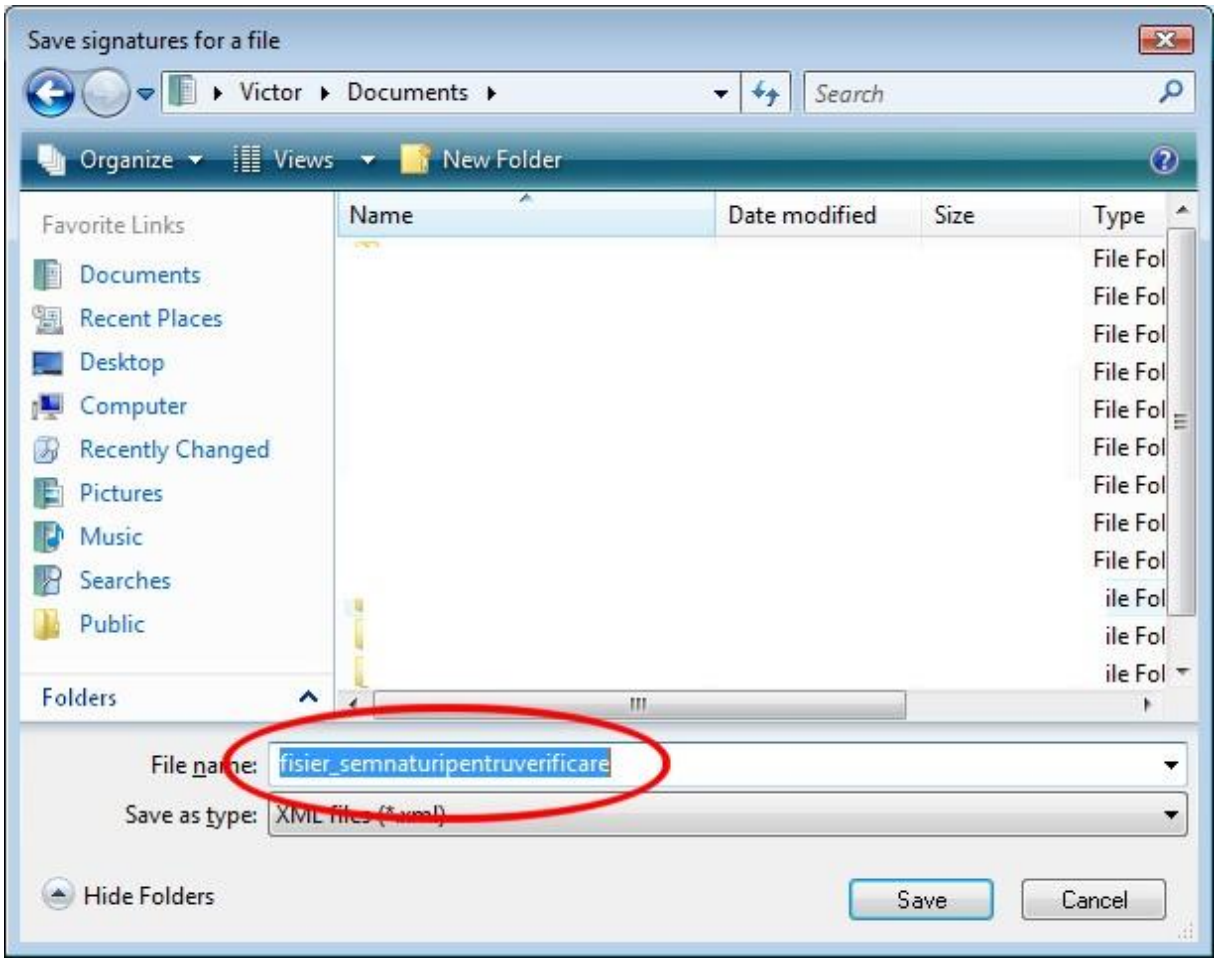
1) în caseta de editare marcată cu eticheta "1. To sign a file, specify the password to sign it with:" specificaţi o parolă pentru generarea semnăturilor fişierului ce va fi verificat ulterior.

2) apoi apăsaţi butonul "2. Load a file, generate its signatures and save them for later, when verifying its integrity") pentru a alege fişierul pe care îl veţi procesa şi pentru a salva informaţia criptografică generată.

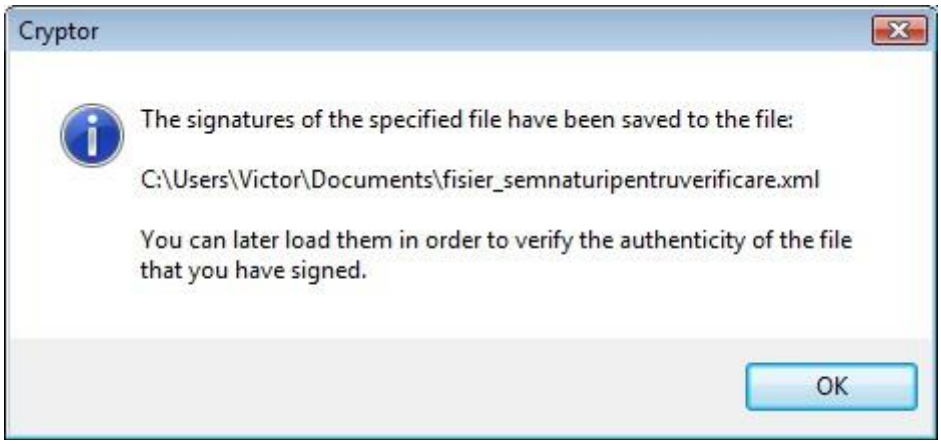
3) după ce alegeţi acel fişier va apărea un dialog ce va anunţa că semnăturile publică şi privată ale fişierului au fost generate şi afişate pe pagină şi vi se va recomanda salvarea lor pentru folosire ulterioară:



În dialogul următor va trebui să specificaţi denumirea fişierului unde va fi salvată informaţia criptografică.

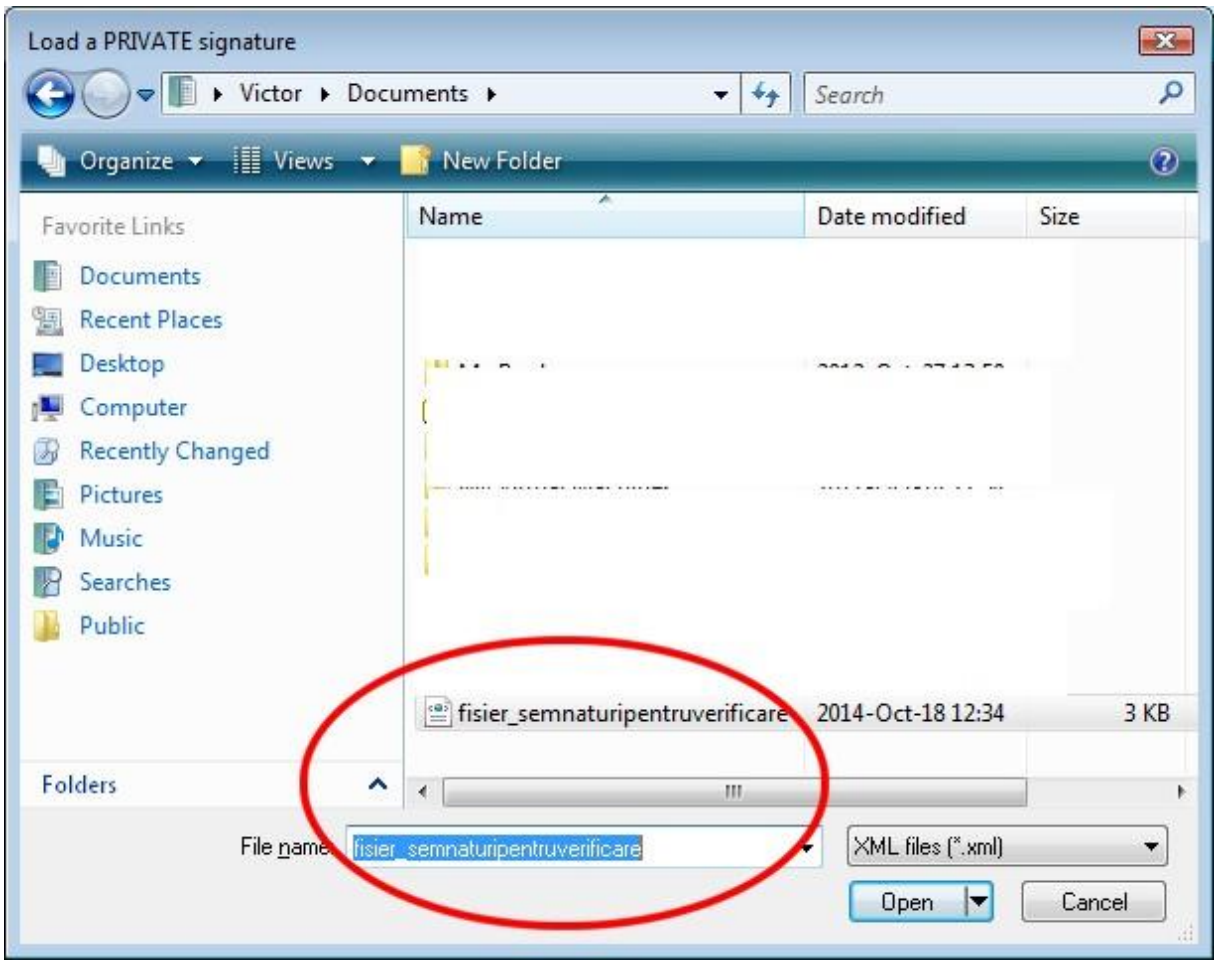


!!! Pentru a verifica autenticitatea fişierului căruia i-au fost detreminate semnăturile va fi nevoie de această informaţie, aşa că trebuie să o salvaţi într-un fişier a cărui denumire să sugereze conţinutul său !!!



Pentru a verifica autenticitatea unui fişier prin semnăturile sale procedaţi astfel:

1) apăsaţi butonul "Verify a file: Load its private signature". În dialogul care va apărea selectaţi fişierul în care aţi salvat informaţia criptografică după determinarea semnăturilor fişierului pe care îl veţi verifica:



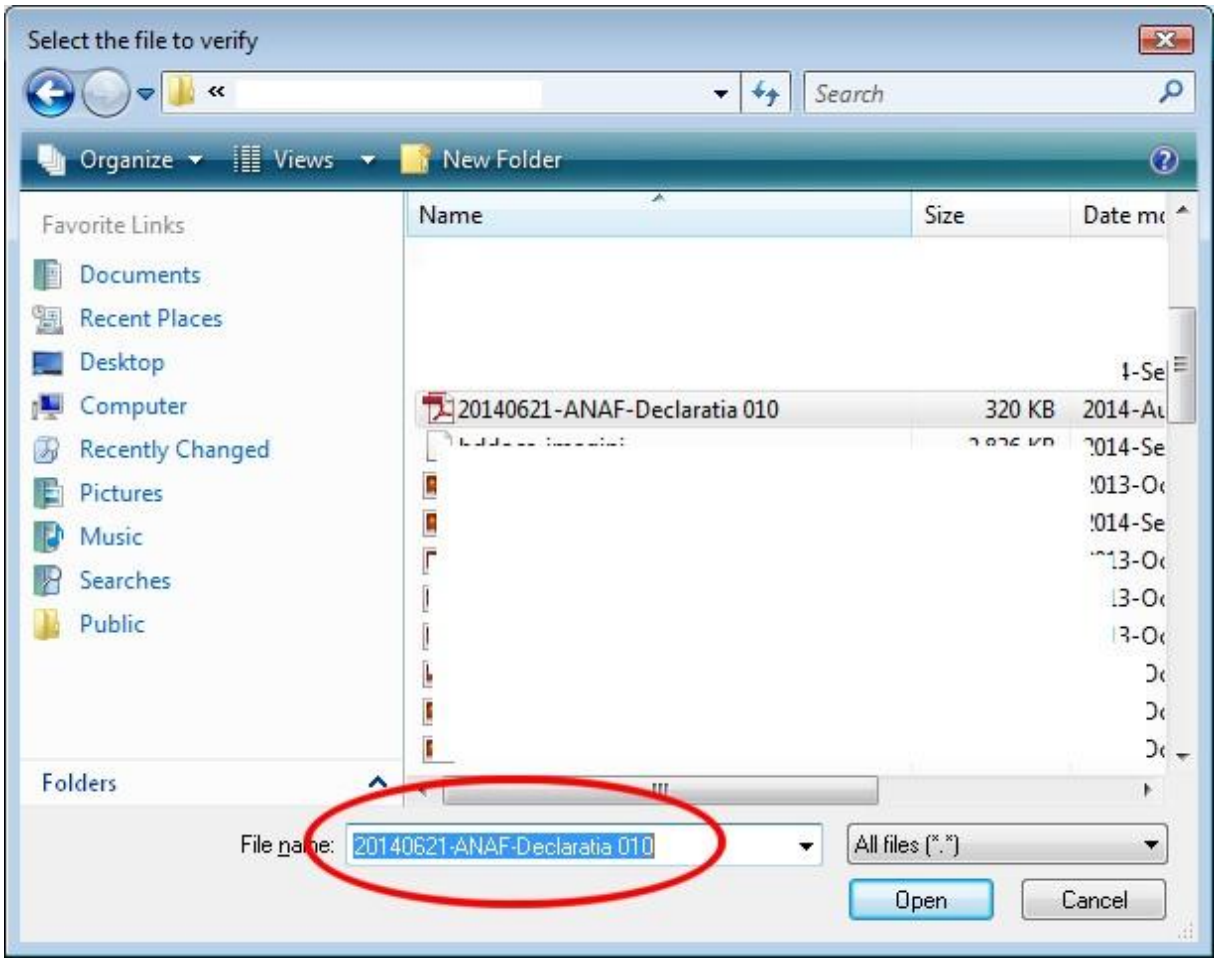
2) apăsaţi butonul "Verify a file: Load its public signature". În dialogul care va apărea selectaţi acelaşi fişier din care aţi încărcat semnătura privată.

Nu contează ordinea în care încărcaţi semnăturile, vor fi afişate oricum.

!!! Totuşi, parola va fi afişată numai după ce încărcaţi semnătura privată, astfel că dacă încărcaţi întâi această semnătură şi apoi pe cea publică parola nu va fi afişată şi nu veţi putea verifica fişierul.

Butonul pentru verificarea auteticităţii unui fişier va fi activ numai dacă sunt afişate ambele semnături şi parola !!!

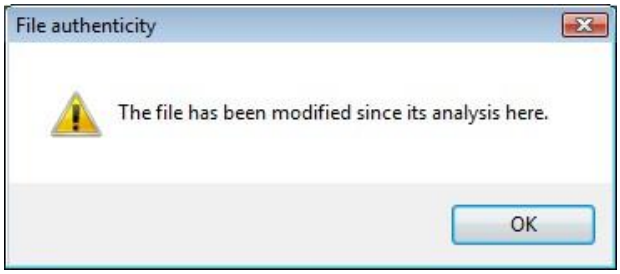
3) apăsaţi butonul "Verify the authenticity of a file: select the file..." ("Verifică autenticitatea unui fişier: selectează fişierul". În dialogul care va apărea selectaţi fişierul a cărui autenticitate vreţi să o verificaţi:



Un mesaj va anunţa dacă fişierul este cel original...

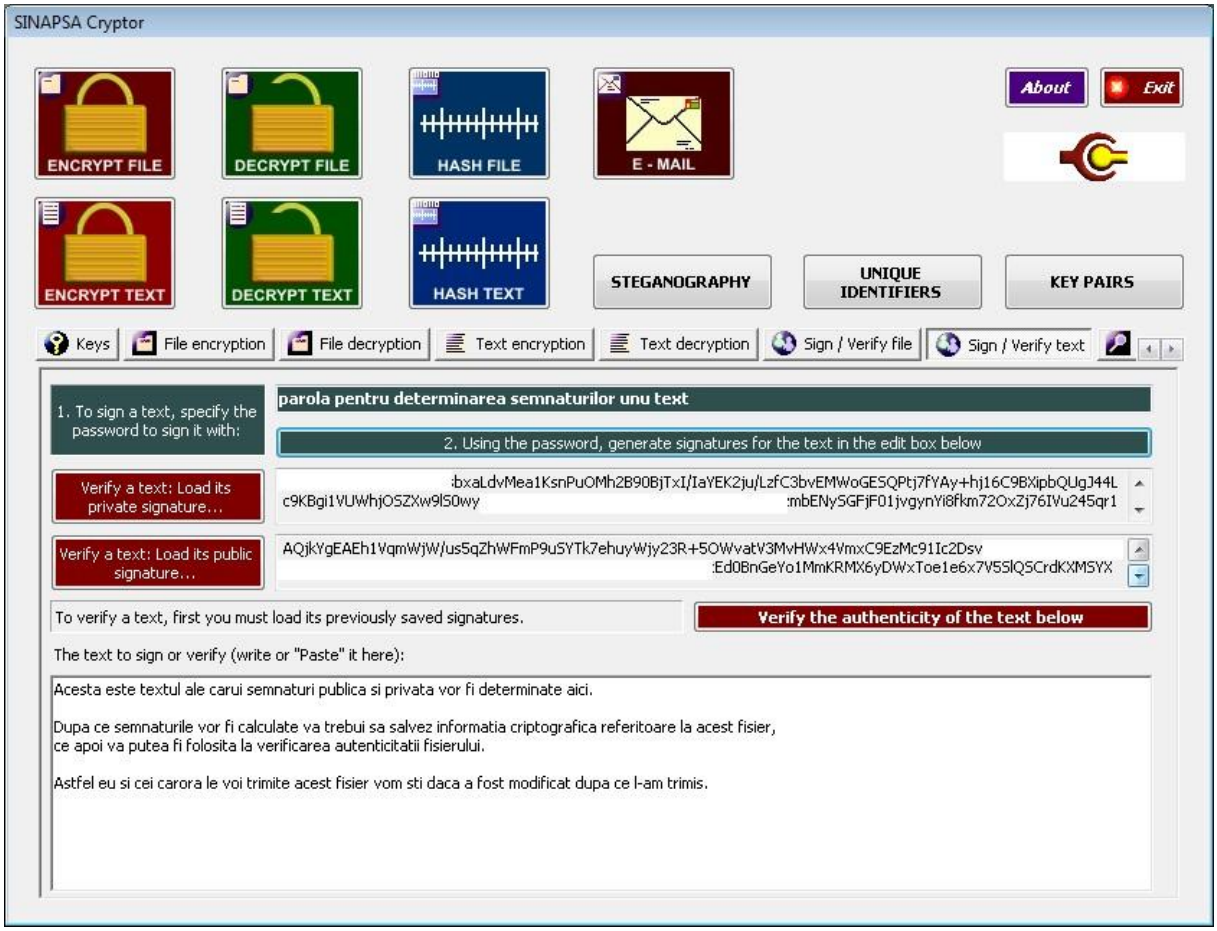


... sau dacă a fost modificat după determinarea semnăturilor sale:



7. PAGINA "Sign / Verify text" ("Semnarea / Verificarea unui text")

Pe această pagină poate fi folosită metoda de verificare a autenticităţii unui text prin metoda "semnăturilor publică şi privată".



Procedurile de urmat pentru verificarea autenticităţii unui text sunt similare celor din cazul verificării autenticităţii unui fişier.

8. PAGINA "Steganography" ("Steganografie")

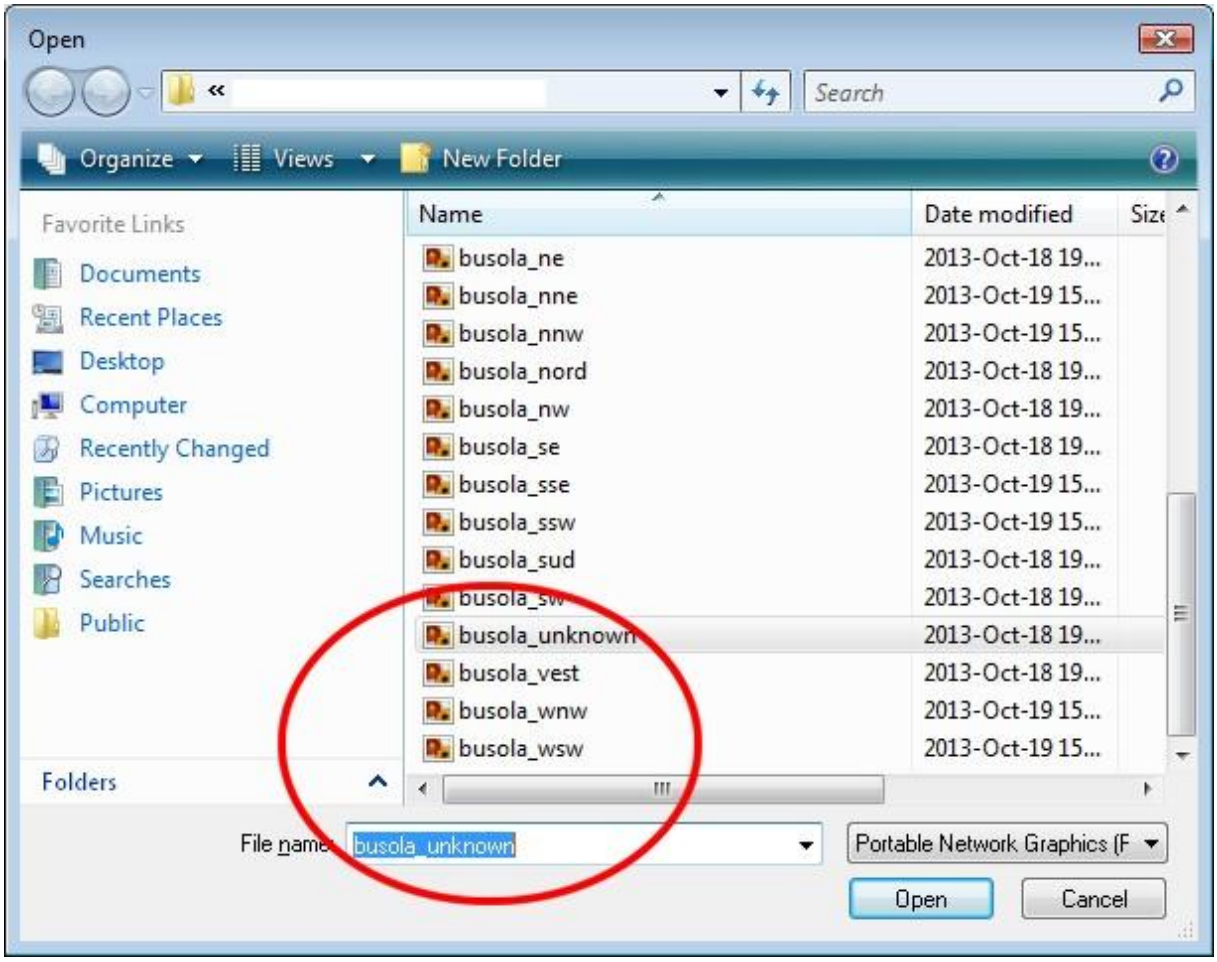
Pe această pagină poate fi ascuns într-o imagine un text ce întâi va fi criptat. De asemenea, un text poate fi recuperat din imaginea în care este ascuns şi poate fi decriptat.

Astfel veţi putea trimite şi citi mesaje "secrete" în forma unor imagini ce conţin textul criptat al mesajelor. Numai cei care vor avea imaginea şi cheia de criptare vor putea citi mesajul.

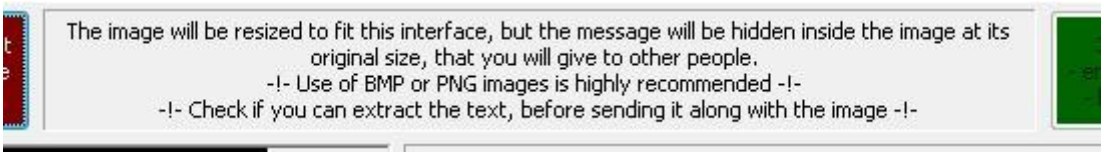
8.1. Ascunderea unui text într-o imagine

1) selectaţi sub-pagina "Steganography: Hide a message" ("Steganografie: Ascunderea unui mesaj")

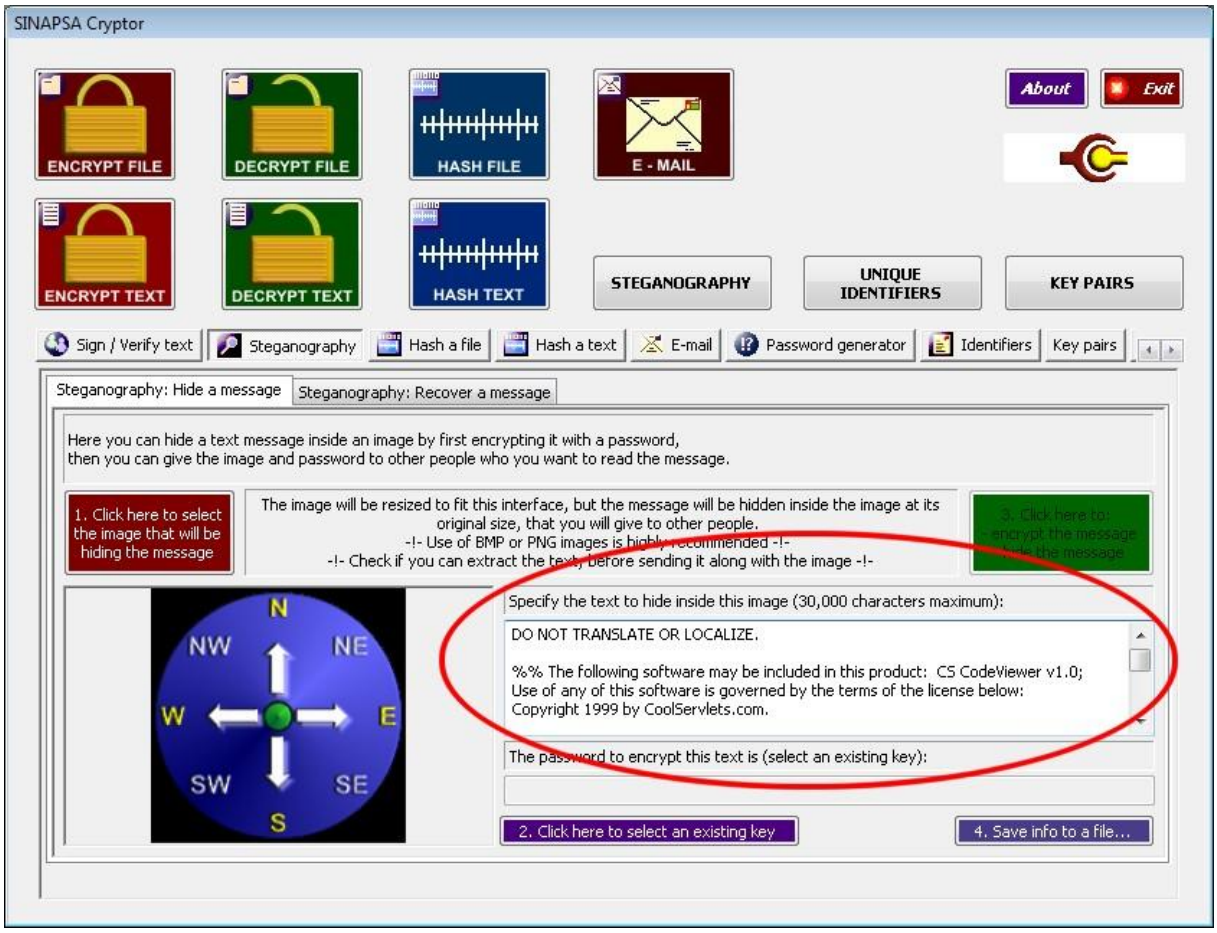
2) apăsaţi butonul "1. Click here to select the image that will be hiding the message" ("Click aici pentru a selecta imaginea ce va ascunde mesajul"). În dialogul ce va apărea alegeţi fişierul-imagine în care veţi ascunde mesajul. Este recomandată folosirea imaginilor din fişiere în formatele Bitmap (.BMP) şi Portable Network Graphics (.PNG):



3) imaginea va fi afişată în stânga acestei pagini. Deşi dimensiunile la care va fi afişată nu sunt cele originale, textul va fi ascuns în imaginea la dimensiunile originale. Informaţia aceasta este prezentată chiar pe pagină:



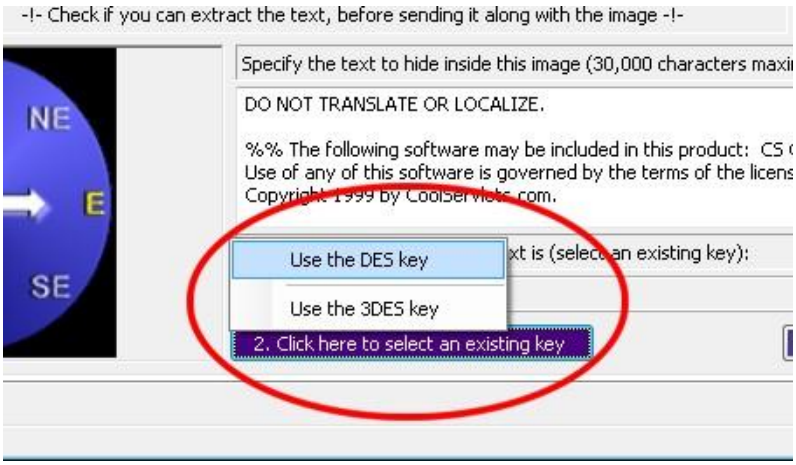
4) specificaţi textul ce va fi criptat şi ascuns în imaginea tocmai afişată. Limita este de 30000 caractere; pentru a trimite mesaje mai lungi puteţi folosi mai multe imagini.



5) selectaţi o cheie de criptare cu care textul va fi criptat:

Apăsaţi butonul "2. Click here to select an existing key" ("Click aici pentru a selecta o cheie existentă deja").

Dacă încă nu este cunoscută nicio cheie DES sau 3DES va fi afişat un mesaj de atenţionare prin care vi se va spune că puteţi crea şi încărca astfel de chei pe pagina "Keys" ("Chei"); altfel, dacă după ce apăsaţi acest buton veţi putea selecta una din meniul ce se deschide:



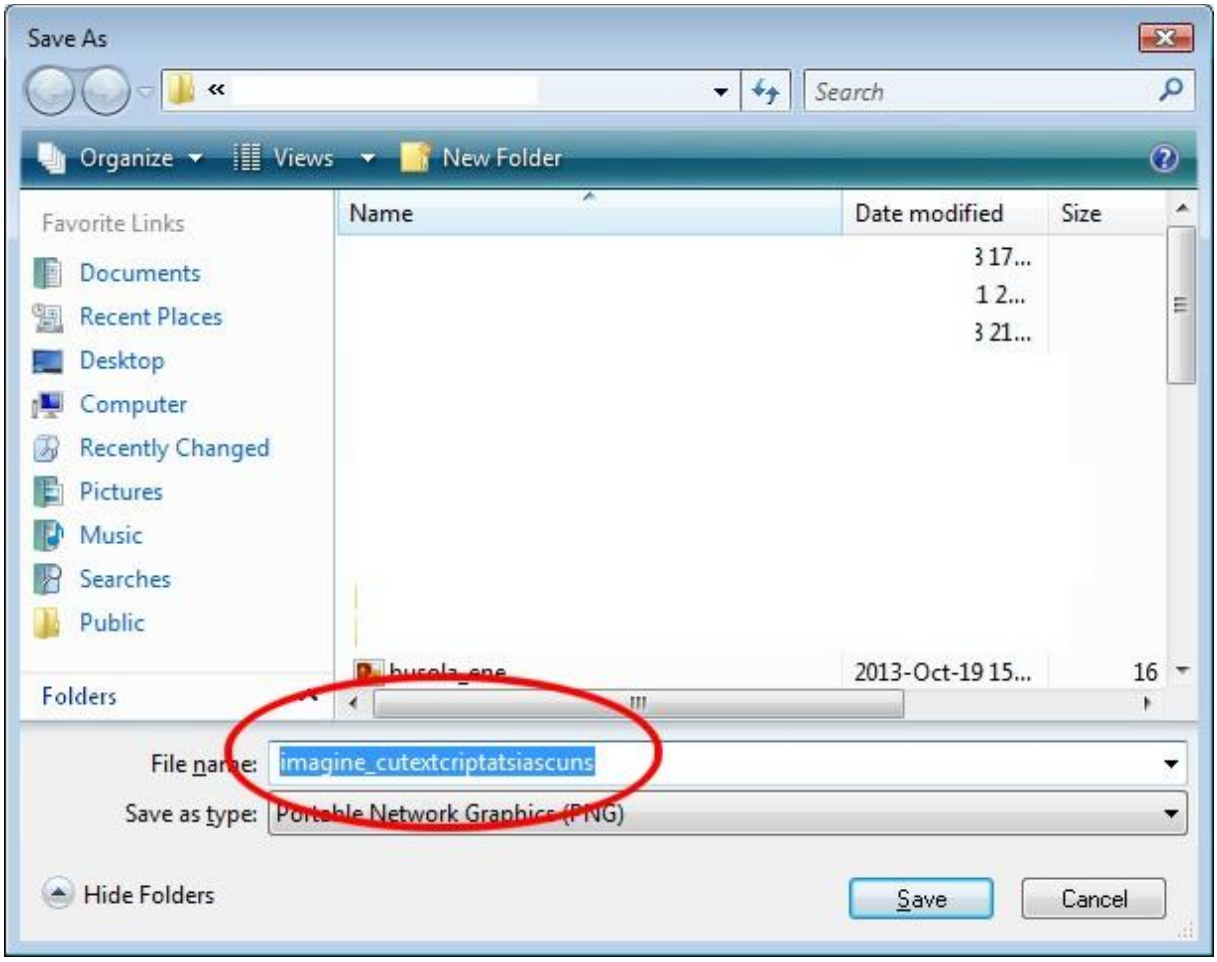
6) după ce selectaţi o cheie din acel meniu va fi activat butonul "3. Click here to: - encrypt the message; - hide the message" ("3. Click aici pentru a: - cripta mesajul; - ascunde mesajul").

Va fi afişat un mesaj ce spune că după ce criptarea reuşeşte vi se va solicita denumirea fişierului-imagine ce va conţine acel mesaj şi că dacă vreţi să trimiteţi mesajul cuiva trebuie să îi trimiteţi atât fişierul-imagine pe care îl veţi salva imediat, cât şi cheia de criptare a mesajului dinăuntrul imaginii:



Apăsaţi butonul "OK" pentru a salva informaţia criptografică referitoare la mesajul din imagine.

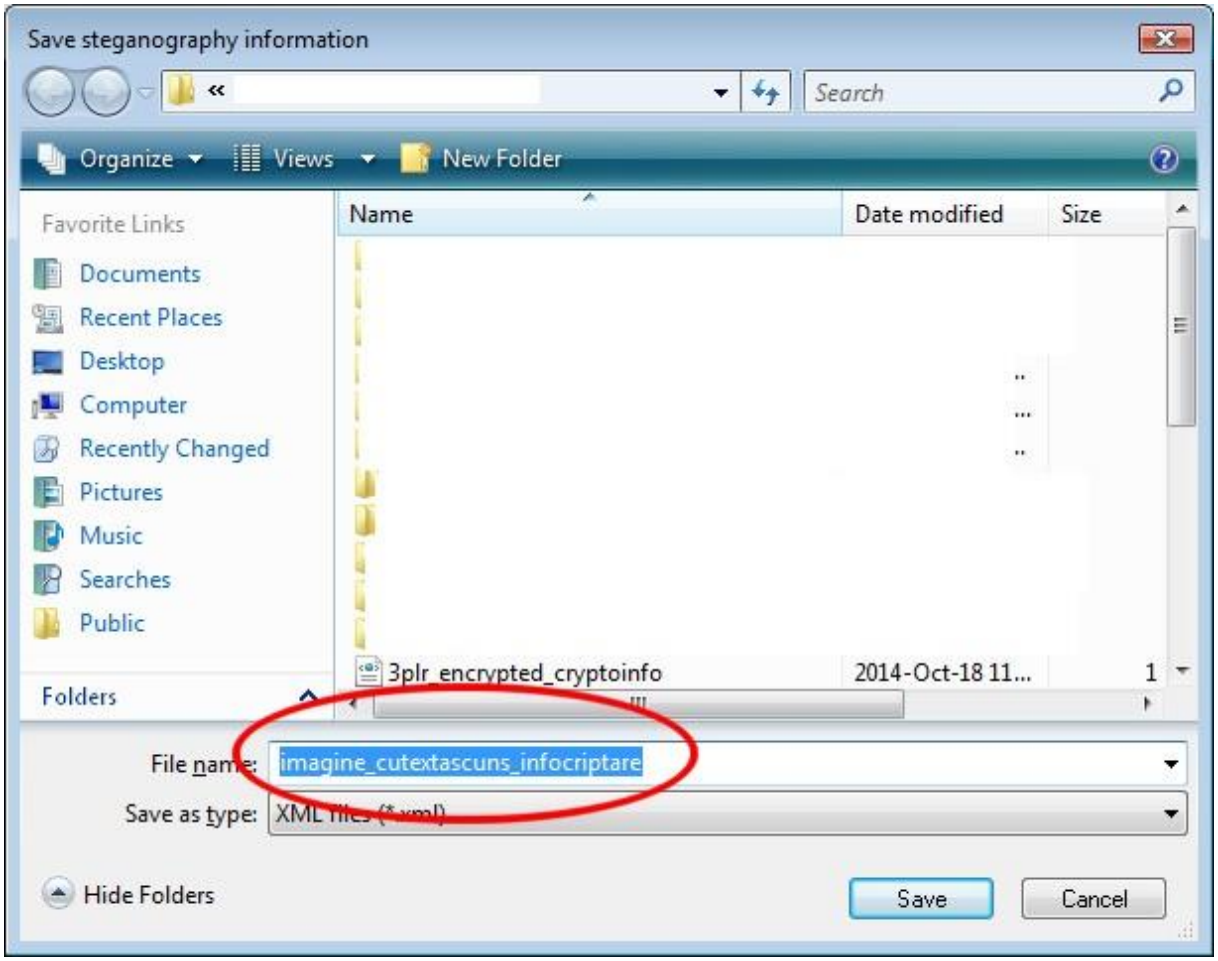
7) În dialogul ce va apărea vi se va solicita denumirea fişierului-imagine ce va conţine textul criptat:



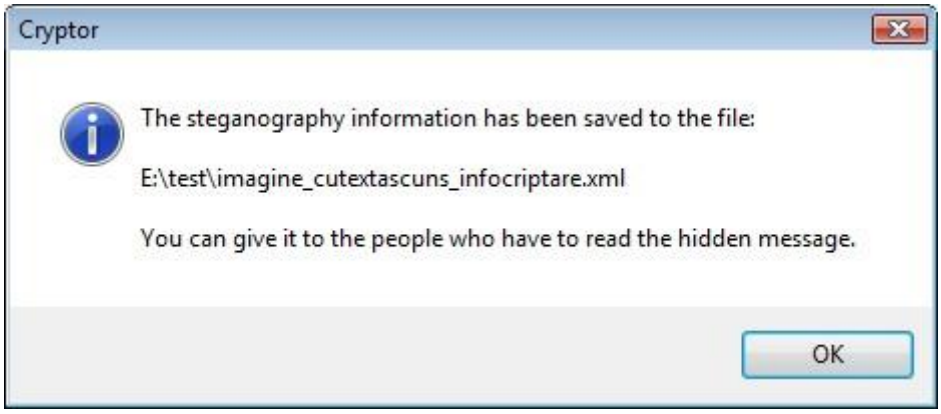
8) După ce salvaţi imaginea ce conţine textul criptat va fi afişat un mesaj ce vă recomandă să salvaţi informaţia criptografică, fără de care textul nu va putea fi recuperat din imagine:



9) Apăsaţi butonul "OK". În dialogul următor vi se va solicita denumirea fişierului în care va fi salvată informaţia criptografică referitoare la txetul criptat şi ascuns în imaginea pe care aţi salvat-o în pasul anterior:



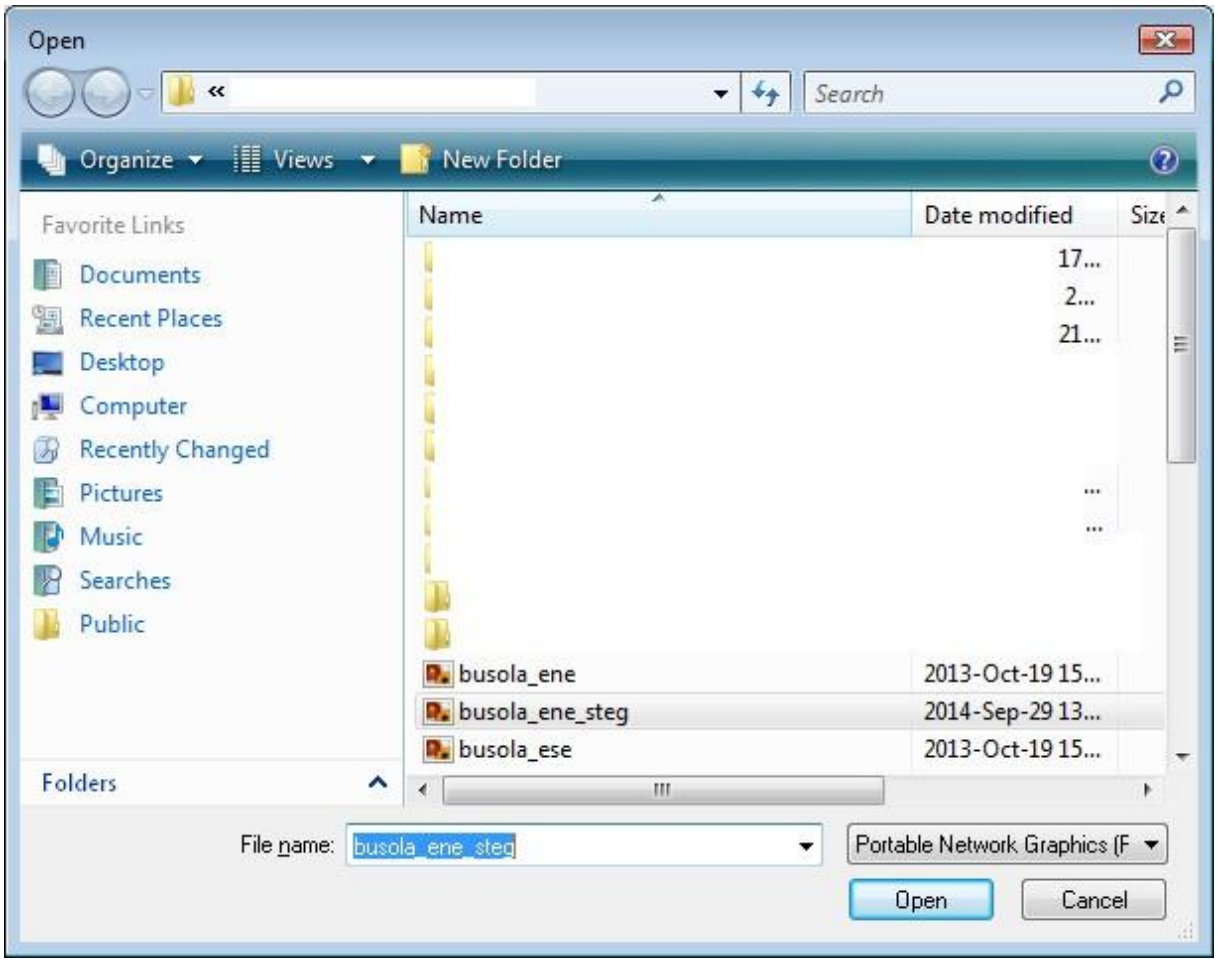
10) Un mesaj vă va anunţa că informaţia criptografică necesară pentru a recupera textul criptat şi ascuns în imagine a fost salvată în fişierul specificat şi că va trebui să trimiteţi acest fişier şi imaginea persoanelor care vreţi să citească acel text:



8.2. Recuperarea unui text ascuns într-o imagine şi decriptarea sa

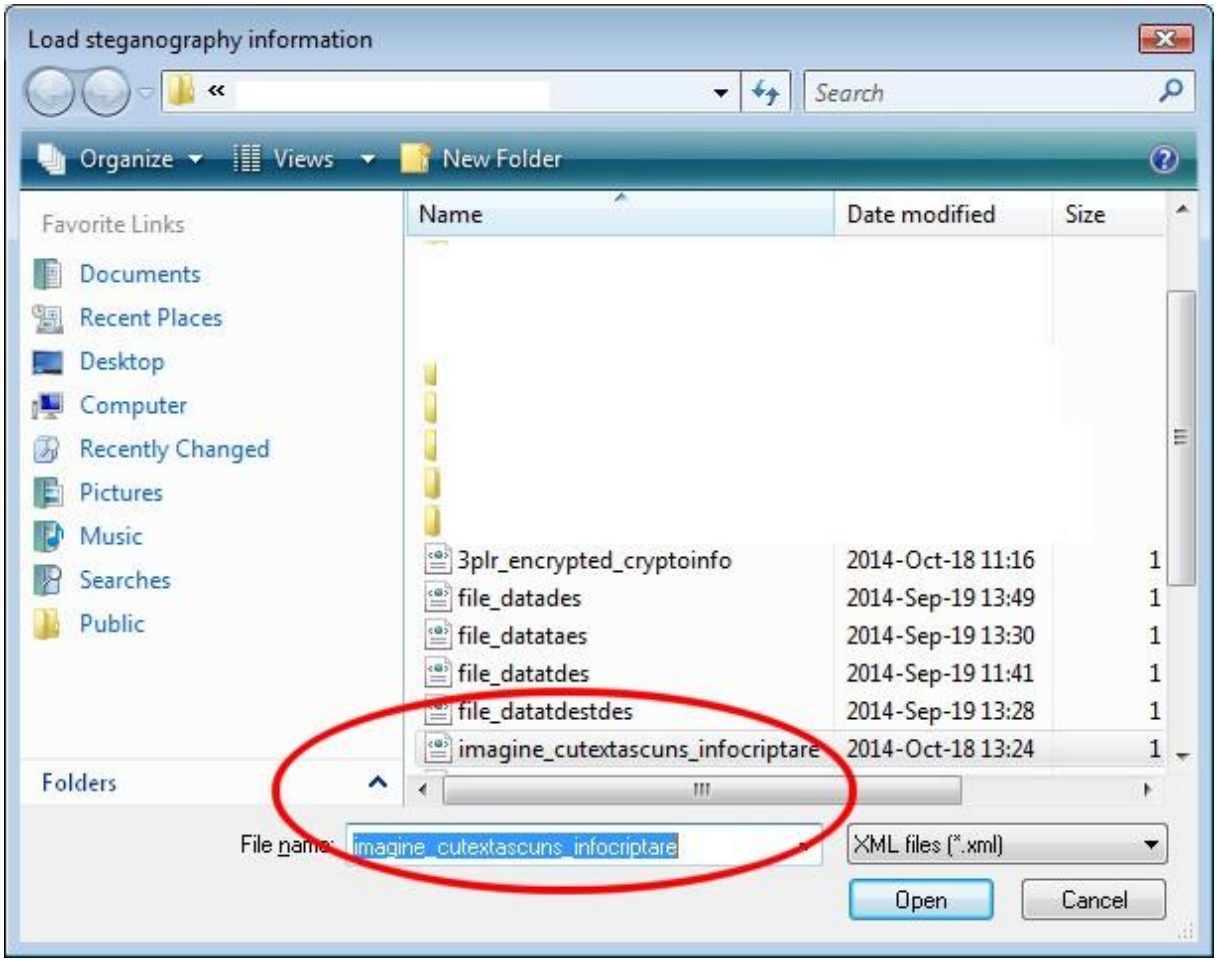
1) selectaţi sub-pagina "Steganography: Recover a message" ("Steganografie: Recuperarea unui mesaj")

2) apăsaţi butonul "1. Click here to select the image that holds the message" ("Click aici pentru a selecta imaginea ce conţine mesajul")



3) imaginea, la dimensiuni adaptate acestei pagini, va fi afişată în stânga paginii.

4) încărcaţi informaţia criptografică referitoare la această imagine şi la textul criptat şi ascuns înăuntrul său: apăsaţi butonul "2'. Load info from a file..." ("2'. Încărcaţi informaţie dintr-un fişier..."). În dialogul ce va apărea alegeţi fişierul în care ştiţi că se află acea informaţie:

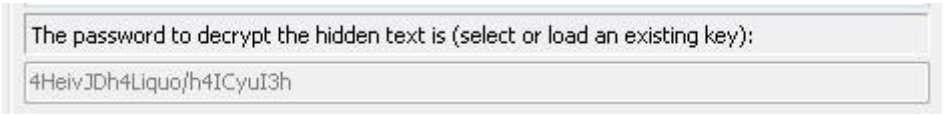


!!! Textul va putea fi decriptat NUMAI cu informaţia criptografică salvată în cursul procedurii de criptare şi ascundere a sa în imagine.

Orice pereche necorespunzătoare imagine + informaţie criptografică nu va putea descifra textul criptat şi ascuns.

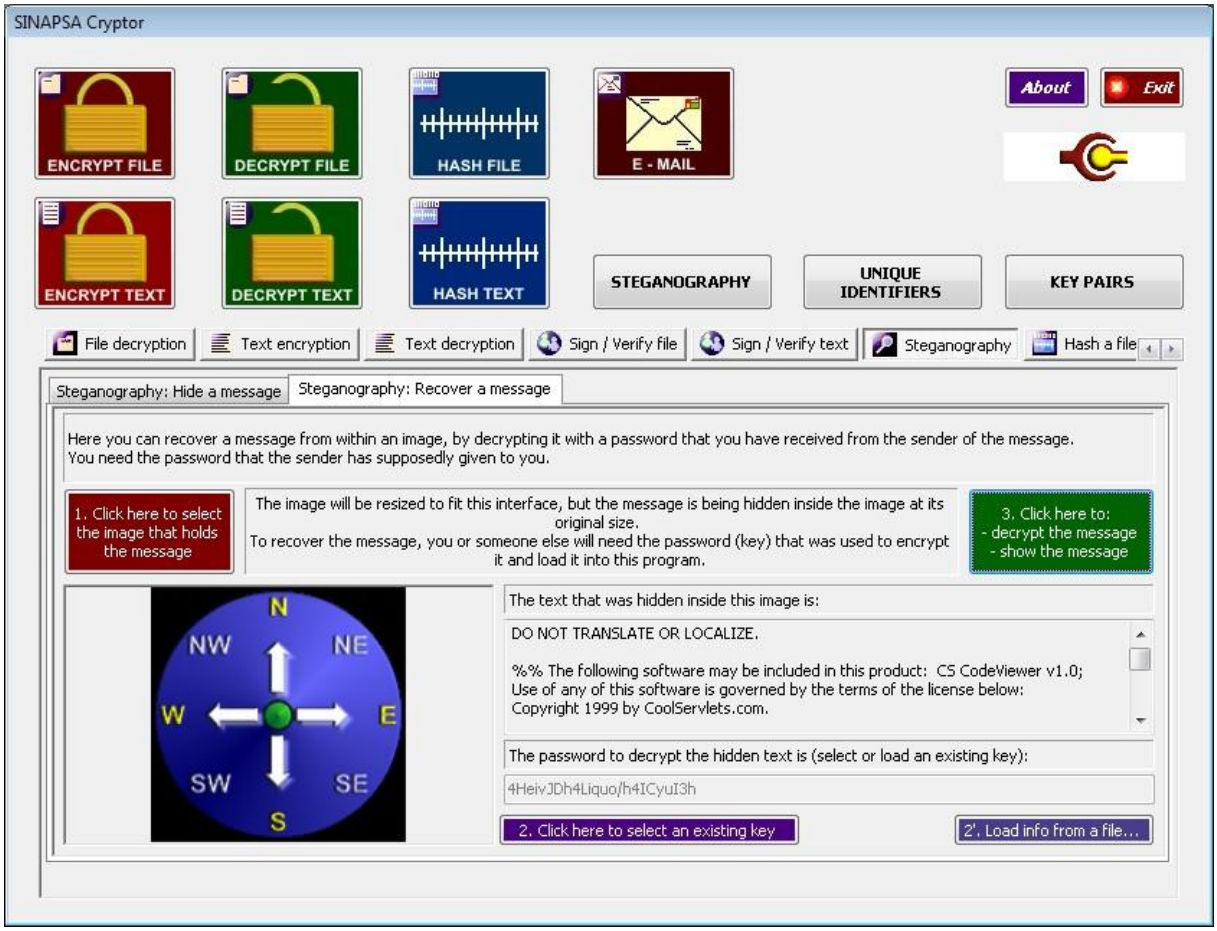
Aşa că trebuie să acordaţi atenţie maximă TUTUROR procedurilor de steganografiere !!!

5) după ce alegeţi fişierul în care se află informaţia pentru recuperarea şi decriptarea textului ascuns în imagine apăsaţi butonul "Open" sau similar al dialogului anterior. Veţi vedea cum pe această sub-pagină va fi afişată cheia de criptare sau "parola" cu care a fost criptat textul din imagine:



6) pentru a decripta şi citi textul ascuns în imagine apăsaţi butonul "3. Click here to: - decrypt the message; - show the message" ("3. Click aici pentru a: - decripta mesajul; - afişa mesajul").

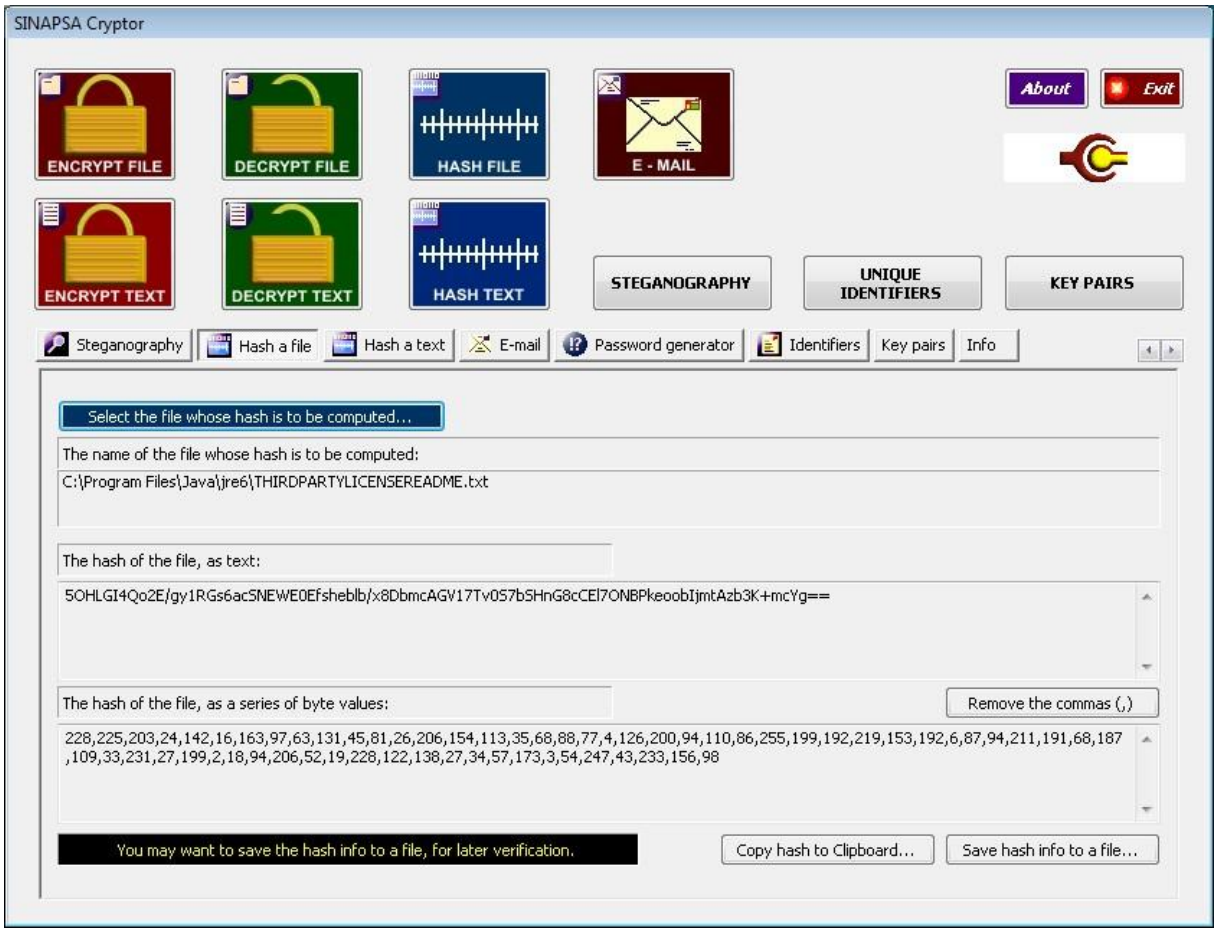
Dacă decriptarea reuşeşte, textul ascuns în imagine va fi afişat în forma sa decriptată, în caseta de editare din dreapta acestei sub-pagini:



9. PAGINA "Hash a file" ("Calcularea *hash*-ului unui fişier")

Pe această pagină poate fi calculată funcţia *hash* a unui fişier, adică reprezentarea într-o secvenţă de caractere a informaţiei din acel fişier.

Această procedură, similar cu cea care determină "semnăturile" unui fişier poate fi folosită pentru verificarea autenticităţii unui fişier.

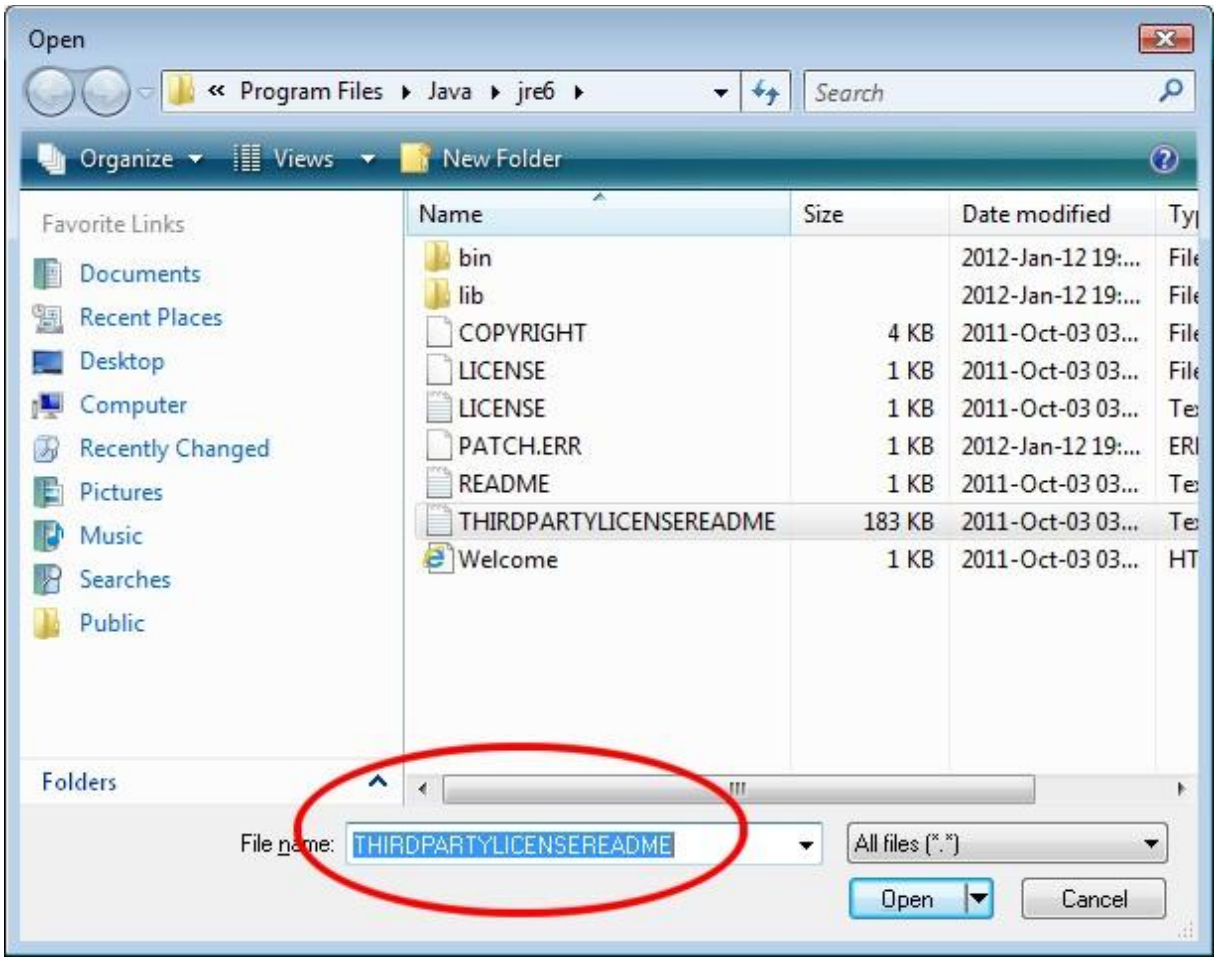


În exemplul din imaginea precedentă se vede cum a fost calculat *hash*-ul unui fişier a cărui denumire este afişată sub eticheta "The name of the file whose hash is to be computed:" ("Fişierul al cărui *hash* va fi calculat:").

Ca în cazul celorlaltor operaţiuni criptografice, pentru ca o persoană să poată verifica autenticitatea fişierului trebuie ca după calcularea *hash*-ului informaţia criptografică rezultată să fie salvată; apoi, cei care vor verifica fişierul vor putea calcula la rându-le *hash*-ul său şi vor compara cele două secvenţe.

Pentru a calcula *hash*-ul unui fişier:

- selectaţi fişierul al cărui *hash* va fi calculat prin apăsarea butonului menţionat anterior. În dialogul care va apărea alegeţi fişierul:



După ce apăsaţi butonul "Open" al acestui dialog *hash*-ul va fi calculat automat şi va fi afişat pe pagină, după cum se vede în prima imagine a acestui punct.

Pe această pagină puteţi întreprinde diverse acţiuni asupra *hash*-ului, anume:

- copierea în Clipboard a uneia dintre cele două forme ale sale (textul ca secvenţă de caractere şi secvenţa de numere/valori ale octeţilor-bytes): apăsaţi butonul "Copy hash to Clipboard" şi selectaţi intrarea de meniu preferată:



- îndepărtarea virgulelor din secvenţa de numere: apăsaţi butonul "Remove the commas (,)" ("Ştergerea virgulelor")

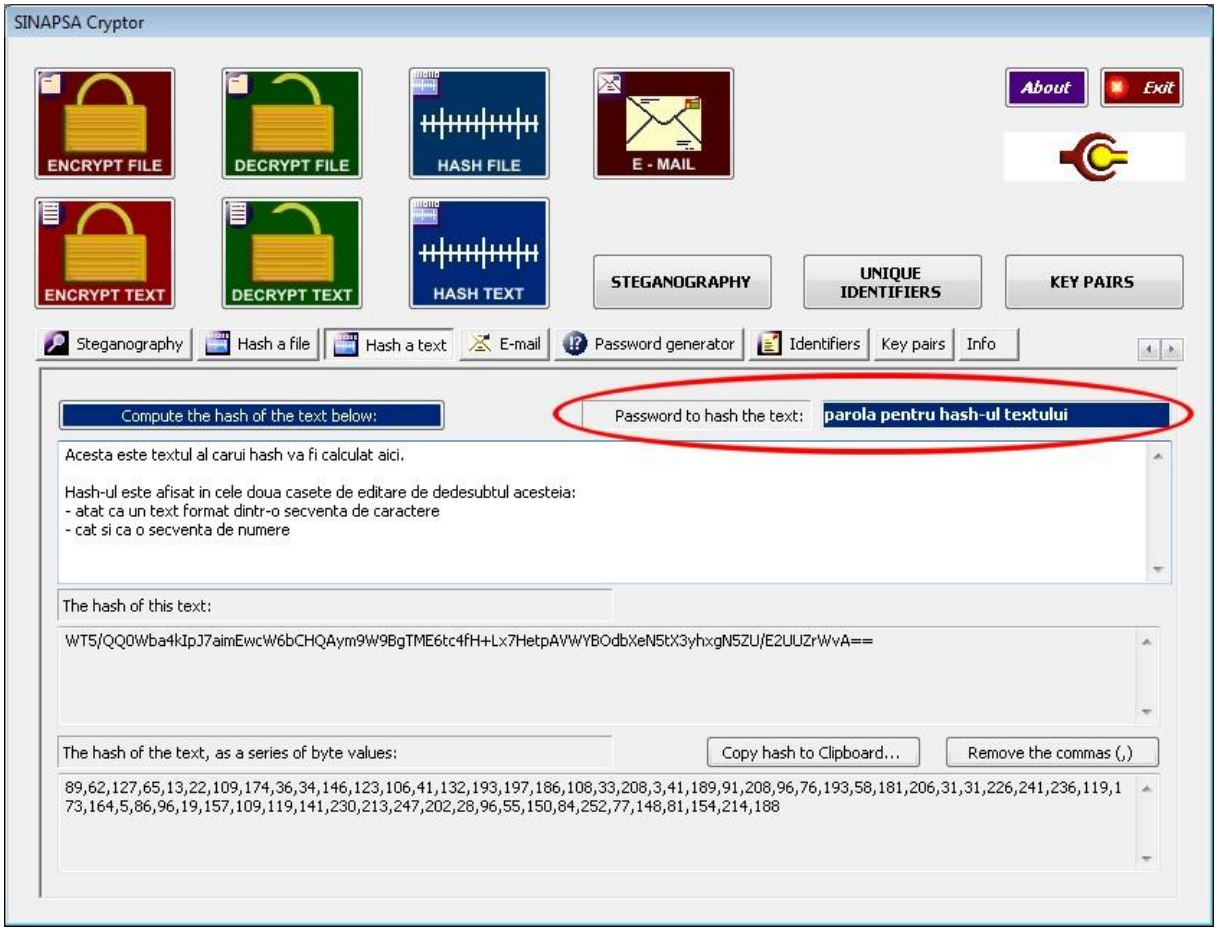
- salvarea *hash*-ului într-un fişier dedicat; cei care vor verifica fişierul al carui *hash* a fost calculat aici vor putea calcula la rându-le *hash*-ul său şi vor compara cele două secvenţe: apăsaţi butonul "Save hash info to a file...".

10. PAGINA "Hash a text" ("Calcularea *hash*-ului unui text")

Pe această pagină poate fi calculată funcţia *hash* a unui text, adică reprezentarea într-o secvenţă de caractere a acelui text.

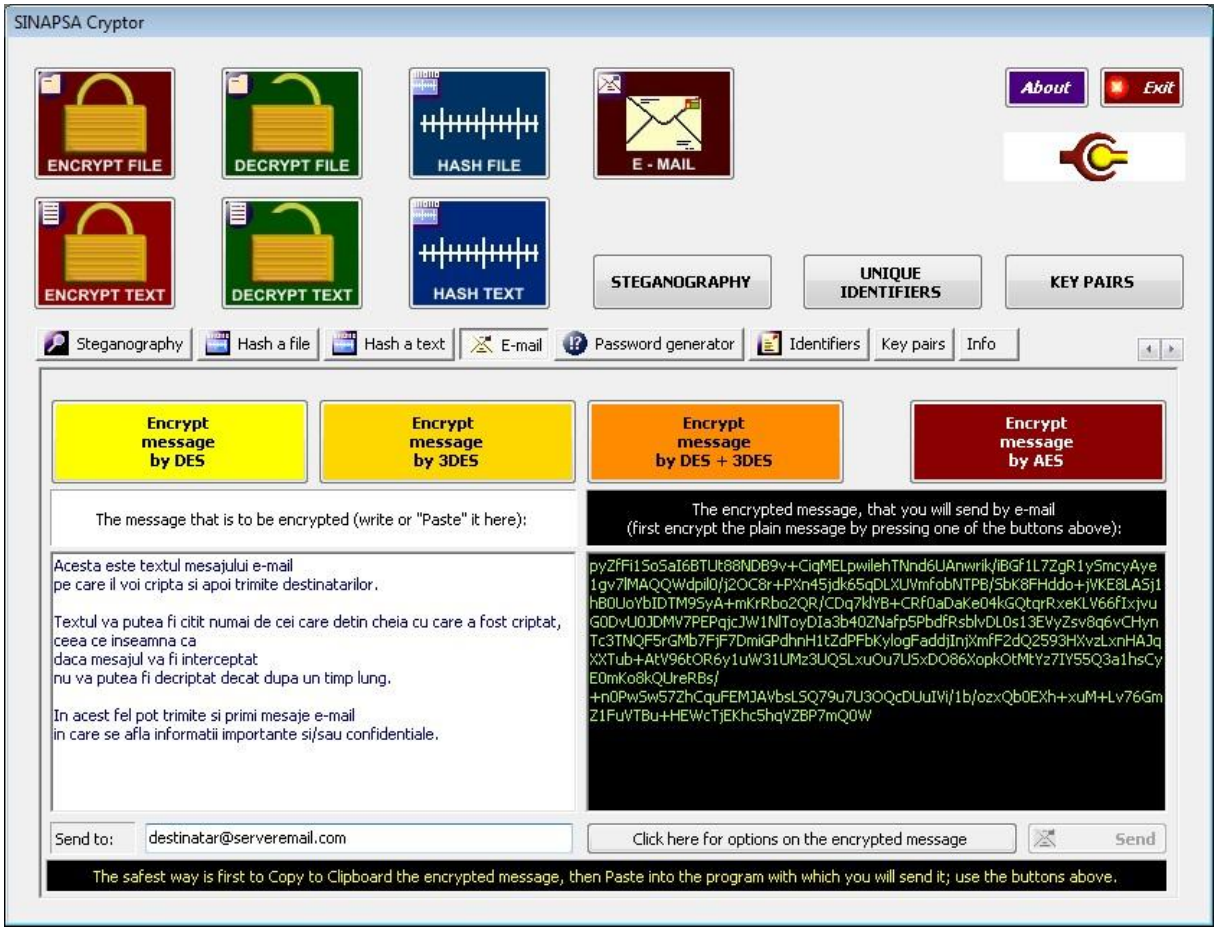
Această procedură este similară celei de calculare a *hash*-ului unui fişier, prezentată anterior.

Spre deosebire de aceea, însă, *hash*-ul textului va fi calculat în acord cu o parolă pe care trebuie să o scrieţi în caseta de editare respectivă (vezi imaginea de mai jos); dacă nu specificaţi nicio parolă, *hash*-ul va fi calculat în acord cu textul nul (adică niciun text).



11. PAGINA "E-mail" ("Poştă electronică")

Pe această pagină puteţi cripta textul unui mesaj e-mail, astfel încât numai cei care deţin cheia de criptare să îl poată citi.



Pentru a folosi metodele de criptare prin DES, 3DES sau DES+3DES este nevoie respectiv de o cheie DES, sau de una 3DES, sau de ambele. În cazul în care vreţi să folosiţi astfel de chei trebuie ca întâi fie să le creaţi pe pagina "Keys", fie să le încărcaţi din fişiere în care au fost salvate anterior; butoanele corespunzătoare acestor metode vor fi active numai dacă astfel de chei sunt cunoscute.

Pentru a folosi metoda de criptare prin AES, apăsaţi butonul "Encrypt message by AES" ("Criptarea mesajului prin AES"); acest buton este activ permanent.

Această procedură este similară celei de criptare a unui text oarecare, disponibilă pe pagina "Text encryption"; însă, pentru a ţine socoteala celor efectuate este bine să faceţi operaţiunile dedicate mesajelor e-mail pe această pagină.

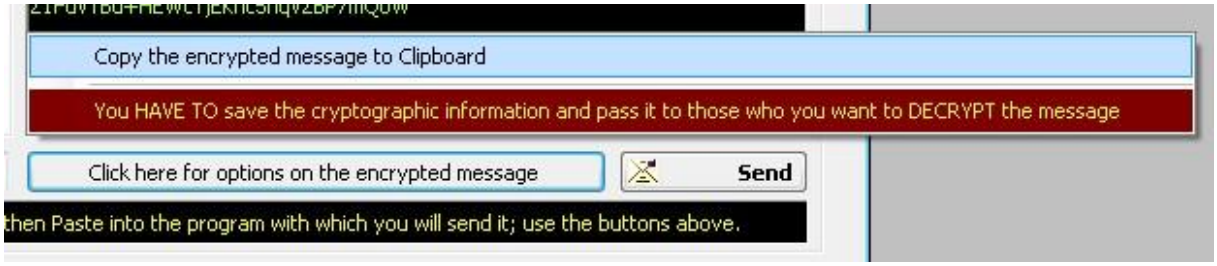
În imaginea de mai sus se vede cum textul unui mesaj e-mail a fost criptat (prin metoda 3DES); în stânga este textul original, iar în dreapta forma sa criptată, pe care o puteţi trimite destinatarilor împreună cu cheia necesară decriptării sale.

Adresele e-mail ale destinatarilor pot fi scrise în caseta de editare din stânga-jos pe această pagină.

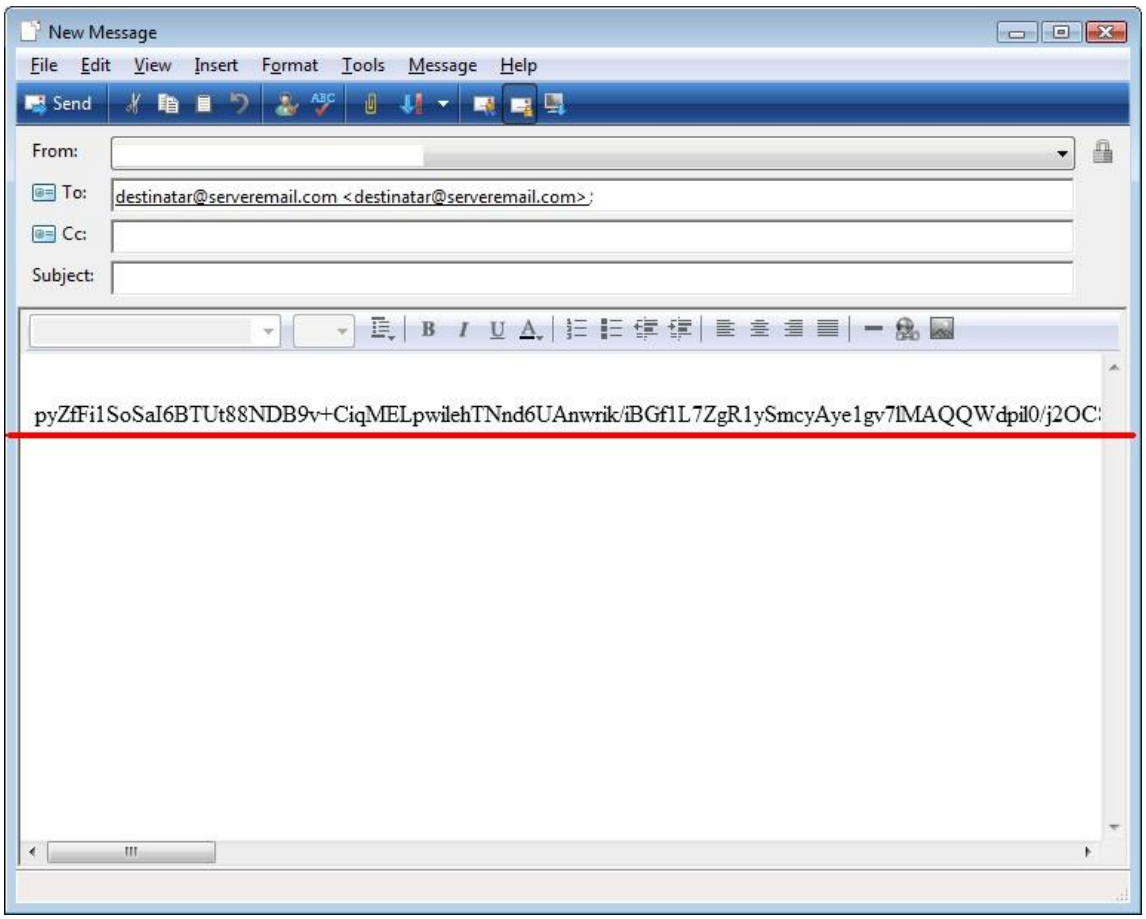
Butonul "Send" ("Trimitere") din dreapta-jos va fi activ numai dacă următoarele trei condiţii sunt îndeplinite:

- dacă textul criptat este afişat;
- dacă există adrese oarecare ale destinatarilor;
- dacă textul criptat a fost copiat în Clipboard.

Înainte de a putea trimite mesajul cu textul criptat, acesta trebuie copiat în Clipboard din motive ce ţin de securitatea sistemului de operare. Odată deschis programul implicit folosit pentru trimiterea mesajelor e-mail, acel text va putea fi preluat din Clipboard cu metoda "Paste" (combinaţia de taste Ctrl + V).



Pentru a deschide programul respectiv apăsaţi butonul "Send"; dacă sistemul de operare va înţelege comanda acel program va fi deschis şi veţi putea trimite mesajul:



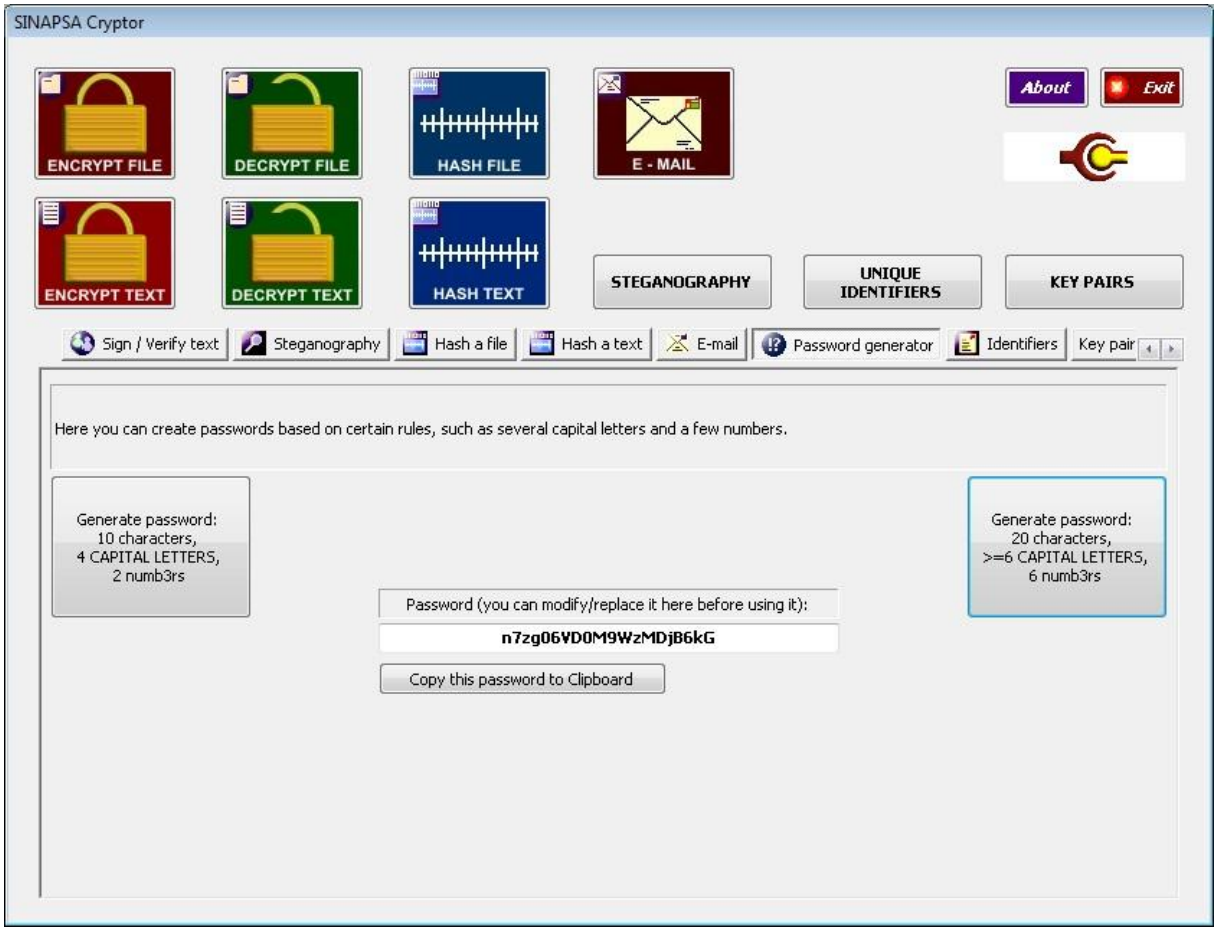
Dacă lungimea textului criptat nu depăşeşte o anumită valoare, acesta va fi plasat automat în caseta de editare a programului implicit de e-mail destinată textului mesajului; însă cel mai sigur este să folosiţi metoda "Paste" pentru a plasa manual textul în program, indiferent de lungimea textului.

Un mesaj criptat primit prin e-mail poate fi decriptat ca orice text, pe pagina "Text decryption".

12. PAGINA "Password generator" ("Creator de parole")

Pe această pagină puteţi genera parole ce se supun anumitor criterii, de exemplu un număr de litere majuscule şi câteva numere.

În versiunile 2.x ale CRYPTOR-ului sunt disponibile două modele de parole, anume alcătuite din:
- 10 caractere, dintre care 2 numere şi 4 majuscule;
- 20 caractere, dintre care 6 numere şi cel puţin 6 majuscule.



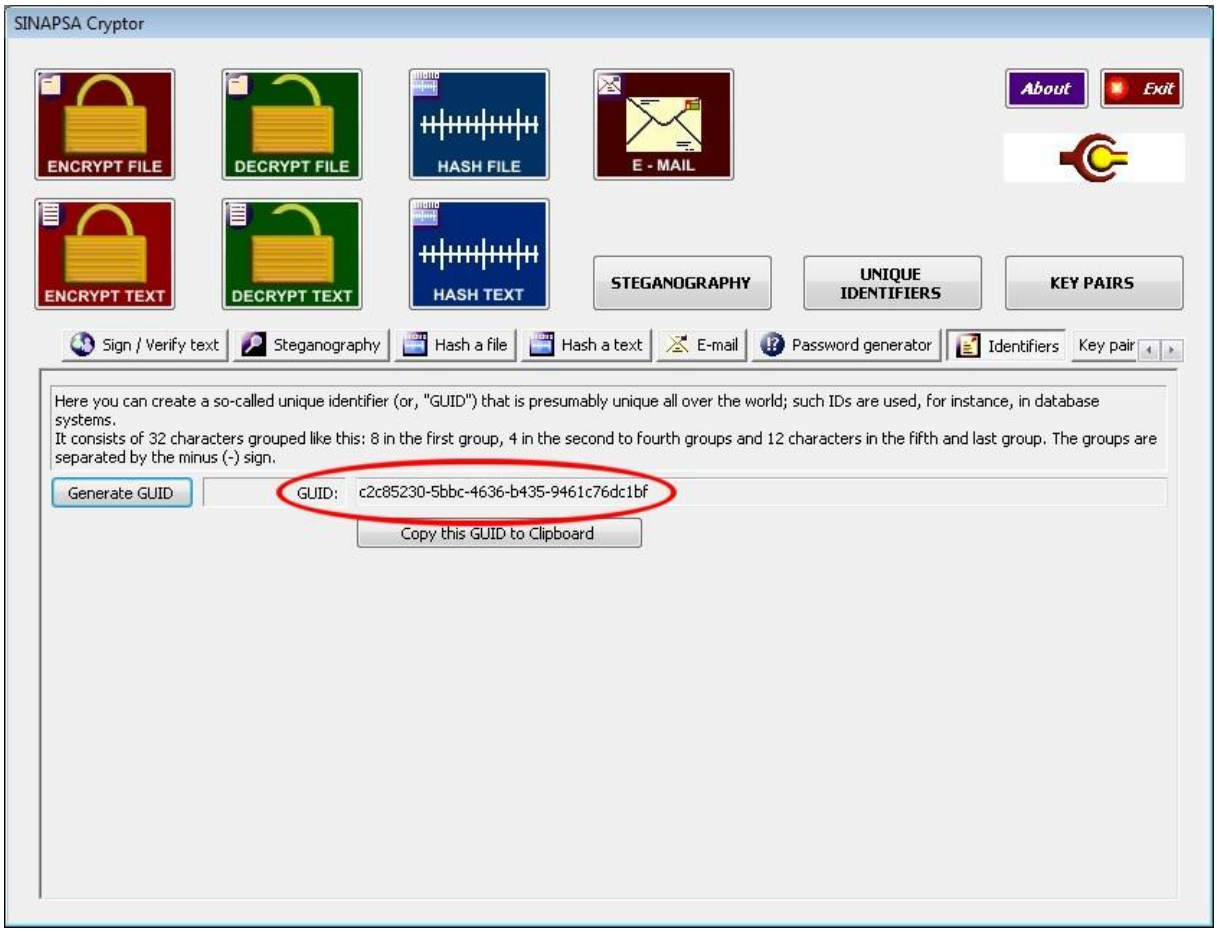
În imaginea precedentă se vede cum a fost creată şi afişată o parolă formată din 20 caractere.

O parolă creată aici poate fi copiată în Clipboard, prin apăsarea butonului "Copy this password to Clipboard".

13. PAGINA "Identifiers" ("Identificatori")

Pe această pagină puteţi genera identificatori unici ("GUID") formaţi din 32 caractere.

Acest model este foarte puternic, asigurând unicitatea obiectului asociat identificatorului prin complexitatea acestuia; de exemplu, în anul 2014 era folosit pe scară largă în identificarea înregistrărilor din baze de date relaţionale complexe.

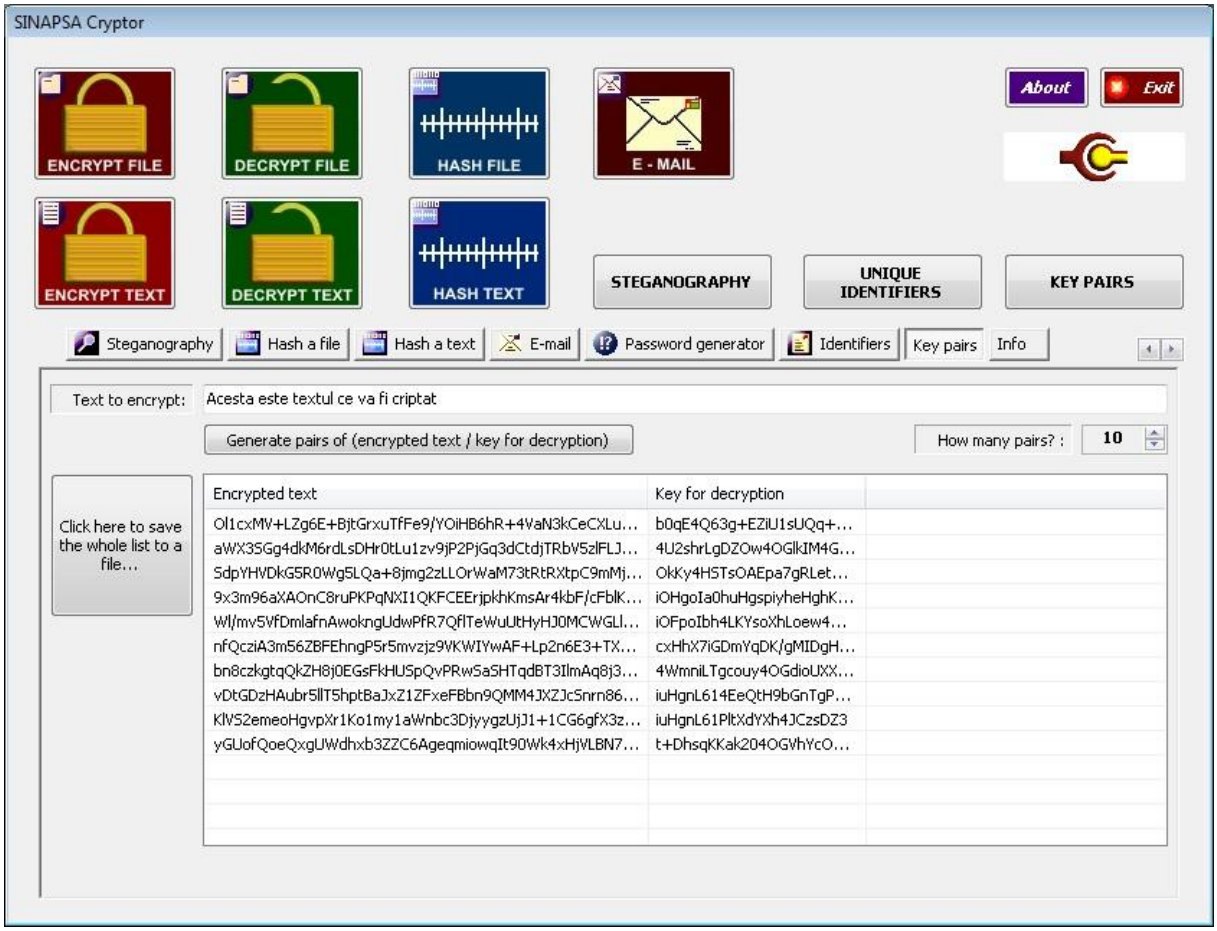


În imaginea precedentă se vede cum a fost creat şi afişat un identificator unic.

Un identificator creat aici poate fi copiat în Clipboard, prin apăsarea butonului "Copy this GUID to Clipboard".

14. PAGINA "Key pairs" ("Perechi de chei")

Pe această pagină puteţi genera serii de perechi text criptat + cheie de criptare pe care le puteţi folosi după cum doriţi după ce le salvaţi într-un fişier.



Toate intrările din lista afişată pot fi salvate într-un fişier prin apăsarea butonului "Click here to save the whole list to a file..." ("Click aici pentru a salva întreaga list ă într-un fişier...".

Fişierul respectiv va conţine perechile din listă în forma:

```
<
pair
encryptedtext="Ol1cxMV+LZg6E+BjtGrxuTfFe9/YOiHB6hR+4VaN3kCeCXLuTvUx5w=="
key="b0qE4Q63g+EZiU1sUQq+4D+A"
customer_name=""
customer_date=""
customer_softwarename=""
/>
```

Această formă este adaptată pentru cazul în care doriţi să trimiteţi mai multor clienţi texte şi parole criptate pe care numai Dumneavoastră să le puteţi decripta, pentru identificarea fiecăruia.