ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής

Εργασία Μαθήματος ***Ασφάλεια Πληροφοριακών Συστημάτων***

Άσκηση *<<αριθμός άσκησης>>*	***<<2η Ασκηση-Κρυπτογραφια και Κρυπταναλυση>>***
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Κουσουννής Κωνσταντίνος p14086
Ημερομηνία παράδοσης	12-11–2018 23:59:00

2η Ασκηση-Κρυπτογραφια και Κρυπταναλυση

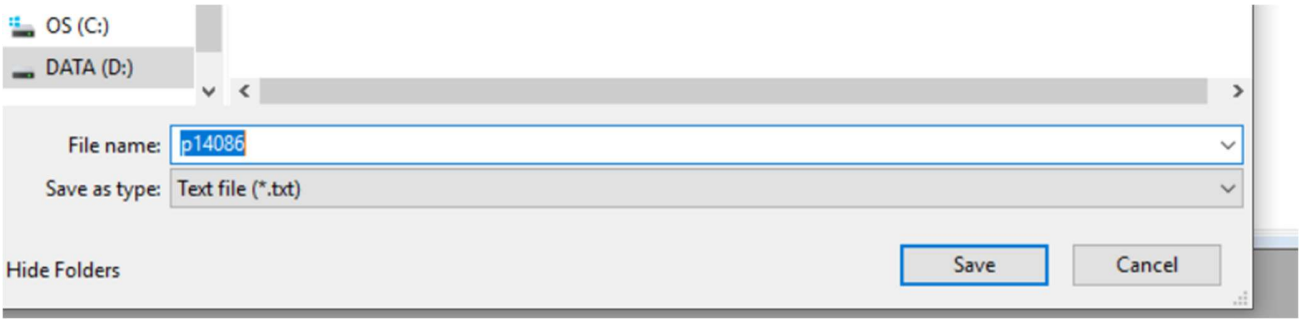
Για την υποβολή της 2ης εργασίας, ακολουθείστε τις γενικές οδηγίες και τις ομάδες που δημιουργήσατε στην 1η εργασία.

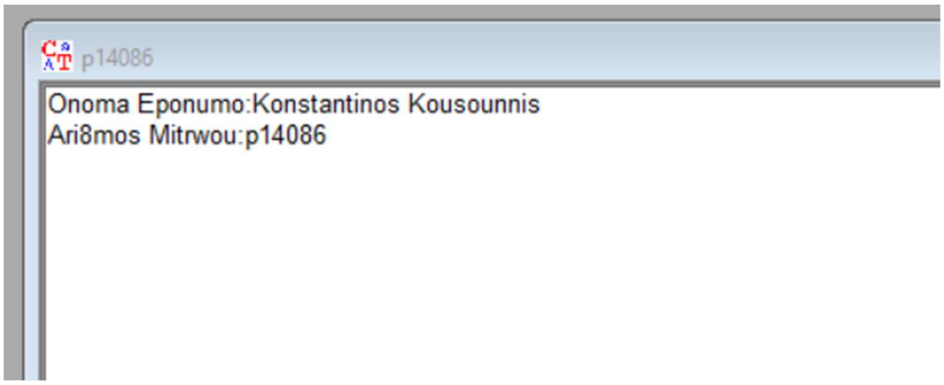
(α) Χρήση Cryptool

1. Δημιουργήστε ένα αρχείο κειμένου με όνομα τους αριθμούς μητρώου των μελών της ομάδας και γράψτε τα παρακάτω στοιχεία (κάθε μέλος της ομάδας).

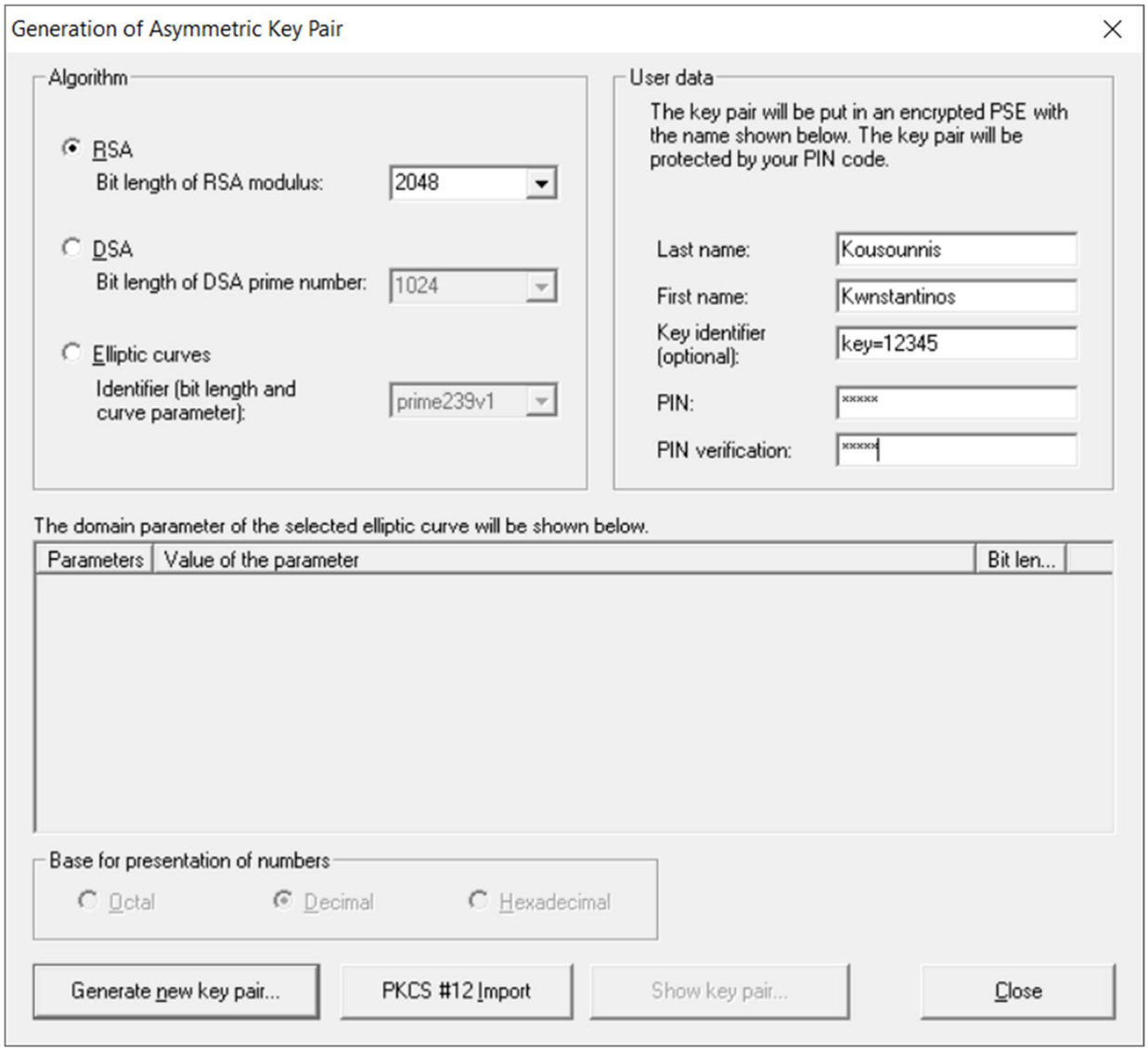
Όνομα Επώνυμο: ……

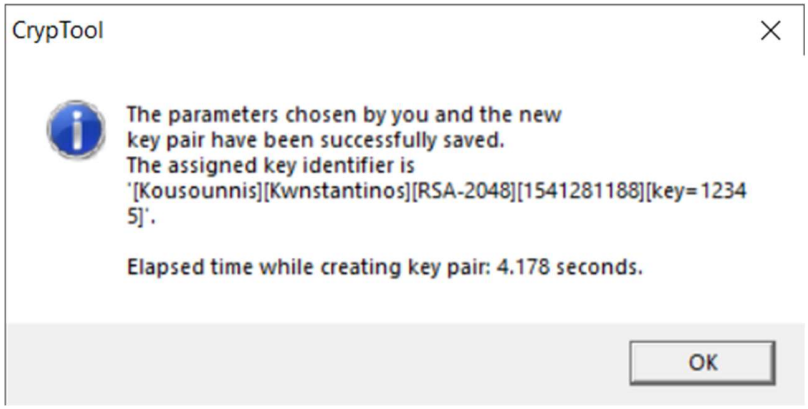
Αριθμός Μητρώου: ……

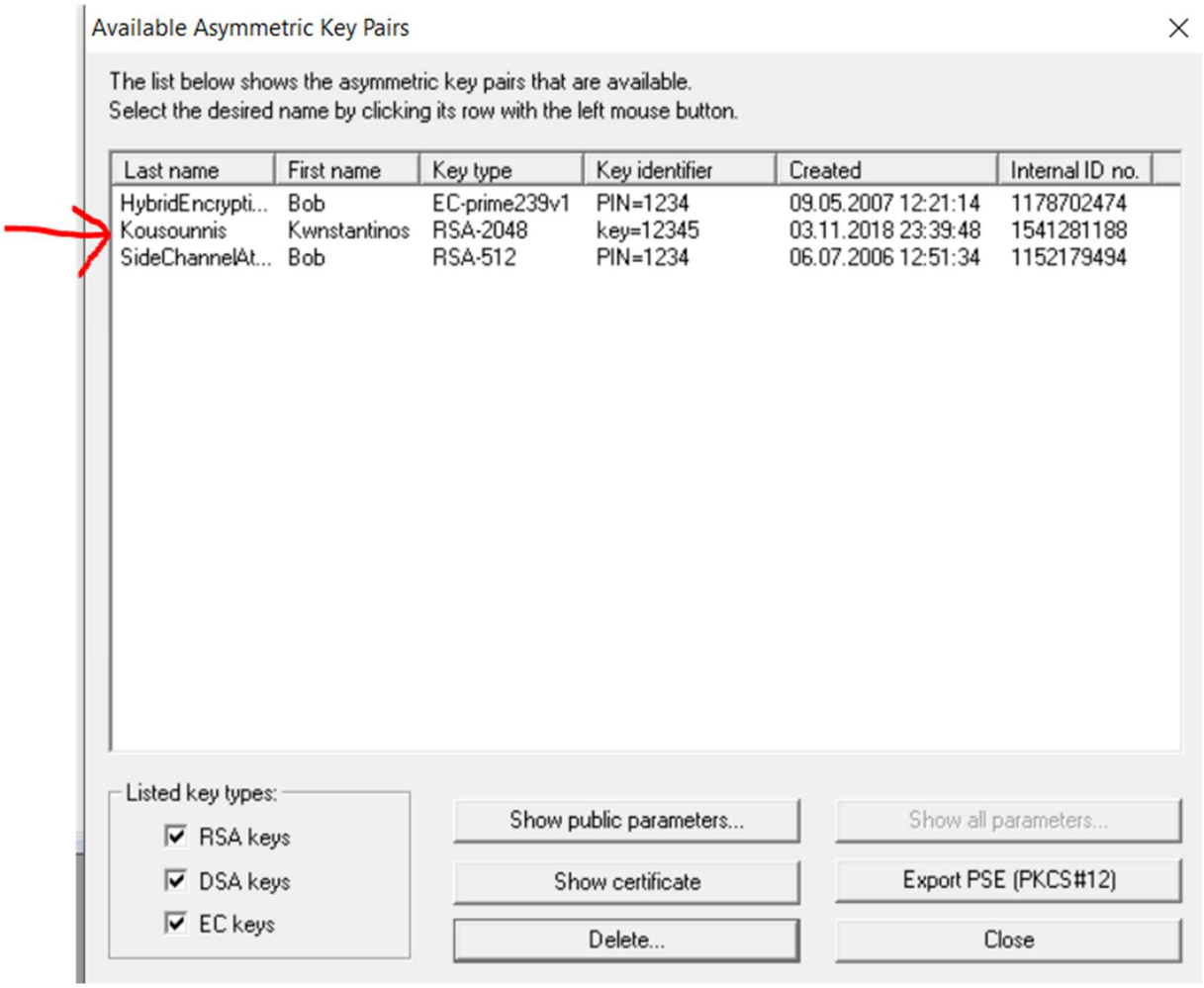


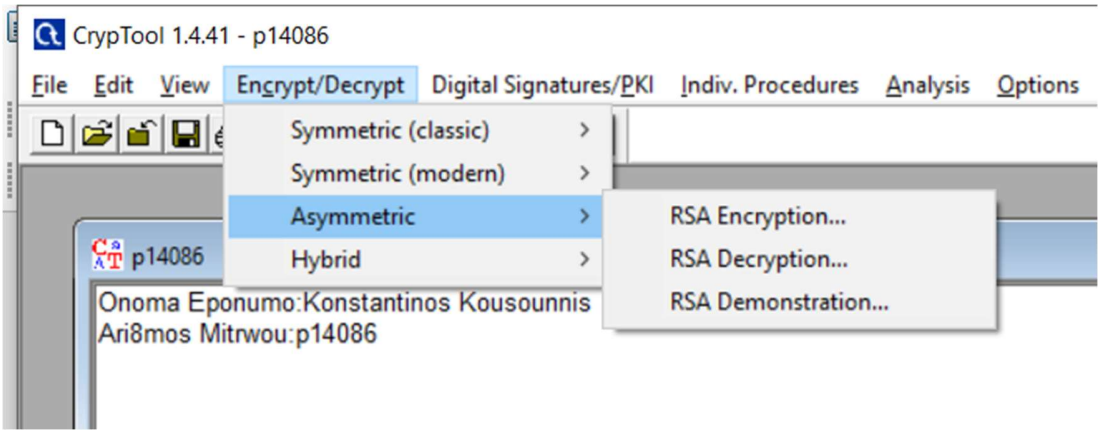


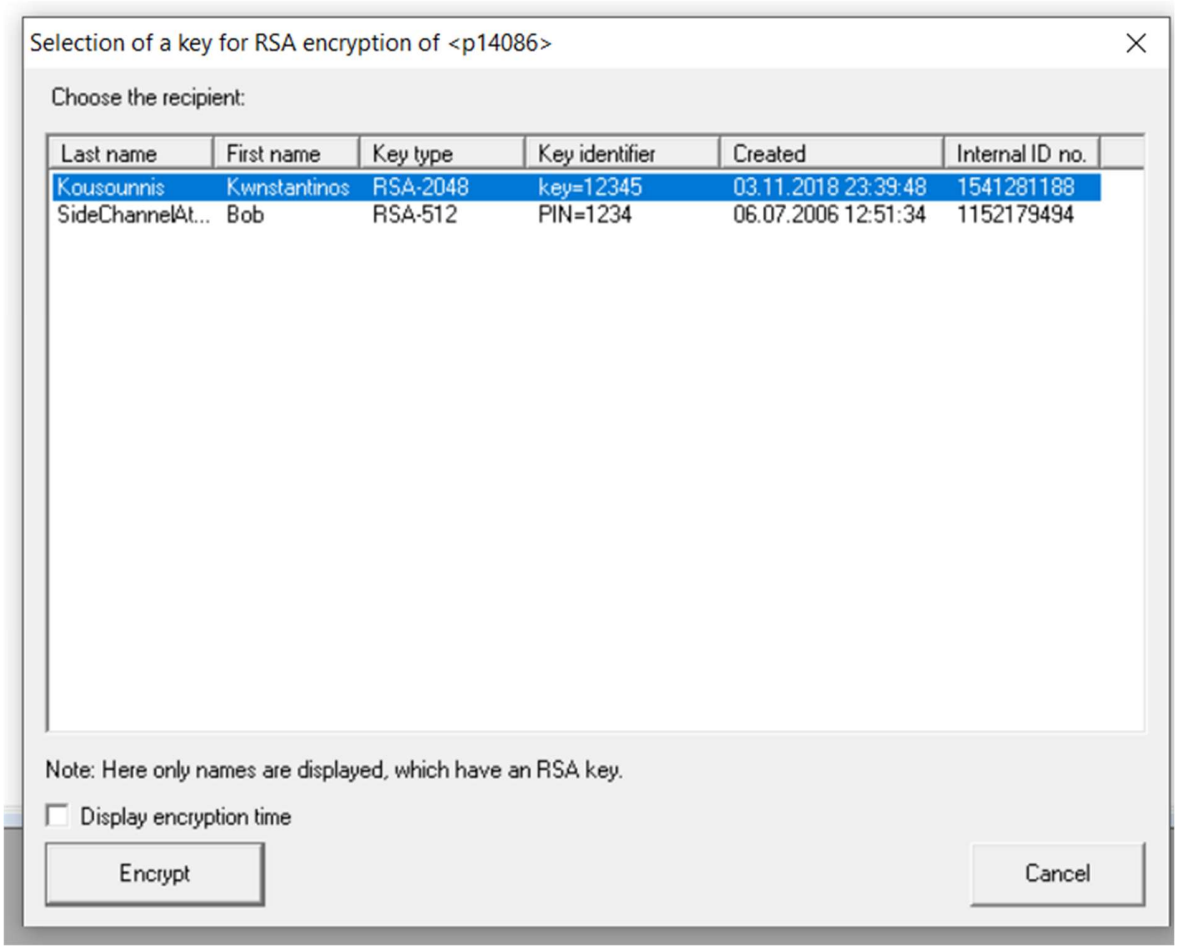
2. Δημιουργία ενός ασύμμετρου ζεύγους κλειδιών RSA. (μήκος κλειδιού 2048 bit). Προβολή του πιστοποιητικού που δημιουργήσατε.

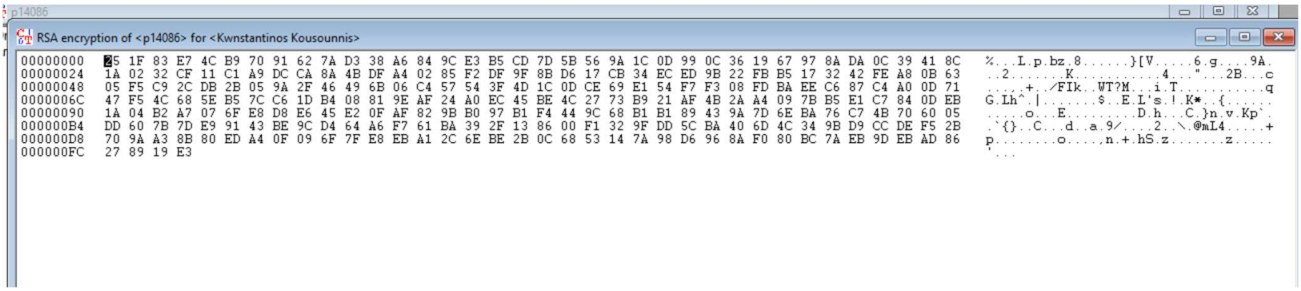

Generation of Asymmetric Key Pair
Algorithm
RSA
Bit length of RSA modulus:
2048
DSA
Bit length of DSA prime number:
1024
Elliptic curves
Identifier (bit length and curve parameter):
prime239v1
User data
The key pair will be put in an encrypted PSE with the name shown below. The key pair will be protected by your PIN code.
Last name:
Kousounnis
First name:
Kwnstantinos
Key identifier (optional):
key=12345
PIN:
*****
PIN verification:
*****
The domain parameter of the selected elliptic curve will be shown below.
Parameters
Value of the parameter
Bit len...
Base for presentation of numbers
Octal
Decimal
Hexadecimal
Generate new key pair...
PKCS #12 Import
Show key pair...
Close


CrypTool
The parameters chosen by you and the new key pair have been successfully saved.
The assigned key identifier is '[Kousounnis][Kwnstantinos][RSA-2048][1541281188][key=12345]'.
Elapsed time while creating key pair: 4.178 seconds.
OK


Available Asymmetric Key Pairs
The list below shows the asymmetric key pairs that are available.
Select the desired name by clicking its row with the left mouse button.
Last name
First name
Key type
Key identifier
Created
Internal ID no.
HybridEncrypti...
Bob
EC-prime239v1
PIN=1234
09.05.2007 12:21:14
1178702474
Kousounnis
Kwnstantinos
RSA-2048
key=12345
03.11.2018 23:39:48
1541281188
SideChannelAt...
Bob
RSA-512
PIN=1234
06.07.2006 12:51:34
1152179494
Listed key types:
RSA keys
DSA keys
EC keys
Show public parameters...
Show all parameters...
Show certificate
Export PSE (PKCS#12)
Delete...
Close


CrypTool 1.4.41 - p14086
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
Options
Symmetric (classic)
Symmetric (modern)
Asymmetric
Hybrid
RSA Encryption...
RSA Decryption...
RSA Demonstration...
p14086
Onoma Eponumo:Konstantinos Kousounnis
Ari8mos Mitrwou:p14086





3. Κρυπτογραφήστε με υβριδική κρυπτογραφία RSA-AES το μήνυμα που φτιάξατε στο βήμα 1, χρησιμοποιώντας το RSA Κλειδί που φτιάξατε στο βήμα 2.
Δείξτε τα εξής:

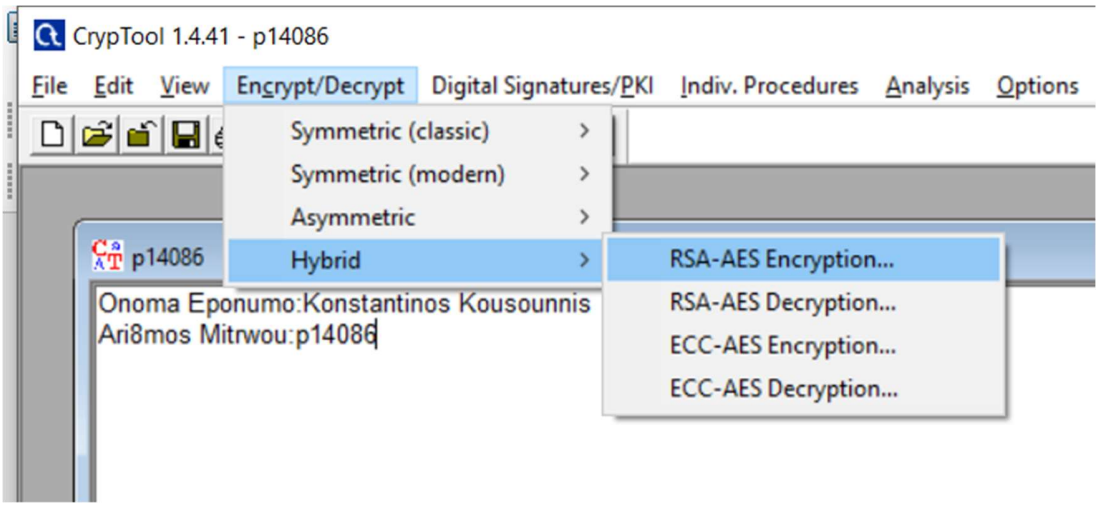
2.

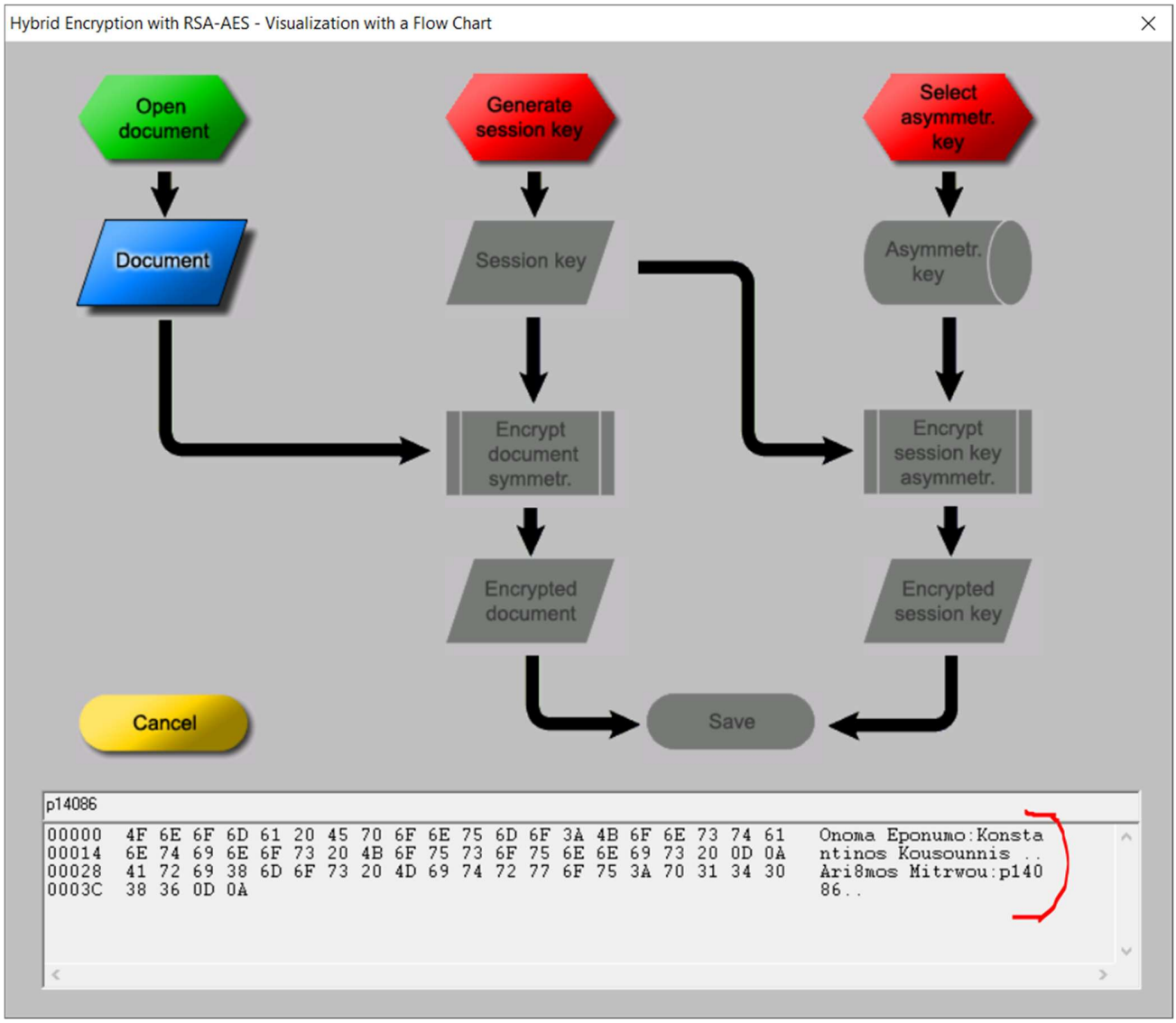
1To sessionkey που χρησιμοποιήσατε.

2To encrypted sessionkey

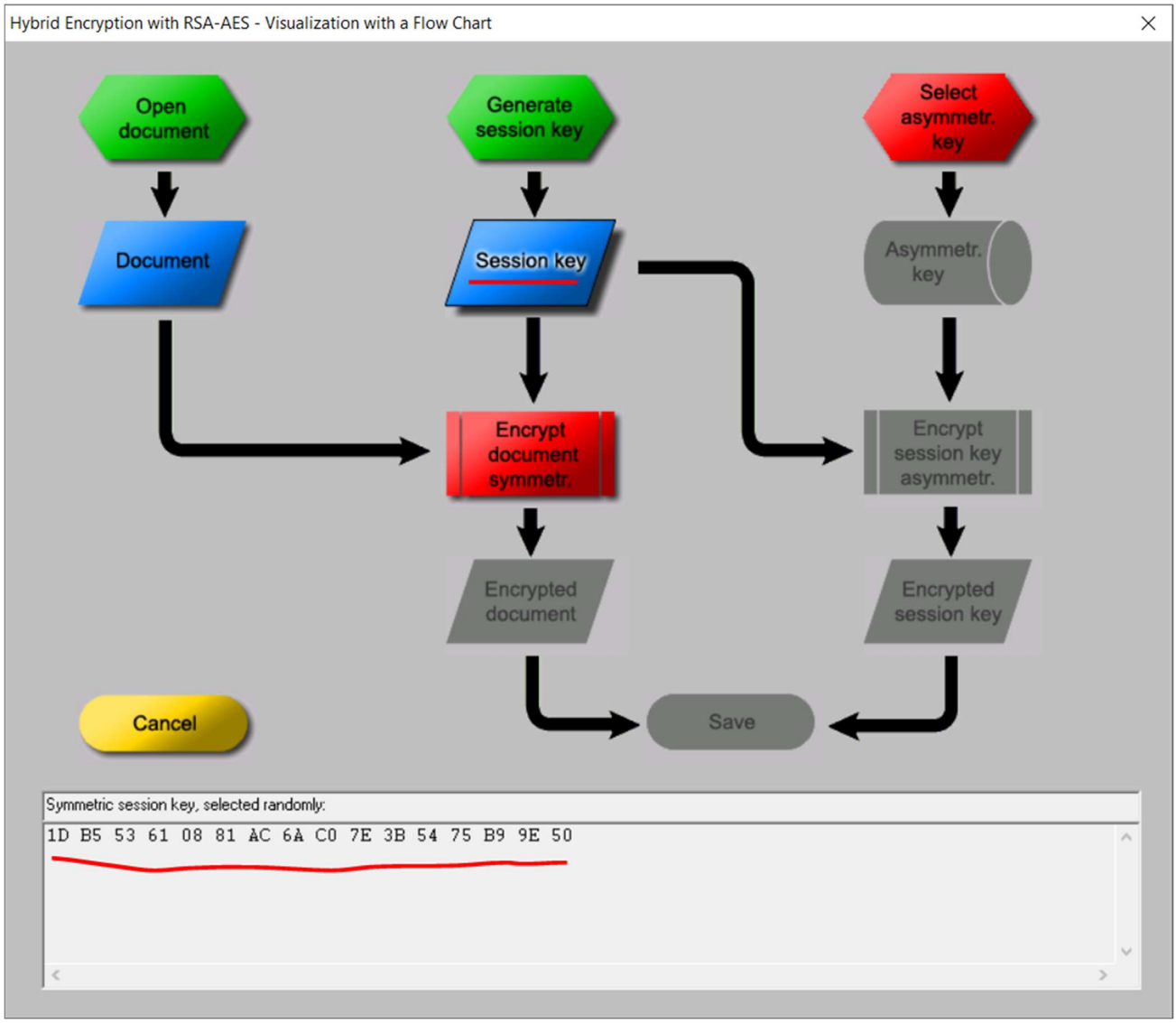
3To encrypted document

Με ποιο κλειδί και με ποιο αλγόριθμο το sessionkey;Με ποιο κλειδί και με ποιο αλγόριθμο κρυπτογραφείται το μήνυμα;

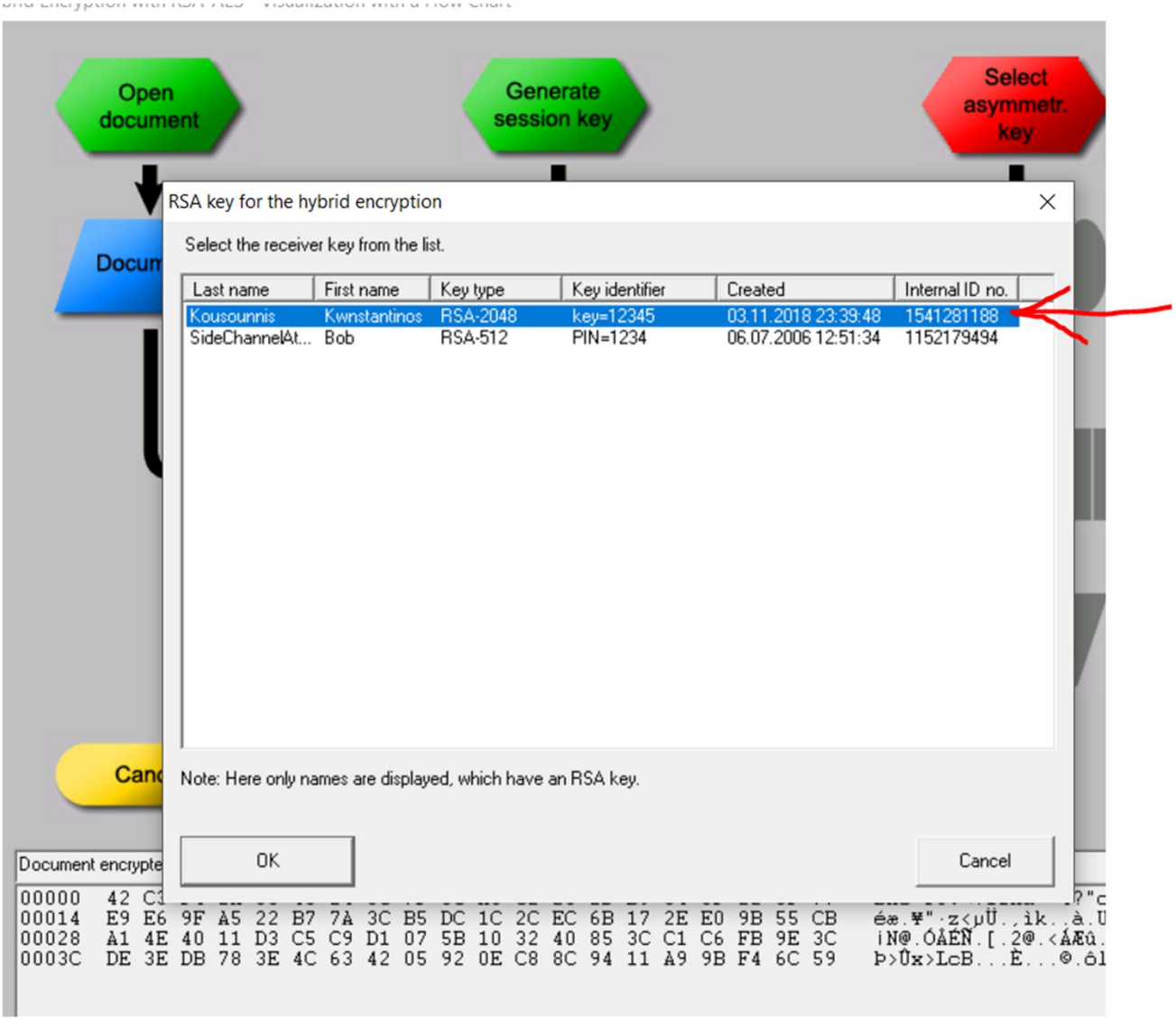


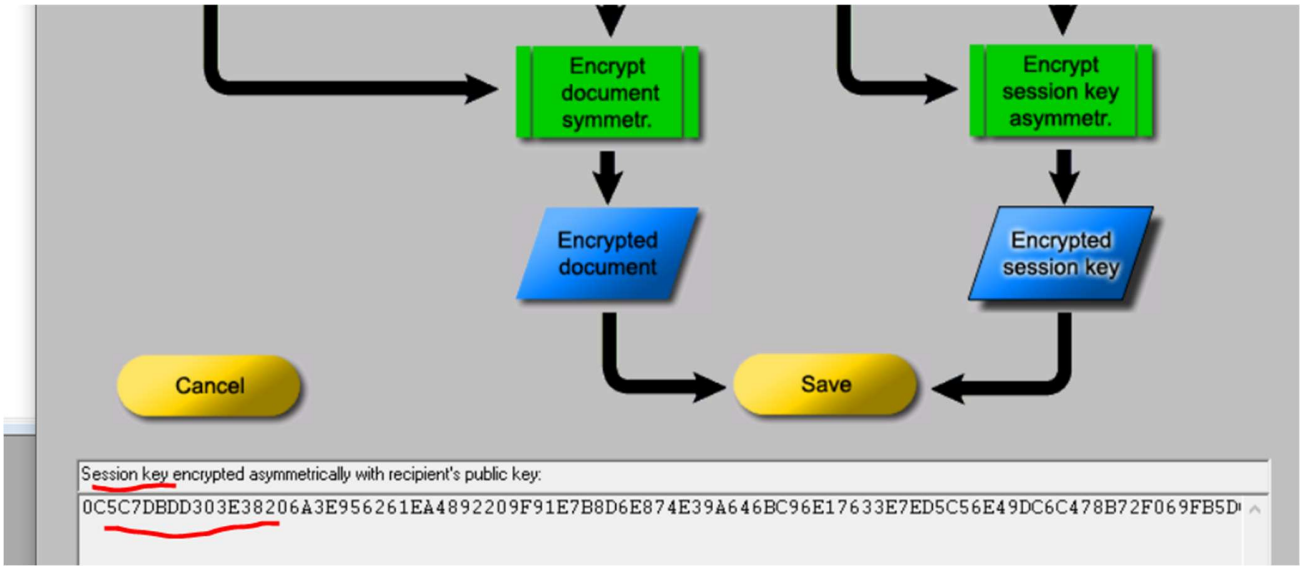

Hybrid Encryption with RSA-AES - Visualization with a Flow Chart
Open document
Document
Generate session key
Session key
Select asymmetr. key
Asymmetr. key
Encrypt document symmetr.
Encrypt session key asymmetr.
Encrypted document
Encrypted session key
Cancel
Save
p14086
00000 4F 6E 6F 6D 61 20 45 70 6F 6E 75 6D 6F 3A 4B 6F 6E 73 74 61 Onoma Eponumo:Konsta
00014 6E 74 69 6E 6F 73 20 4B 6F 75 73 6F 75 6E 6E 69 73 20 0D 0A ntinos Kousounnis ..
00028 41 72 69 38 6D 6F 73 20 4D 69 74 72 77 6F 75 3A 70 31 34 30 Ari8mos Mitrwou:p140
0003C 38 36 0D 0A 86..

1)Το sessionkey που χρησιμοποιήσατε.

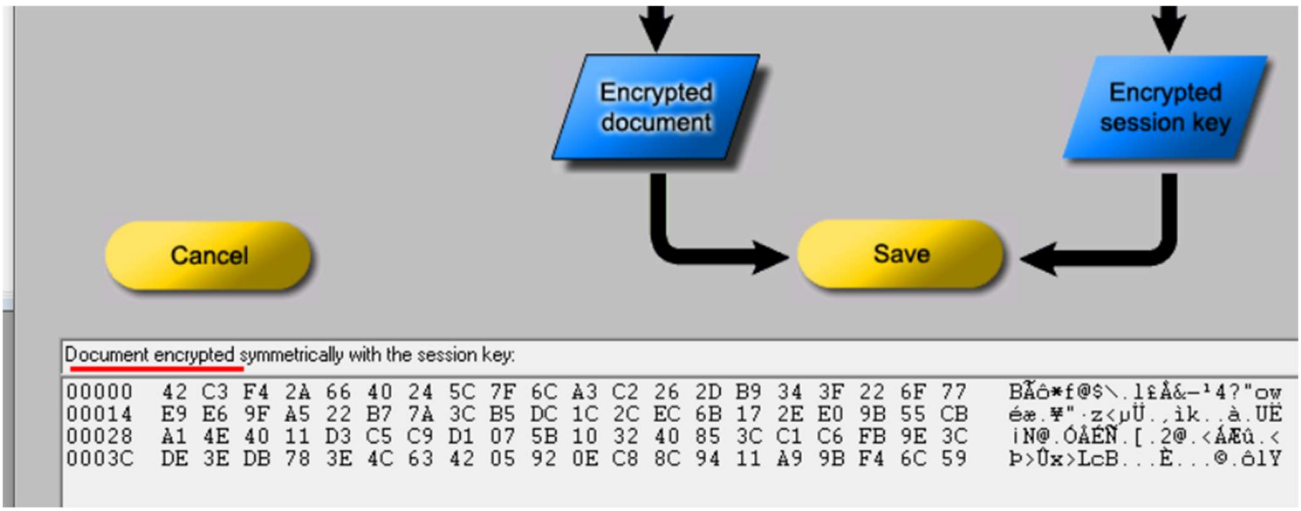


2)To encrypted sessionkey


Open document
Generate session key
Select asymmetr. key
RSA key for the hybrid encryption
Select the receiver key from the list.
Last name
First name
Key type
Key identifier
Created
Internal ID no.
Kousounnis
Kwnstantinos
RSA-2048
key=12345
03.11.2018 23:39:48
1541281188
SideChannelAt...
Bob
RSA-512
PIN=1234
06.07.2006 12:51:34
1152179494
Note: Here only names are displayed, which have an RSA key.
OK
Cancel



3)To encrypted document



4)Φτιαξτε δυο txt αρχεία με το κείμενο που σας δίδεται παρακάτω.Το πραγμάτικο αρχείο

(original.txt)θα έχει το παρακάτω κείμενο:

Dear miss Mallory,

on behalf of XYZ company,I declare non acceptance of the proposed contract no. 12345.

Regards,

Kostantinos Kousounnis

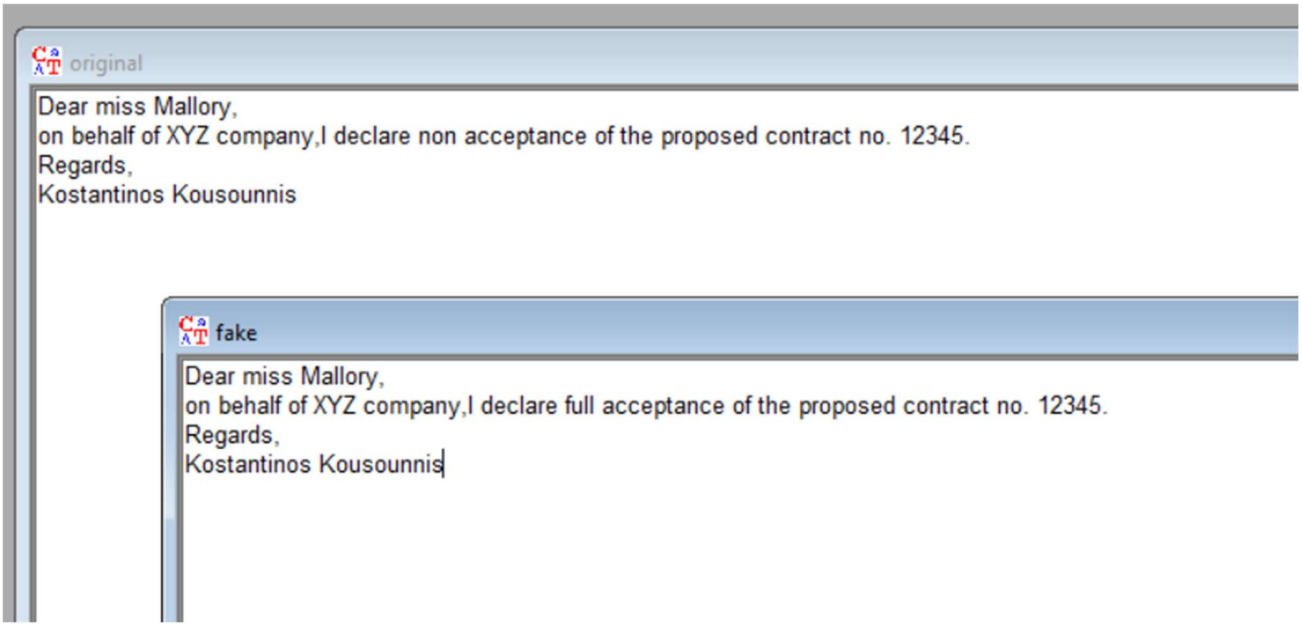
Το τροποποιημένο αρχείο (fake.txt)θα έχει το παρακάτω κείμενο:

Dear miss Mallory,

on behalf of XYZ company,I declare full acceptance of the proposed contract no. 12345.

Regards,

Kostantinos Kousounnis



5)Με βάση τα κείμενα που δημιουργήσατε στο παραπάνω βήμα,προσπάθηστε να βρείτε ένα επικίνδυνο μηνυμα το οποίο μοιάζει στο fake.txt και έχει την ίδια τιμή hash με το original.txt για τις παρακάτω περιπτώσεις:

2) |. Για τον αλγόριθμο MD2 και τα πρώτα 16 bit της τιμής hash.

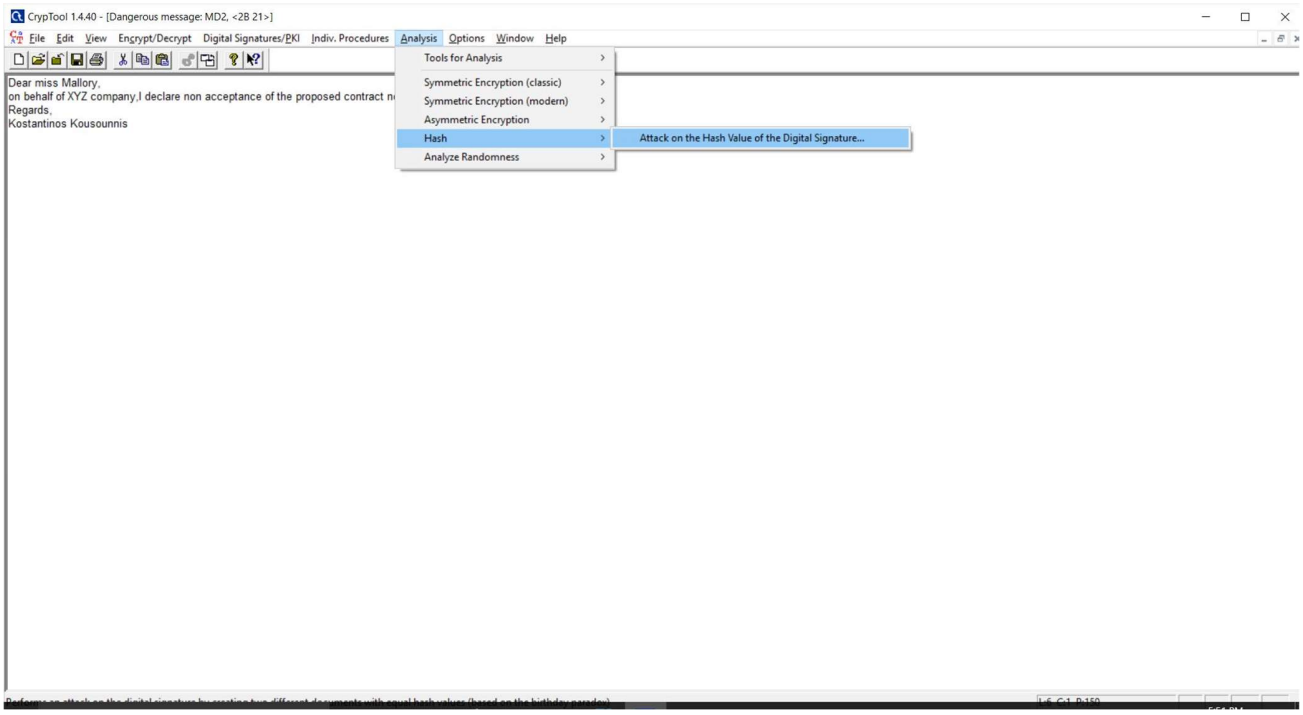
||.Για τον αλγόριθμο MD2 και τα πρώτα 50 bit της τιμής hash.

|||.Για τον αλγόριθμο SHA1 και τα πρώτα 80 bit της τιμής hash.

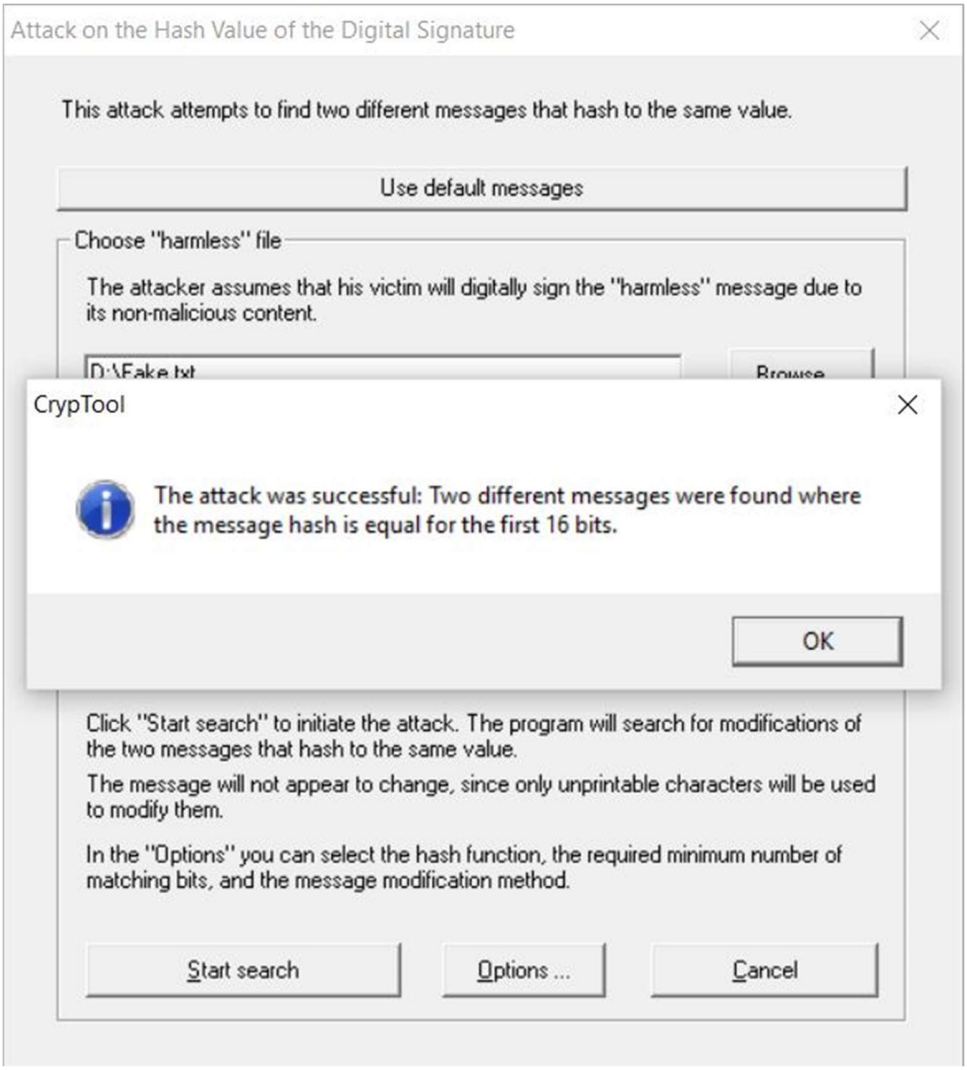
||||. Για τον αλγόριθμο SHA1 και όλα (160)τα bit της τιμής hash.

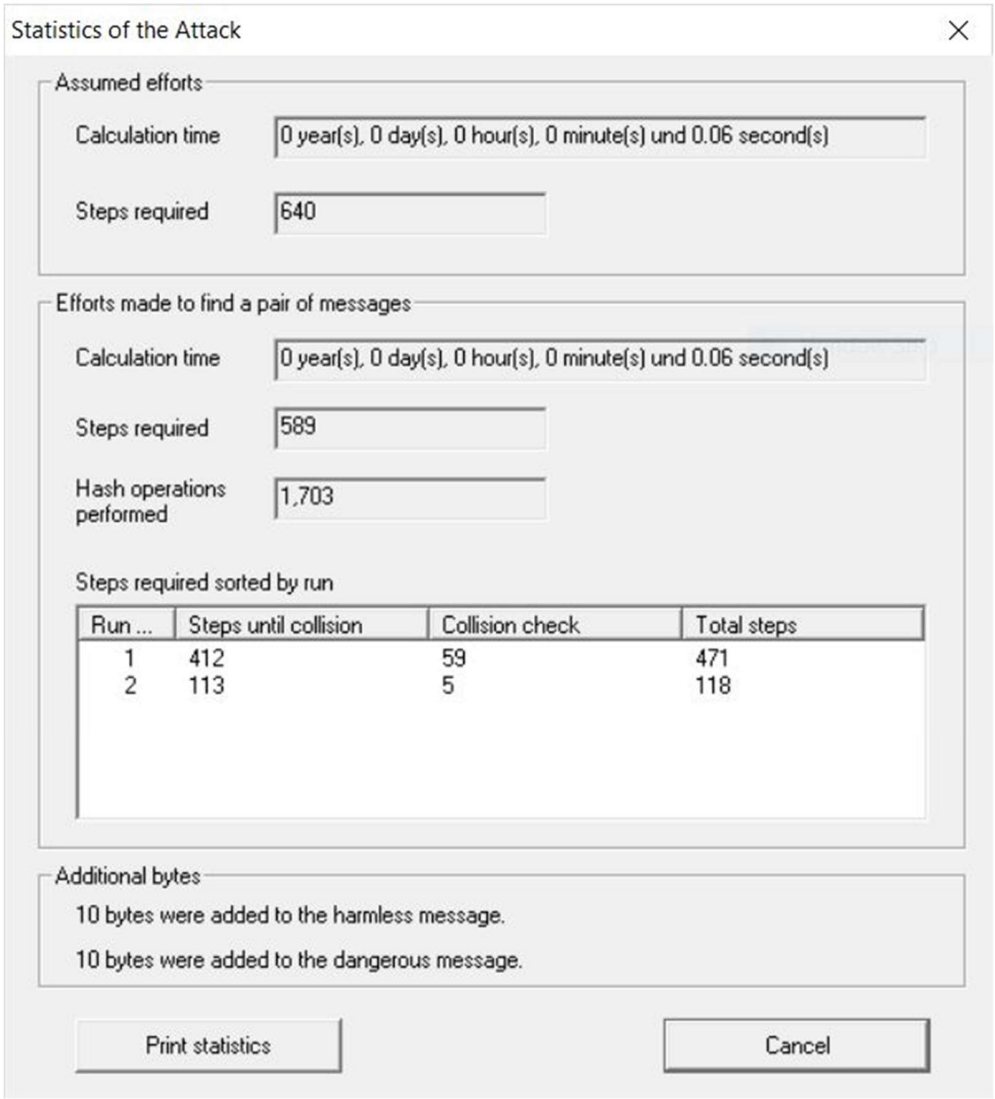
Για κάθε μια περίπτωση αναφέρετε,πόσες λειτουργίες hash(hashoperations)πραγματοποιήθηκαν και πόσος χρόνος χρειάστηκε/θα χριαζόταν στον υπολογιστη σας

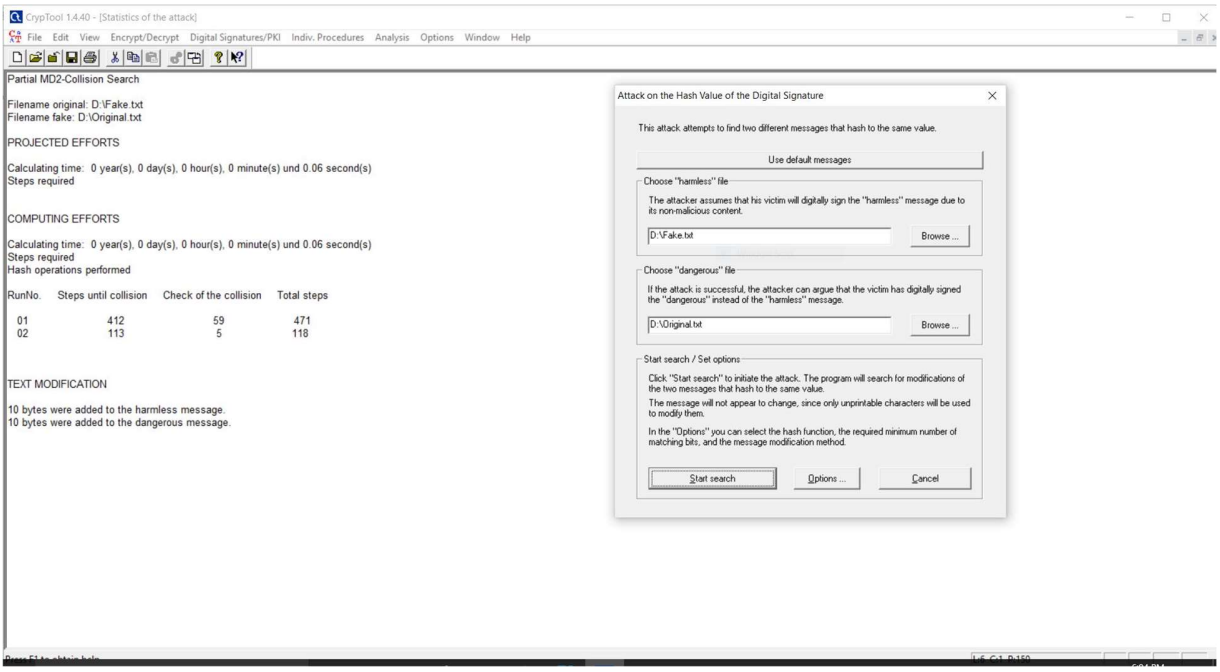
MD2 KAI 16 bit



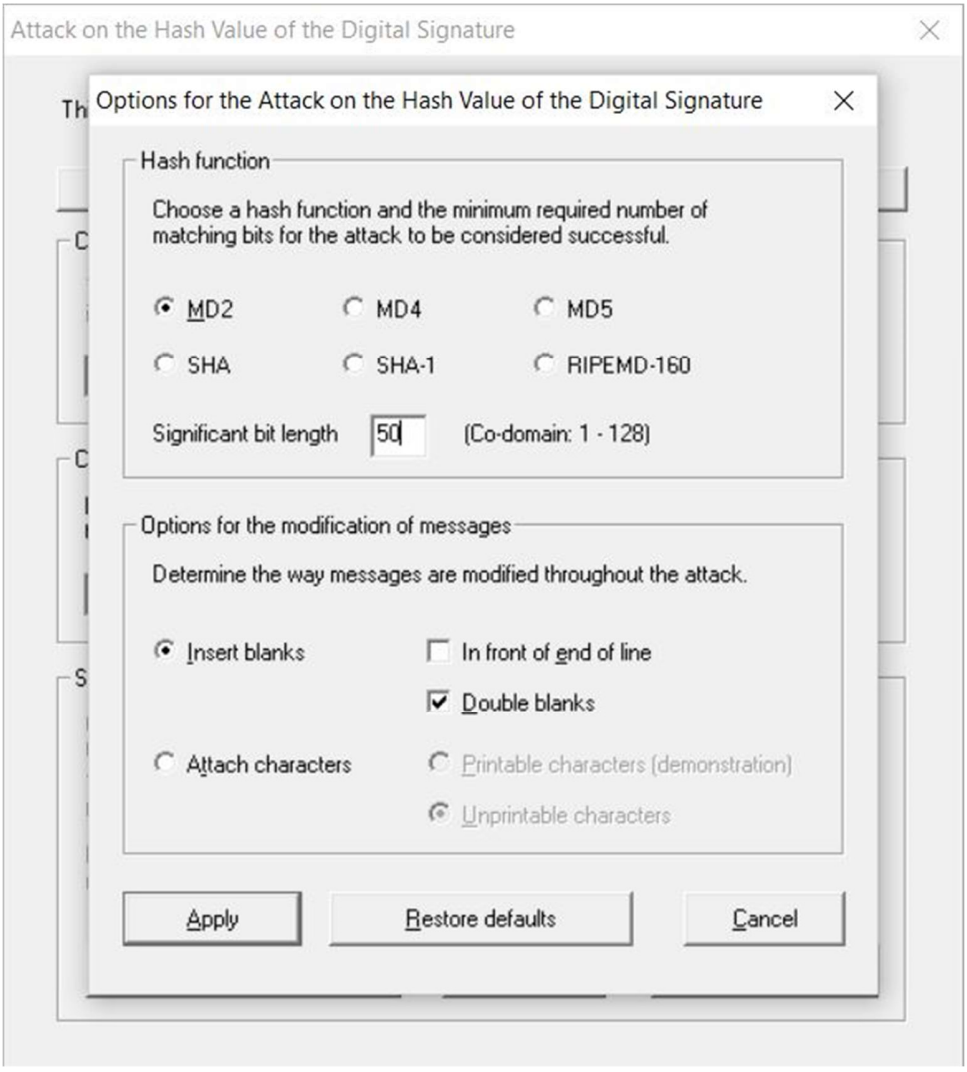

Attack on the Hash Value of the Digital Signature
This attack attempts to find two different messages that hash to the same value.
Use default messages
Choose "harmless" file
The attacker assumes that his victim will digitally sign the "harmless" message due to its non-malicious content.
D:\Fake.txt
Browse ...
Choose "dangerous" file
If the attack is successful, the attacker can argue that the victim has digitally signed the "dangerous" instead of the "harmless" message.
D:\Original.txt
Browse ...
Start search / Set options
Click "Start search" to initiate the attack. The program will search for modifications of the two messages that hash to the same value.
The message will not appear to change, since only unprintable characters will be used to modify them.
In the "Options" you can select the hash function, the required minimum number of matching bits, and the message modification method.
Start search
Options ...
Cancel

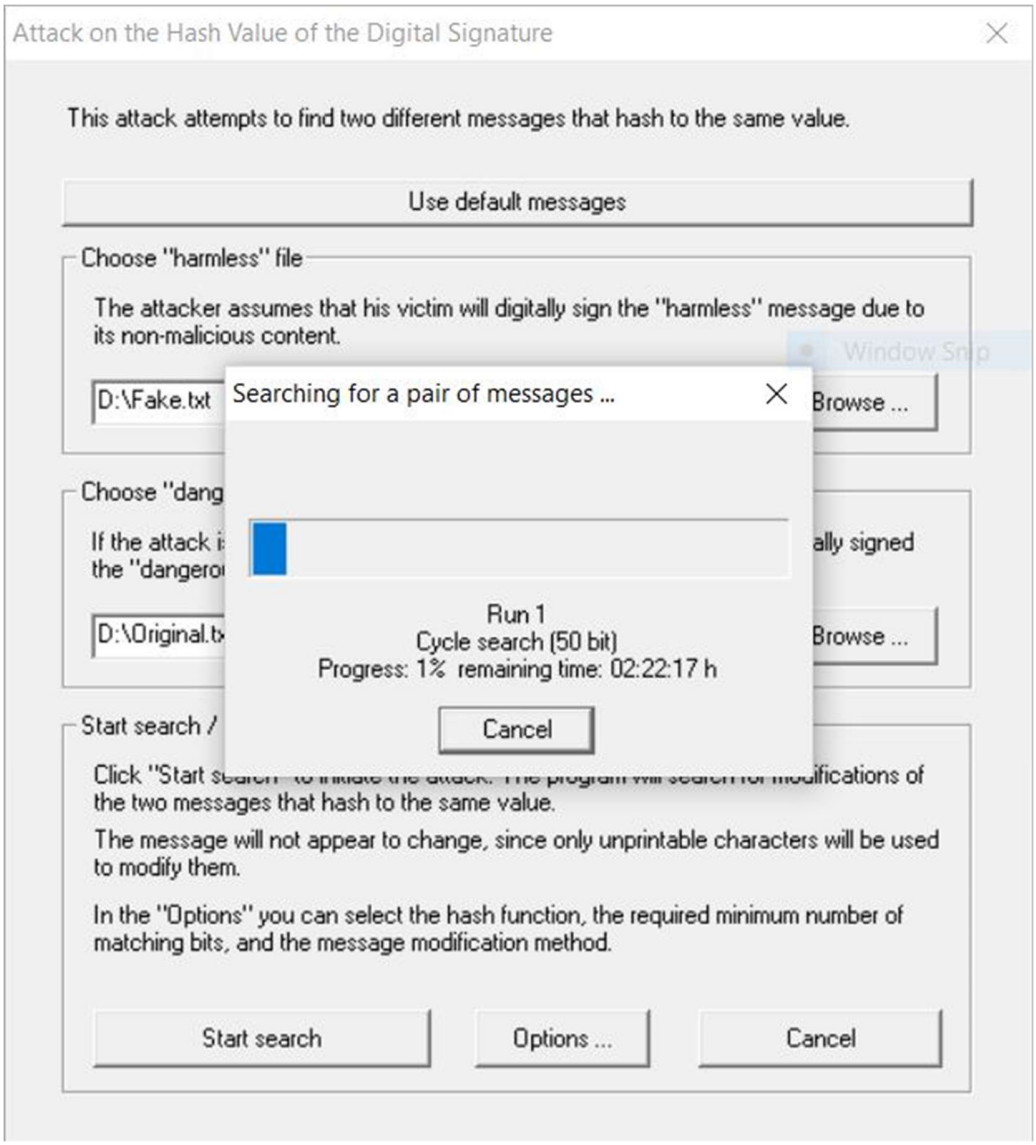

Attack on the Hash Value of the Digital Signature
This attack attempts to find two different messages that hash to the same value.
Use default messages
Choose "harmless" file
The attacker assumes that his victim will digitally sign the "harmless" message due to its non-malicious content.
D:\Fake.txt
Browse...
CrypTool
The attack was successful: Two different messages were found where the message hash is equal for the first 16 bits.
OK
Click "Start search" to initiate the attack. The program will search for modifications of the two messages that hash to the same value.
The message will not appear to change, since only unprintable characters will be used to modify them.
In the "Options" you can select the hash function, the required minimum number of matching bits, and the message modification method.
Start search
Options ...
Cancel


Statistics of the Attack
Assumed efforts
Calculation time
0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.06 second(s)
Steps required
640
Efforts made to find a pair of messages
Calculation time
0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.06 second(s)
Steps required
589
Hash operations performed
1,703
Steps required sorted by run
Run ...
Steps until collision
Collision check
Total steps
1
412
59
471
2
113
5
118
Additional bytes
10 bytes were added to the harmless message.
10 bytes were added to the dangerous message.
Print statistics
Cancel

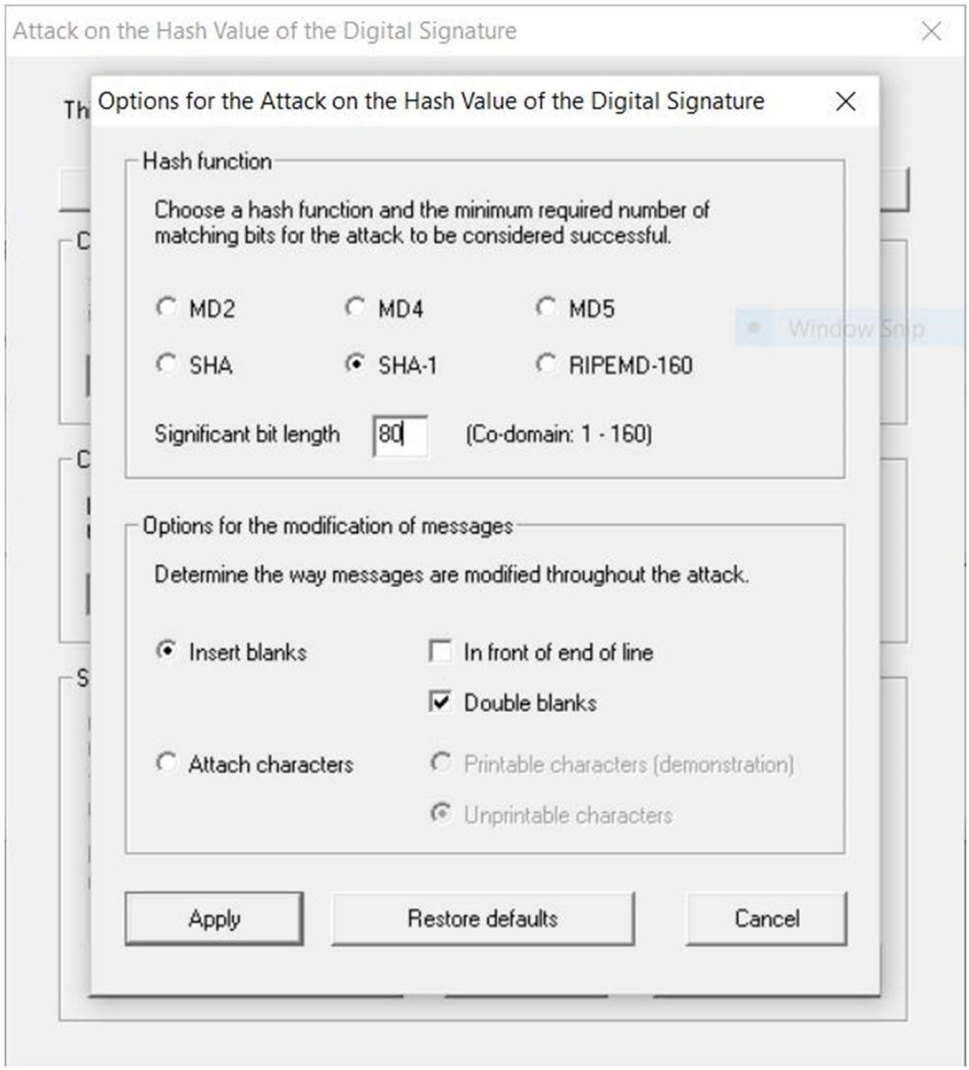

CrypTool 1.4.40 - [Statistics of the attack]
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Partial MD2-Collision Search
Filename original: D:\Fake.txt
Filename fake: D:\Original.txt
PROJECTED EFFORTS
Calculating time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.06 second(s)
Steps required
COMPUTING EFFORTS
Calculating time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.06 second(s)
Steps required
Hash operations performed
RunNo. Steps until collision Check of the collision Total steps
01 412 59 471
02 113 5 118
TEXT MODIFICATION
10 bytes were added to the harmless message.
10 bytes were added to the dangerous message.
Attack on the Hash Value of the Digital Signature
This attack attempts to find two different messages that hash to the same value.
Use default messages
Choose "harmless" file
The attacker assumes that his victim will digitally sign the "harmless" message due to its non-malicious content.
D:\Fake.txt
Browse ...
Choose "dangerous" file
If the attack is successful, the attacker can argue that the victim has digitally signed the "dangerous" instead of the "harmless" message.
D:\Original.txt
Browse ...
Start search / Set options
Click "Start search" to initiate the attack. The program will search for modifications of the two messages that hash to the same value.
The message will not appear to change, since only unprintable characters will be used to modify them.
In the "Options" you can select the hash function, the required minimum number of matching bits, and the message modification method.
Start search
Options ...
Cancel

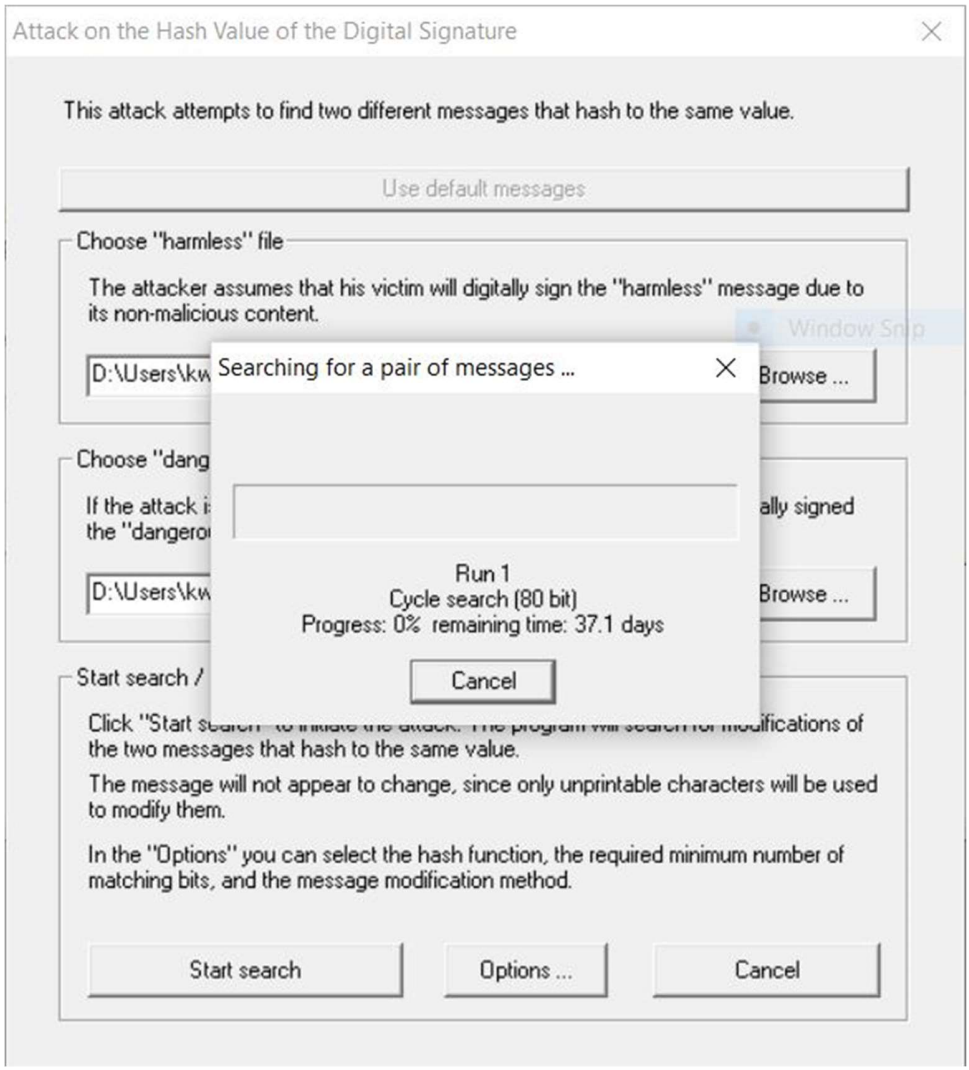
MD2 και 50 bit



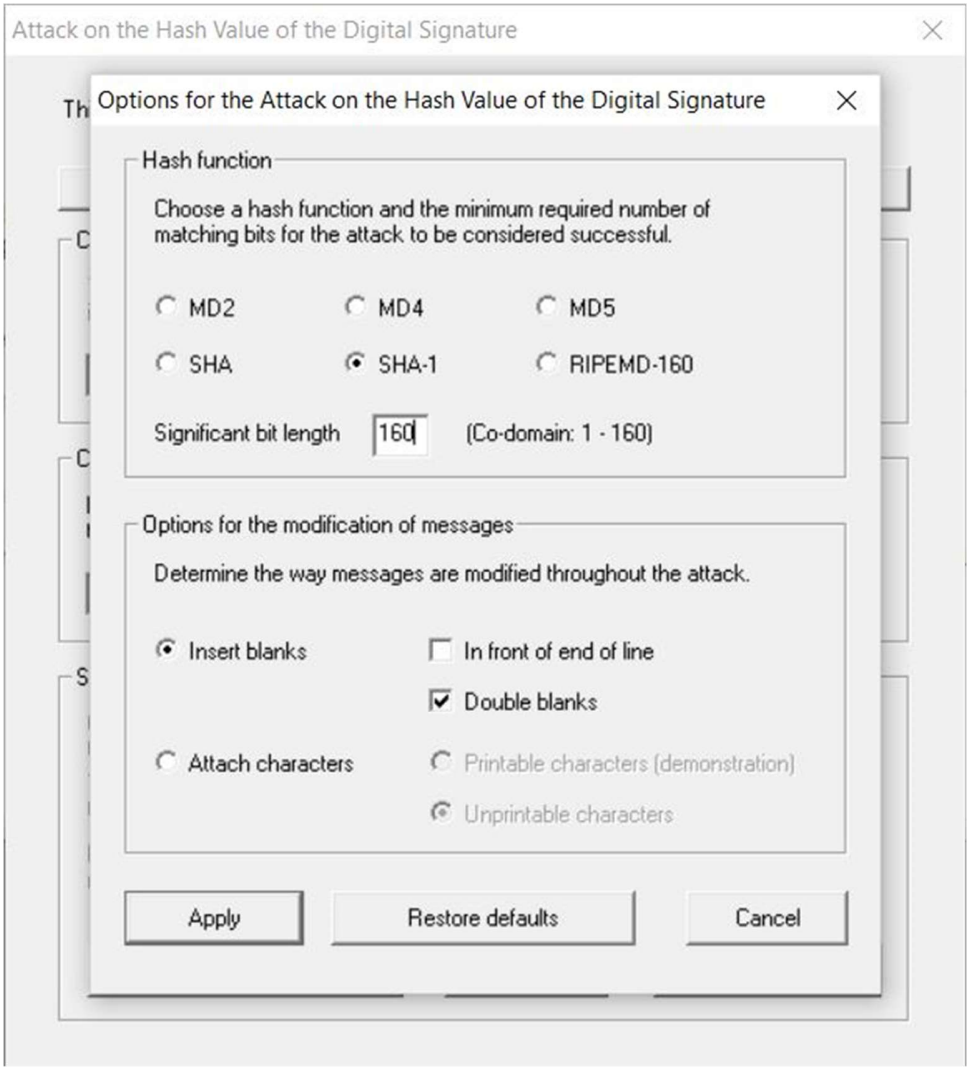

Attack on the Hash Value of the Digital Signature
This attack attempts to find two different messages that hash to the same value.
Use default messages
Choose "harmless" file
The attacker assumes that his victim will digitally sign the "harmless" message due to its non-malicious content.
D:\Fake.txt
Browse ...
Searching for a pair of messages ...
Run 1
Cycle search (50 bit)
Progress: 1% remaining time: 02:22:17 h
Cancel
Choose "dang
If the attack i
the "dangero
ally signed
D:\Original.t
Browse ...
Start search /
Click "Start search" to initiate the attack. The program will search for modifications of the two messages that hash to the same value.
The message will not appear to change, since only unprintable characters will be used to modify them.
In the "Options" you can select the hash function, the required minimum number of matching bits, and the message modification method.
Start search
Options ...
Cancel

SHA1 80 bit

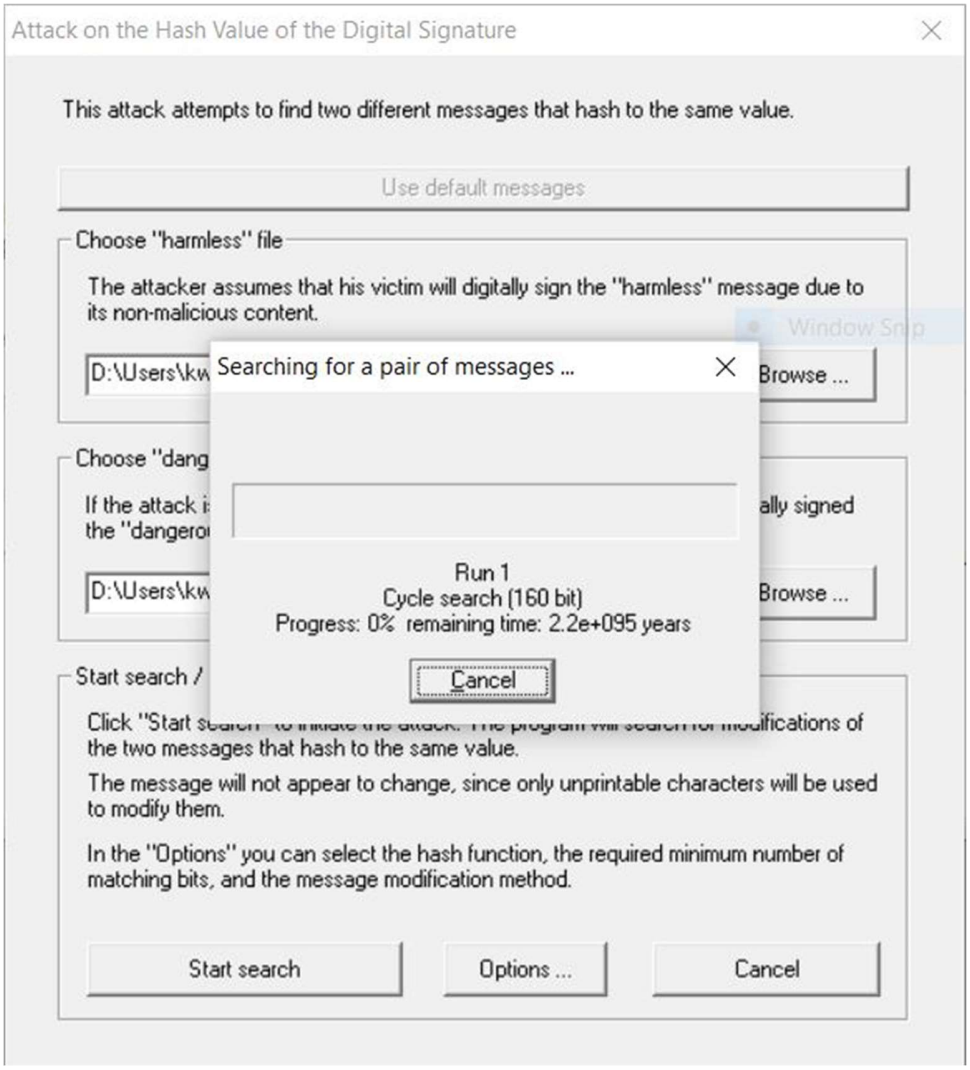

Attack on the Hash Value of the Digital Signature
Options for the Attack on the Hash Value of the Digital Signature
Hash function
Choose a hash function and the minimum required number of matching bits for the attack to be considered successful.
MD2
MD4
MD5
SHA
SHA-1
RIPEMD-160
Significant bit length
80
(Co-domain: 1 - 160)
Options for the modification of messages
Determine the way messages are modified throughout the attack.
Insert blanks
In front of end of line
Double blanks
Attach characters
Printable characters (demonstration)
Unprintable characters
Apply
Restore defaults
Cancel


Attack on the Hash Value of the Digital Signature
This attack attempts to find two different messages that hash to the same value.
Use default messages
Choose "harmless" file
The attacker assumes that his victim will digitally sign the "harmless" message due to its non-malicious content.
D:\Users\kw
Browse ...
Searching for a pair of messages ...
Run 1
Cycle search (80 bit)
Progress: 0% remaining time: 37.1 days
Cancel
Choose "dang
If the attack i
the "dangero
ally signed
D:\Users\kw
Browse ...
Start search /
Click "Start search" to initiate the attack. The program will search for modifications of the two messages that hash to the same value.
The message will not appear to change, since only unprintable characters will be used to modify them.
In the "Options" you can select the hash function, the required minimum number of matching bits, and the message modification method.
Start search
Options ...
Cancel

SHA 160

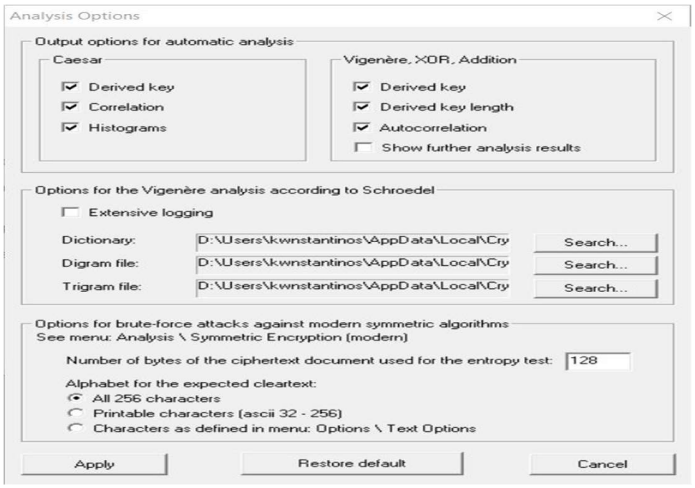

Attack on the Hash Value of the Digital Signature
Options for the Attack on the Hash Value of the Digital Signature
Hash function
Choose a hash function and the minimum required number of matching bits for the attack to be considered successful.
MD2
MD4
MD5
SHA
SHA-1
RIPEMD-160
Significant bit length
160
(Co-domain: 1 - 160)
Options for the modification of messages
Determine the way messages are modified throughout the attack.
Insert blanks
In front of end of line
Double blanks
Attach characters
Printable characters (demonstration)
Unprintable characters
Apply
Restore defaults
Cancel

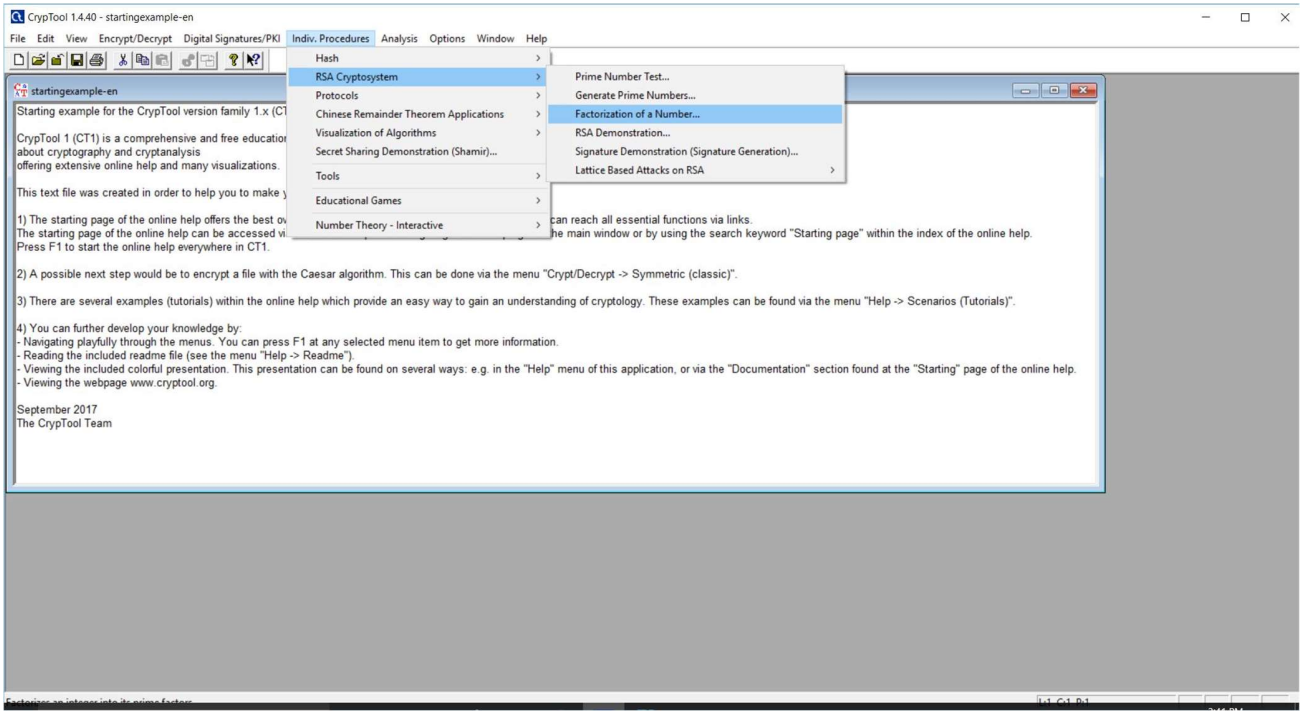
6.)Πως μπορεί να επηρεάσει την ασφάλεια μιας ψηφιακής υπογραφής μια επίθεση στην συνάρτηση hash(οπως στο βήμα 5)



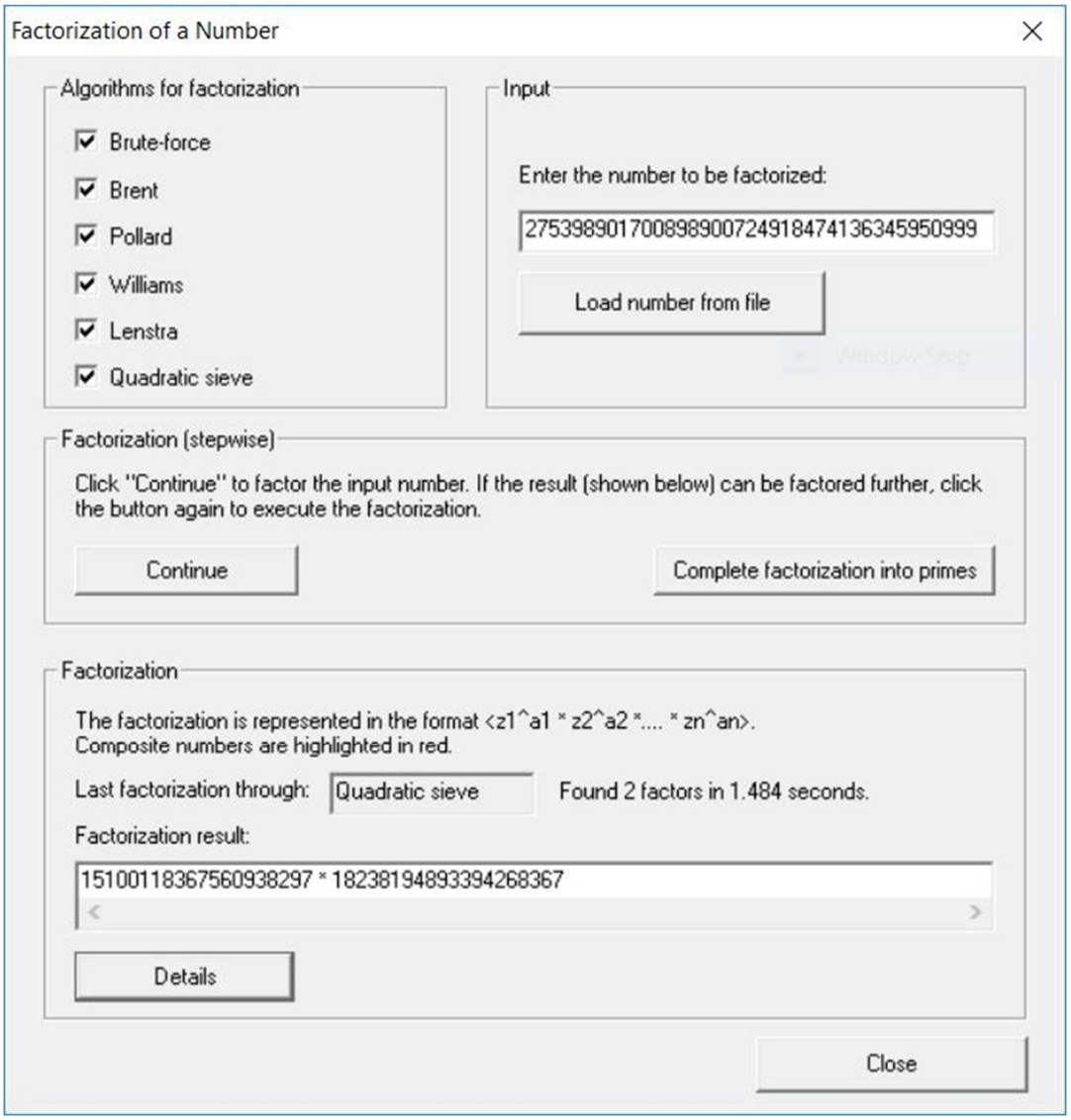
7)Πραγματοποιήστε επίθεση παραγοντοποιήσης για τα παρακάτω RSAmoduli.

n = 275398901700898900724918474136345950999 (128 bit modulo)

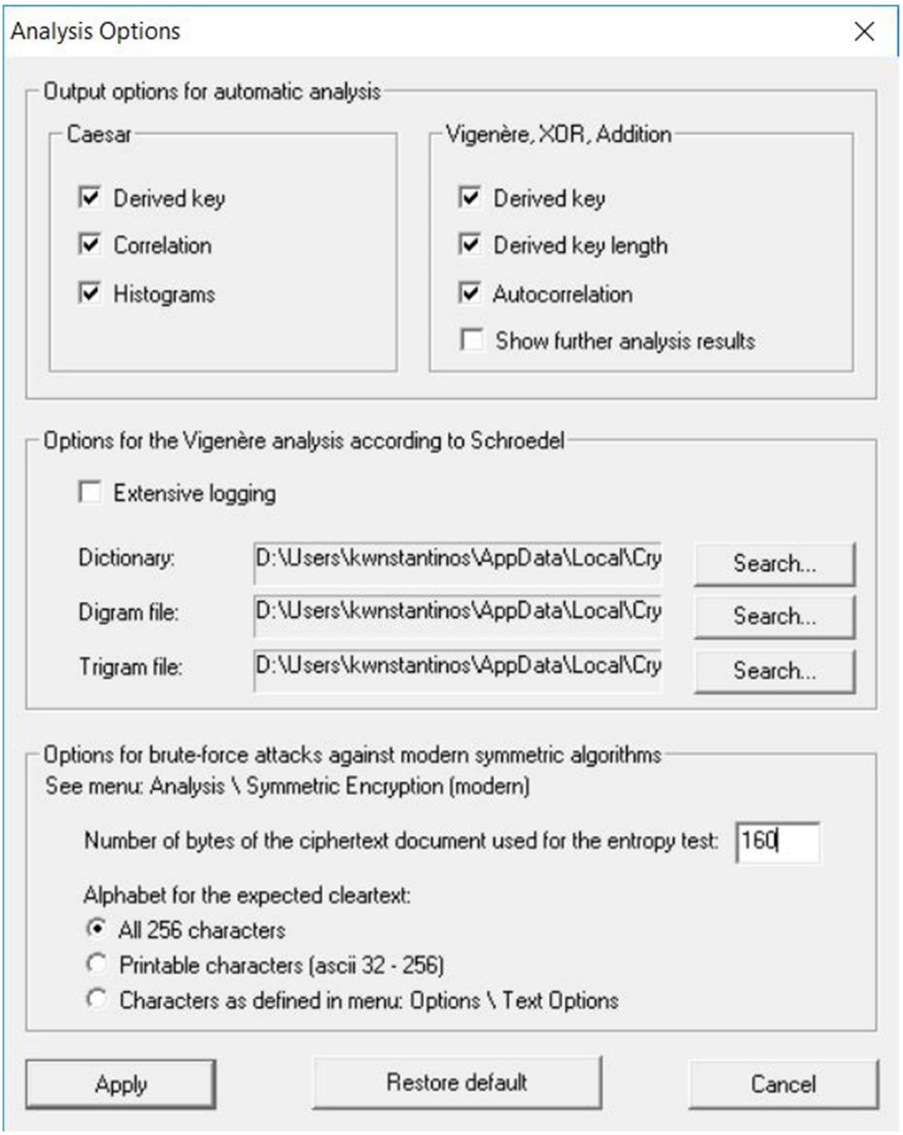




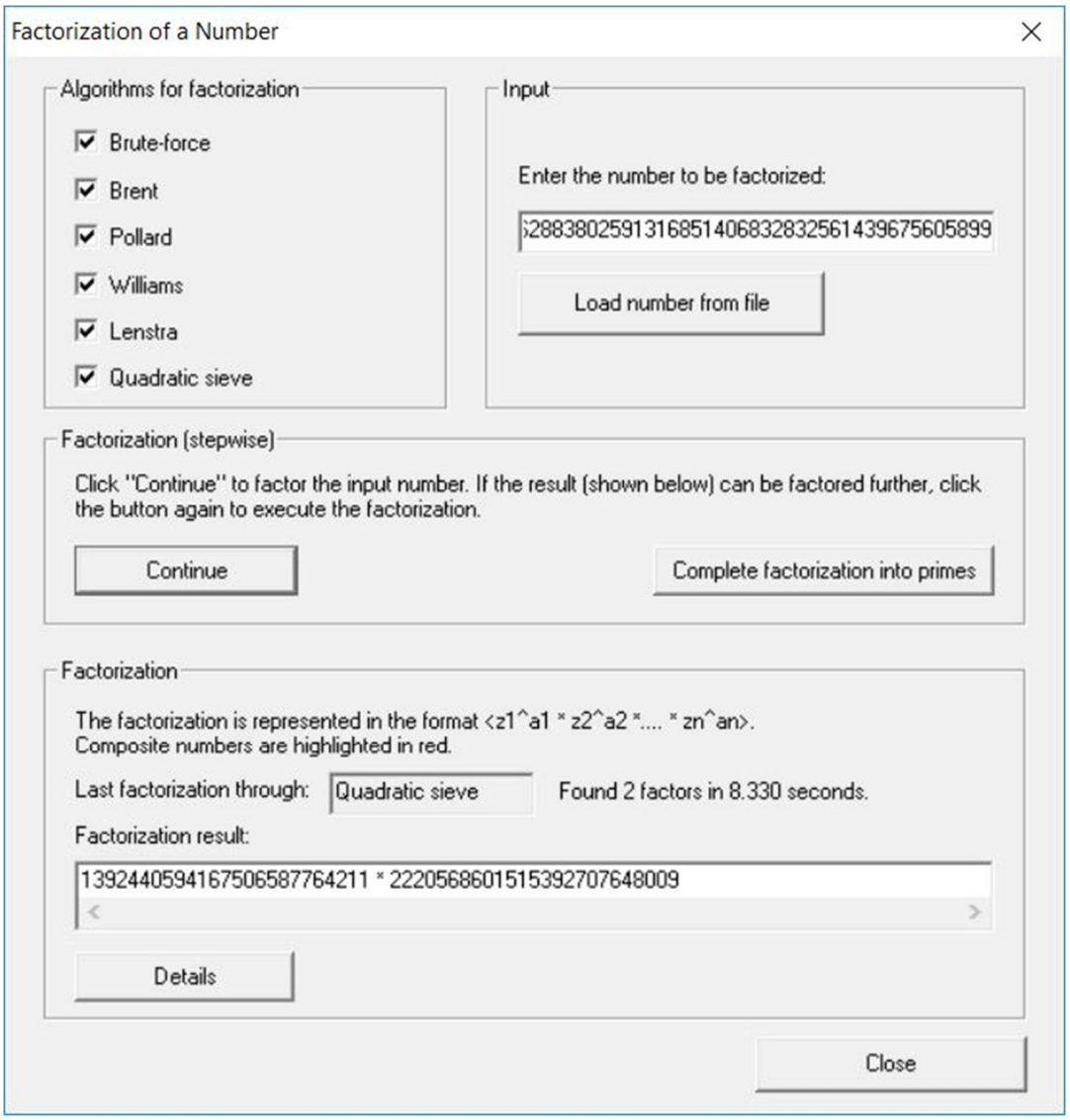
n =



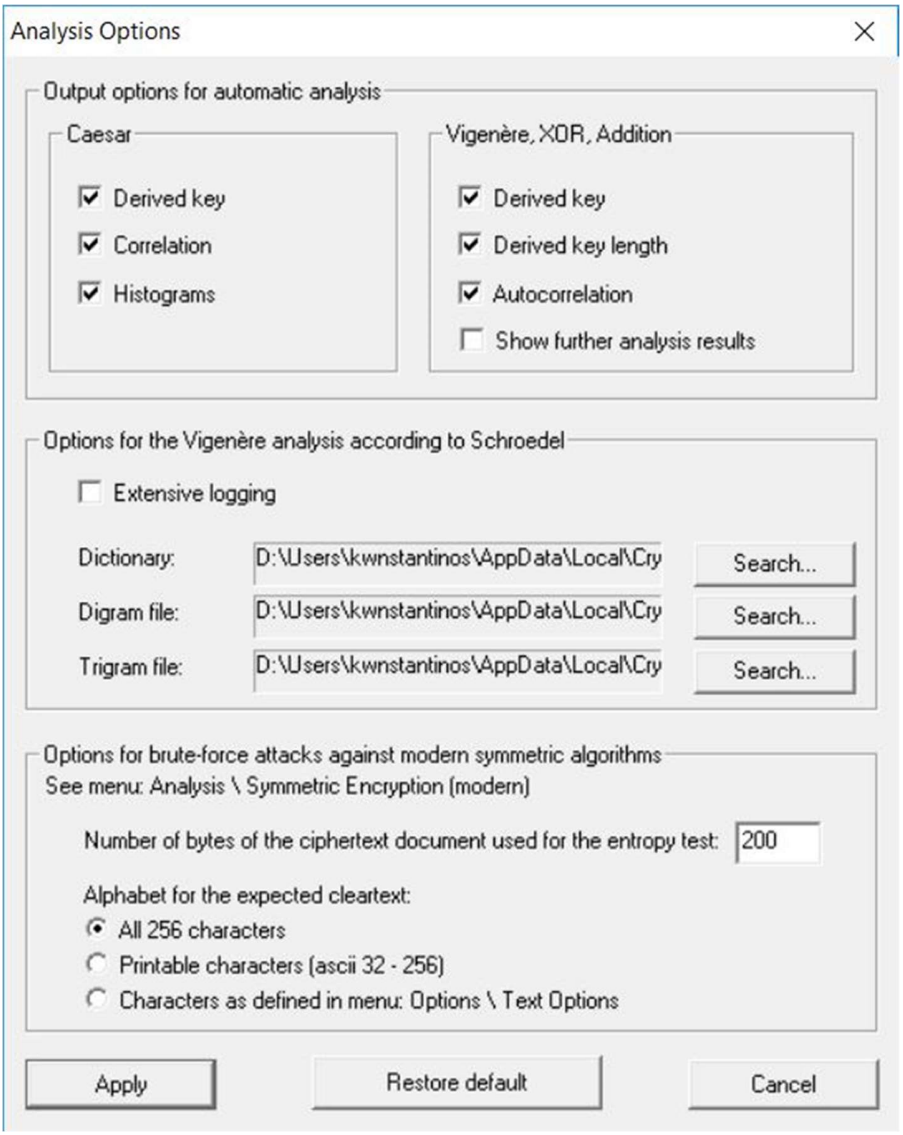
309200986288380259131685140683283256143967560589 9 (160 bit)

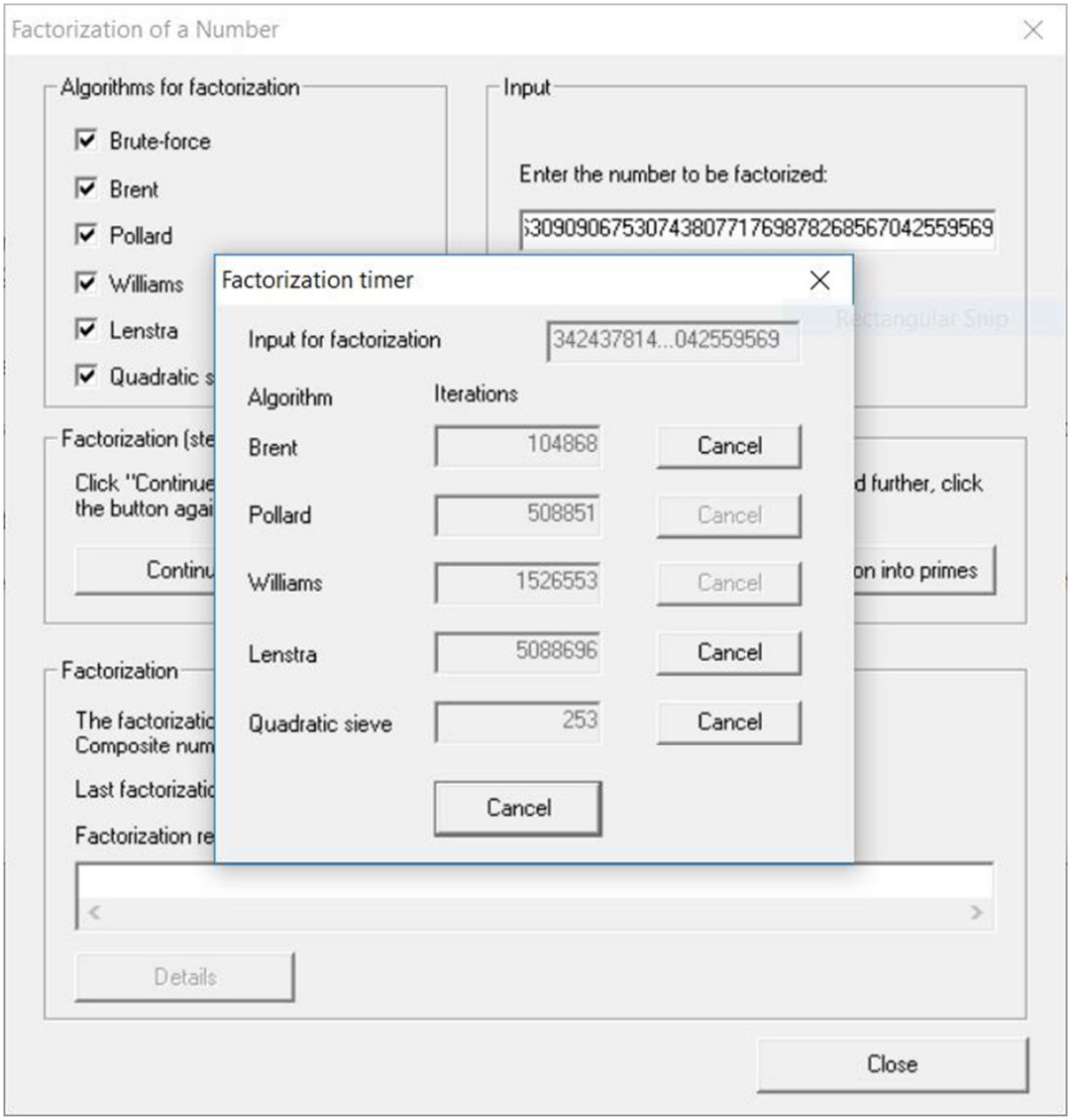

Analysis Options
Output options for automatic analysis
Caesar
Derived key
Correlation
Histograms
Vigenère, XOR, Addition
Derived key
Derived key length
Autocorrelation
Show further analysis results
Options for the Vigenère analysis according to Schroedel
Extensive logging
Dictionary:
D:\Users\kwnstantinos\AppData\Local\Cry
Search...
Digram file:
D:\Users\kwnstantinos\AppData\Local\Cry
Search...
Trigram file:
D:\Users\kwnstantinos\AppData\Local\Cry
Search...
Options for brute-force attacks against modern symmetric algorithms
See menu: Analysis \ Symmetric Encryption (modern)
Number of bytes of the ciphertext document used for the entropy test:
160
Alphabet for the expected cleartext:
All 256 characters
Printable characters (ascii 32 - 256)
Characters as defined in menu: Options \ Text Options
Apply
Restore default
Cancel

n =

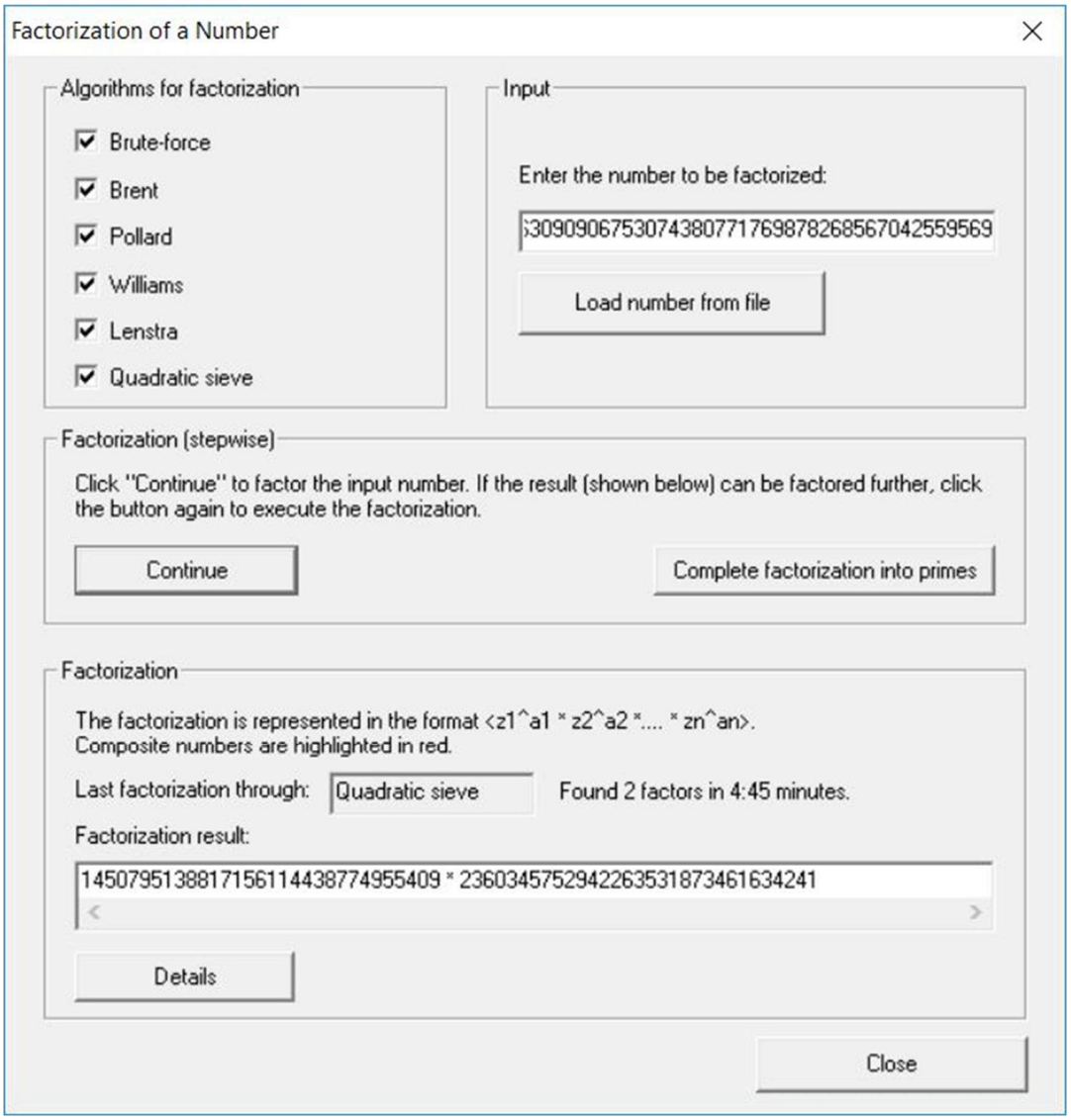


342437814429635609096309090675307438077176987826856704255 9569(200 bit)

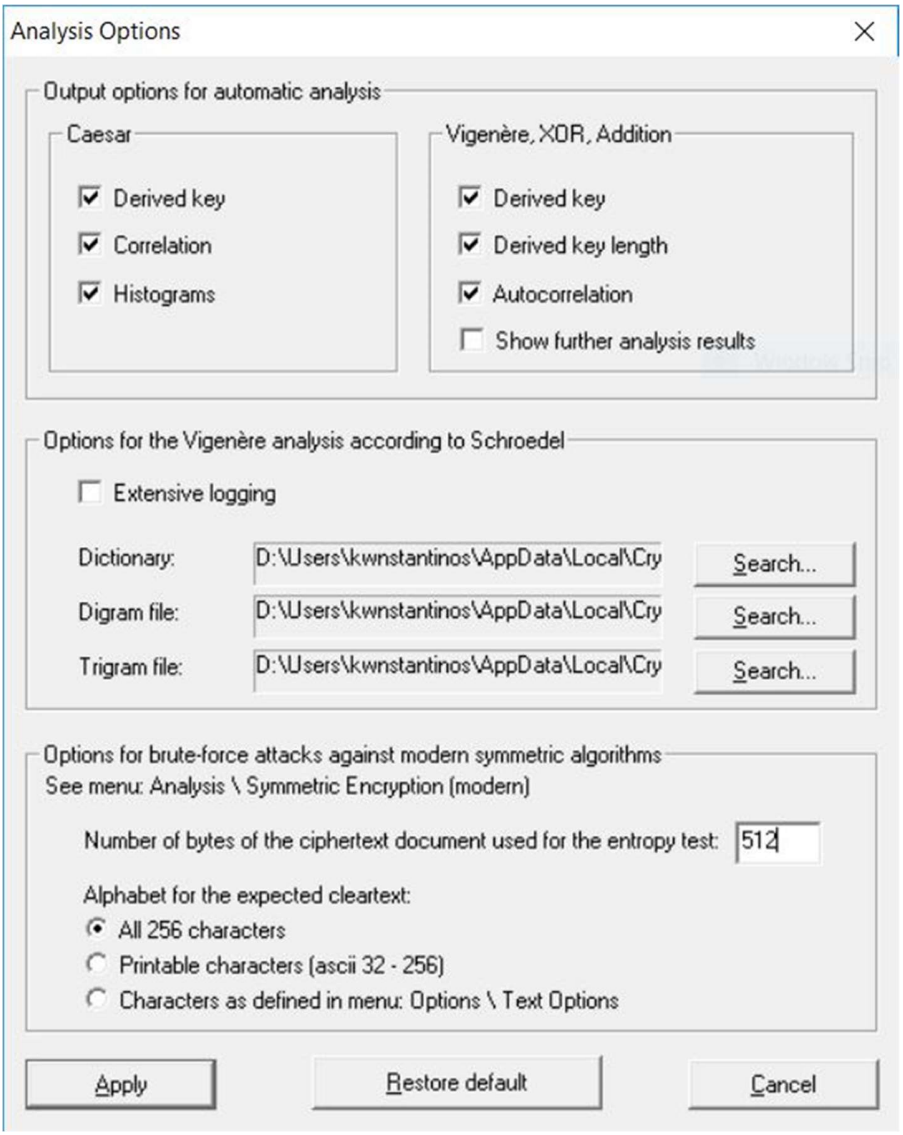

Analysis Options
Output options for automatic analysis
Caesar
Derived key
Correlation
Histograms
Vigenère, XOR, Addition
Derived key
Derived key length
Autocorrelation
Show further analysis results
Options for the Vigenère analysis according to Schroedel
Extensive logging
Dictionary:
D:\Users\kwnstantinos\AppData\Local\Cry
Search...
Digram file:
D:\Users\kwnstantinos\AppData\Local\Cry
Search...
Trigram file:
D:\Users\kwnstantinos\AppData\Local\Cry
Search...
Options for brute-force attacks against modern symmetric algorithms
See menu: Analysis \ Symmetric Encryption (modern)
Number of bytes of the ciphertext document used for the entropy test:
200
Alphabet for the expected cleartext:
All 256 characters
Printable characters (ascii 32 - 256)
Characters as defined in menu: Options \ Text Options
Apply
Restore default
Cancel

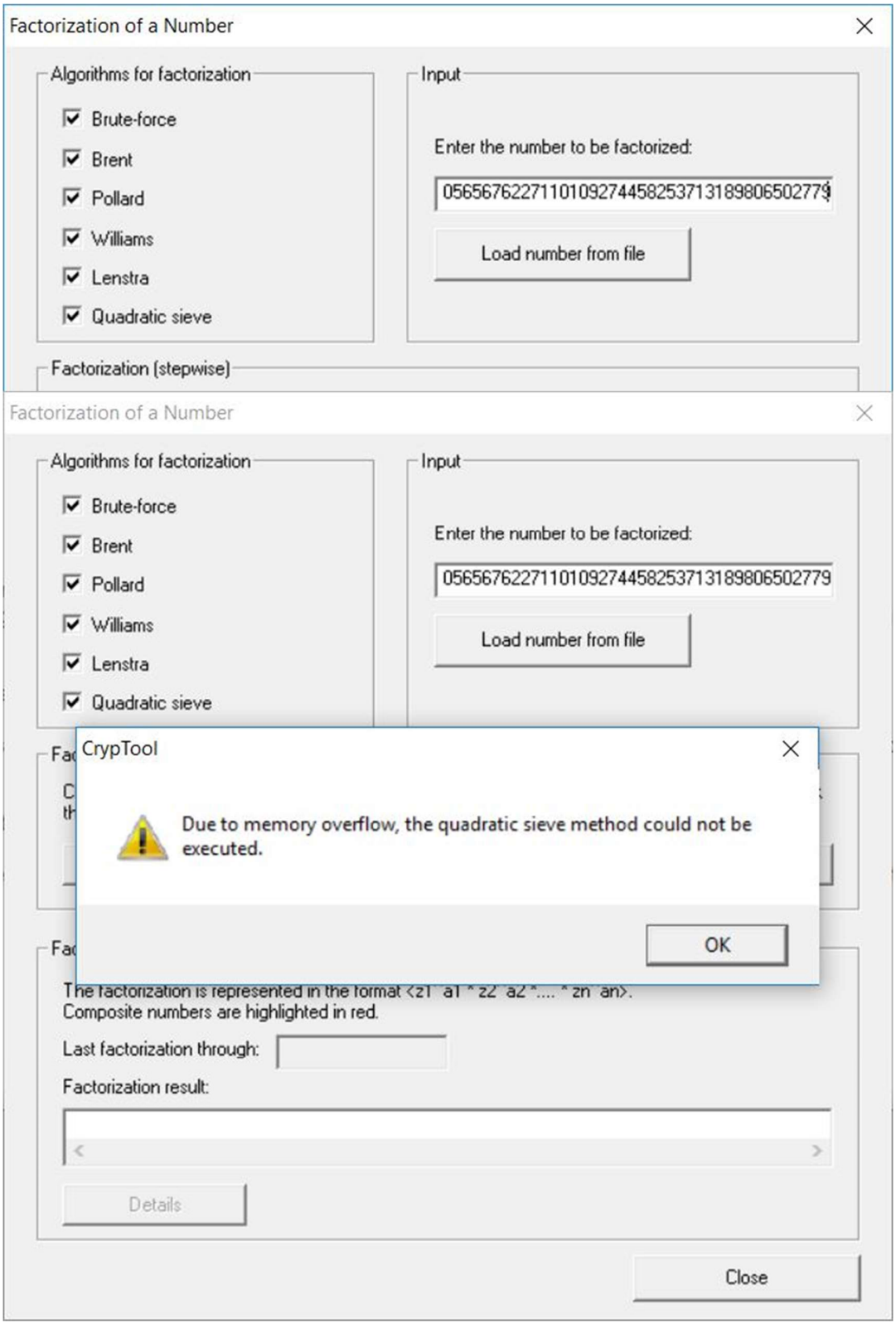

Factorization of a Number
Algorithms for factorization
Brute-force
Brent
Pollard
Williams
Lenstra
Quadratic s
Input
Enter the number to be factorized:
Factorization timer
Input for factorization
342437814...042559569
Algorithm
Iterations
Brent
104868
Cancel
Pollard
508851
Cancel
Williams
1526553
Cancel
Lenstra
5088696
Cancel
Quadratic sieve
253
Cancel
Cancel
Factorization (ste
Click "Continue
the button agai
Continu
d further, click
on into primes
Factorization
The factorizatic
Composite num
Last factorizatic
Factorization re
Details
Close

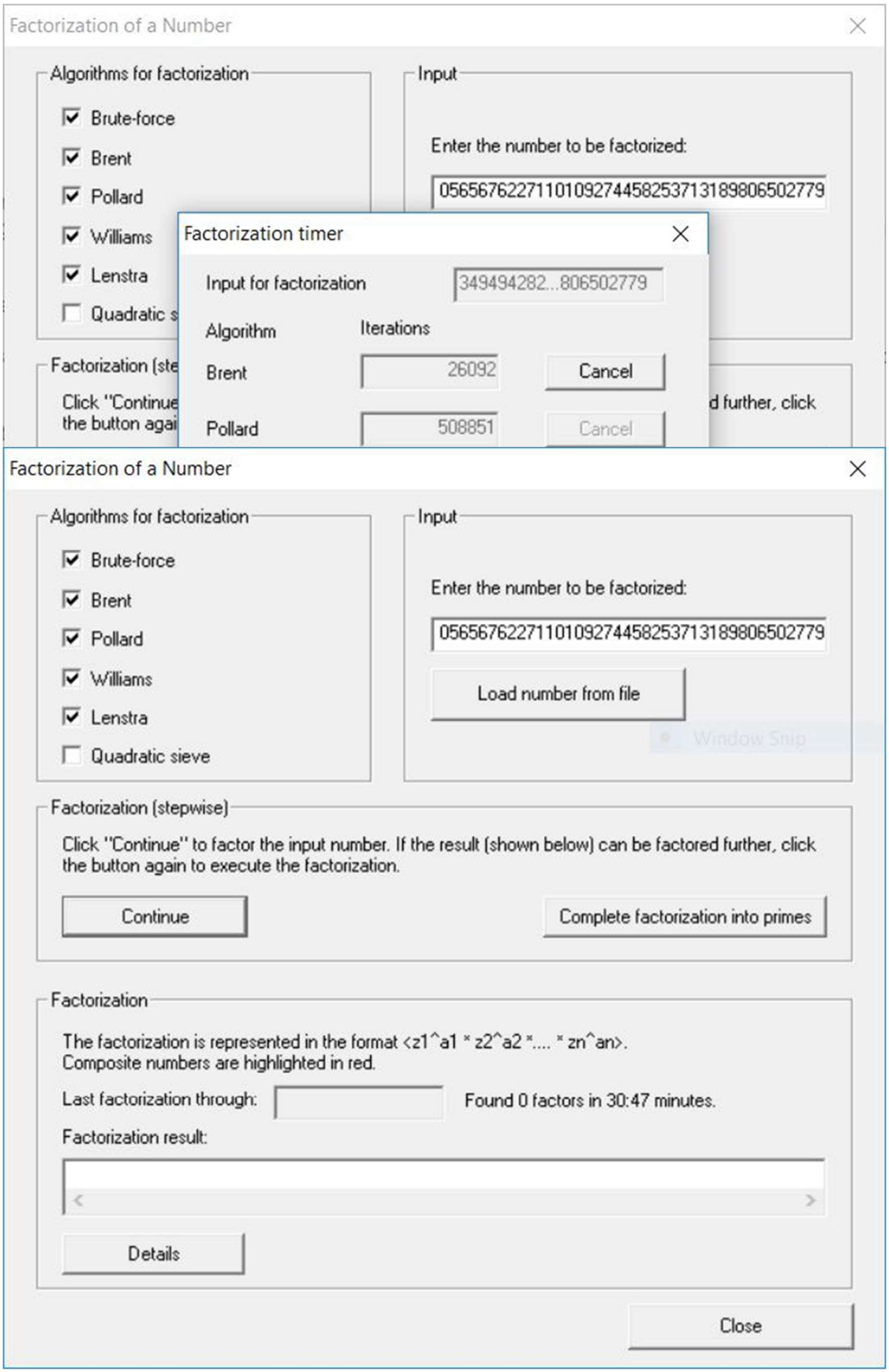
n =



34949428219027603669916737263191942467425261103383711036964777686816647287093628783
84114602968564594305134011762031056567622711010927445825371318980650277 9 (512 bit)


Analysis Options
Output options for automatic analysis
Caesar
Derived key
Correlation
Histograms
Vigenère, XOR, Addition
Derived key
Derived key length
Autocorrelation
Show further analysis results
Options for the Vigenère analysis according to Schroedel
Extensive logging
Dictionary:
D:\Users\kwnstantinos\AppData\Local\Cry
Search...
Digram file:
D:\Users\kwnstantinos\AppData\Local\Cry
Search...
Trigram file:
D:\Users\kwnstantinos\AppData\Local\Cry
Search...
Options for brute-force attacks against modern symmetric algorithms
See menu: Analysis \ Symmetric Encryption (modern)
Number of bytes of the ciphertext document used for the entropy test:
512
Alphabet for the expected cleartext:
All 256 characters
Printable characters (ascii 32 - 256)
Characters as defined in menu: Options \ Text Options
Apply
Restore default
Cancel


Factorization of a Number
Algorithms for factorization
Brute-force
Brent
Pollard
Williams
Lenstra
Quadratic sieve
Input
Enter the number to be factorized:
056567622711010927445825371318980650277
Load number from file
Factorization (stepwise)
Factorization of a Number
Algorithms for factorization
Brute-force
Brent
Pollard
Williams
Lenstra
Quadratic sieve
Input
Enter the number to be factorized:
056567622711010927445825371318980650277
Load number from file
CrypTool
Due to memory overflow, the quadratic sieve method could not be executed.
OK
Composite numbers are highlighted in red.
Last factorization through:
Factorization result:
Details
Close



(β) Χρήση GPG (Κάθε

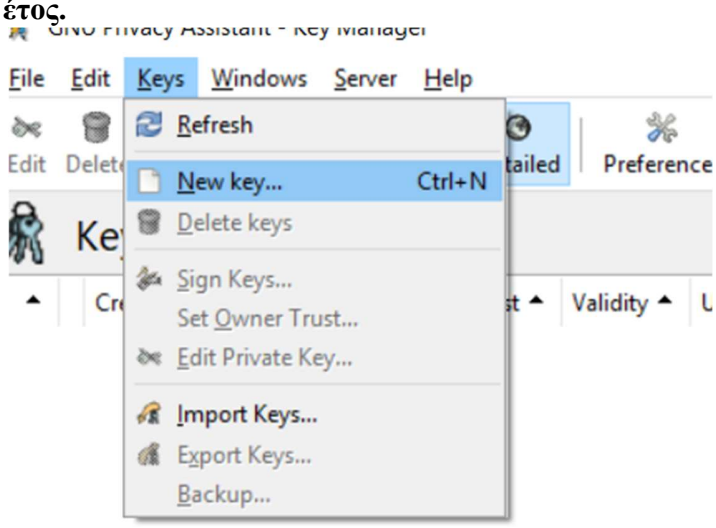
μέλος της ομάδας εργασίας εκτελεί τα παρακάτω βήματα)

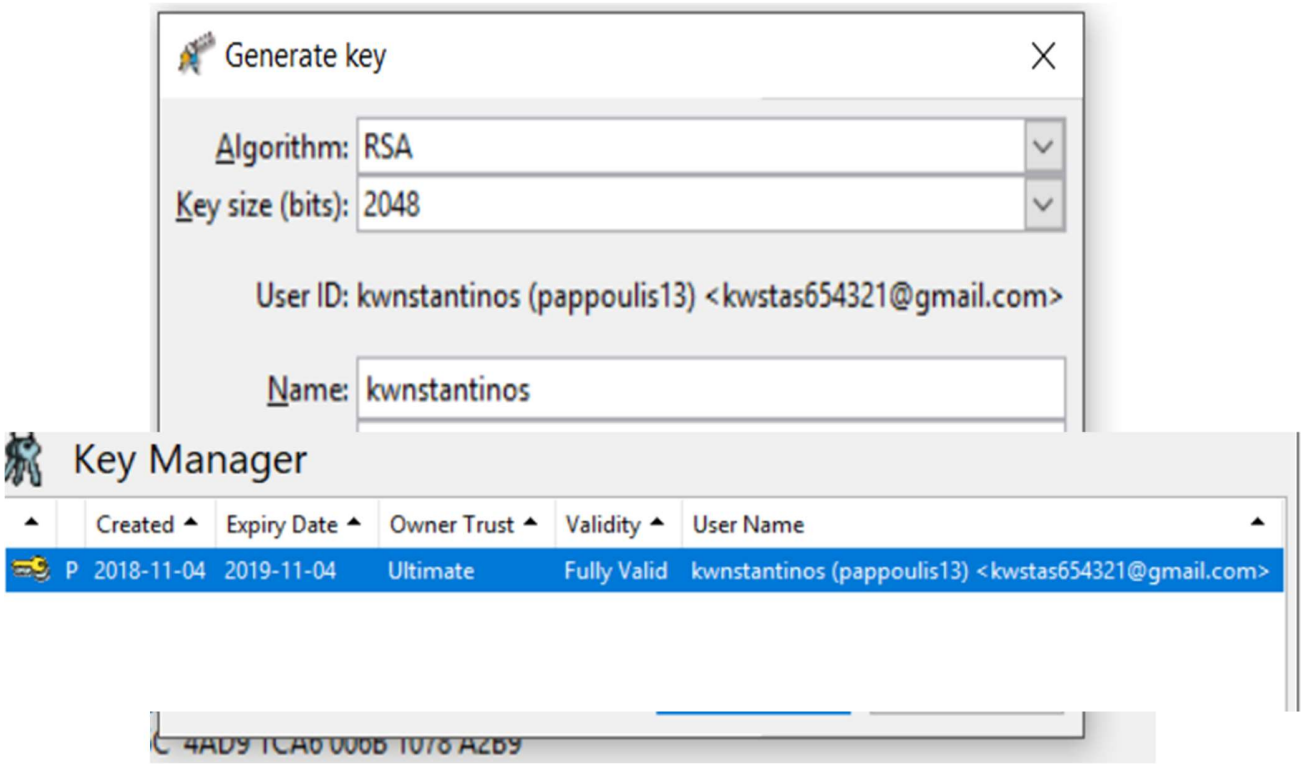
1. Δημιουργήστε ένα ζεύγος κλειδιών με τη χρήση του GPG με ημερομηνία λήξης του κλειδιού σας 1 έτος.
2. Ανεβάστε το κλειδί (πιστοποιητικό) σας σε κάποιον key server.
3. Αναζητήστε και εγκαταστήστε τα κλειδιά των άλλων μελών της ομάδας σας στον υπολογιστή σας (μέσω του GPG). Υπογράψτε τα κλειδιά των άλλων μελών της ομάδας σας με το δικό σας κλειδί. Αλλάξτε το επίπεδο εμπιστοσύνης των κλειδιών αυτών σε έμπιστα.
4. Εγκαταστήστε σε έναν mail client της επιλογής σας το δικό σας πιστοποιητικό καθώς και τα πιστοποιητικά των άλλων χρηστών.

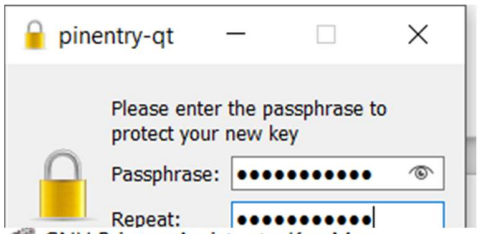
Ανταλλάξτε μέσω email ένα κρυπτογραφημένο και υπογεγραμμένο μήνυμα.(Υπόδειξη: εγκαταστήστε κάποιο κατάλληλο plugin για τον mail client. Πχ. στον thunderbird μπορείτε να εγκαταστήσετε το πρόσθετο enigmail για τη διαχείριση κλειδιών του openPGP).

Συμπεριλάβετε στο παραδοτέο σας ενδεικτικά screenshots για τα βήματα που απαιτείται.

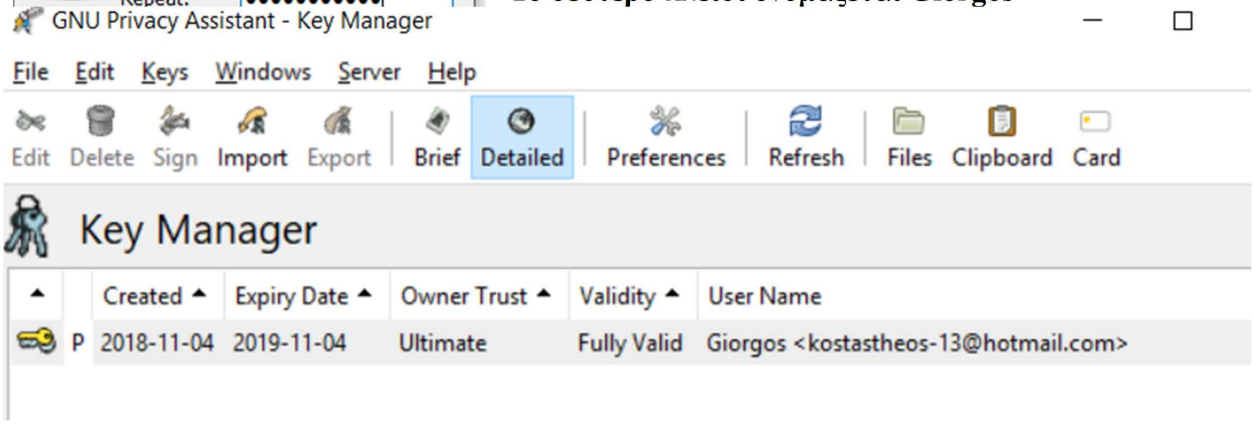
1. Δημιουργήστε ένα ζεύγος κλειδιών με τη χρήση του GPG με ημερομηνία λήξης του κλειδιού σας 1 έτος.





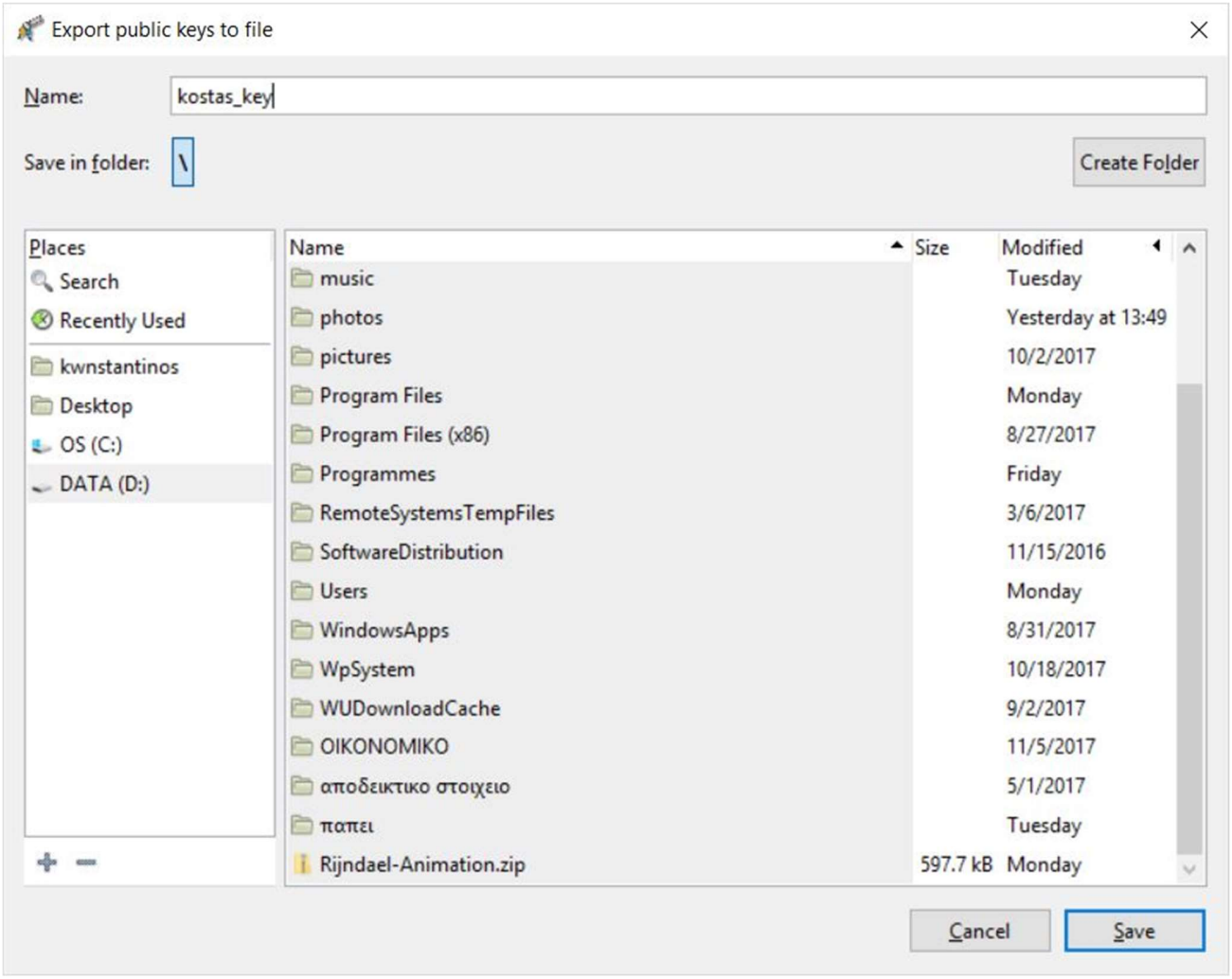


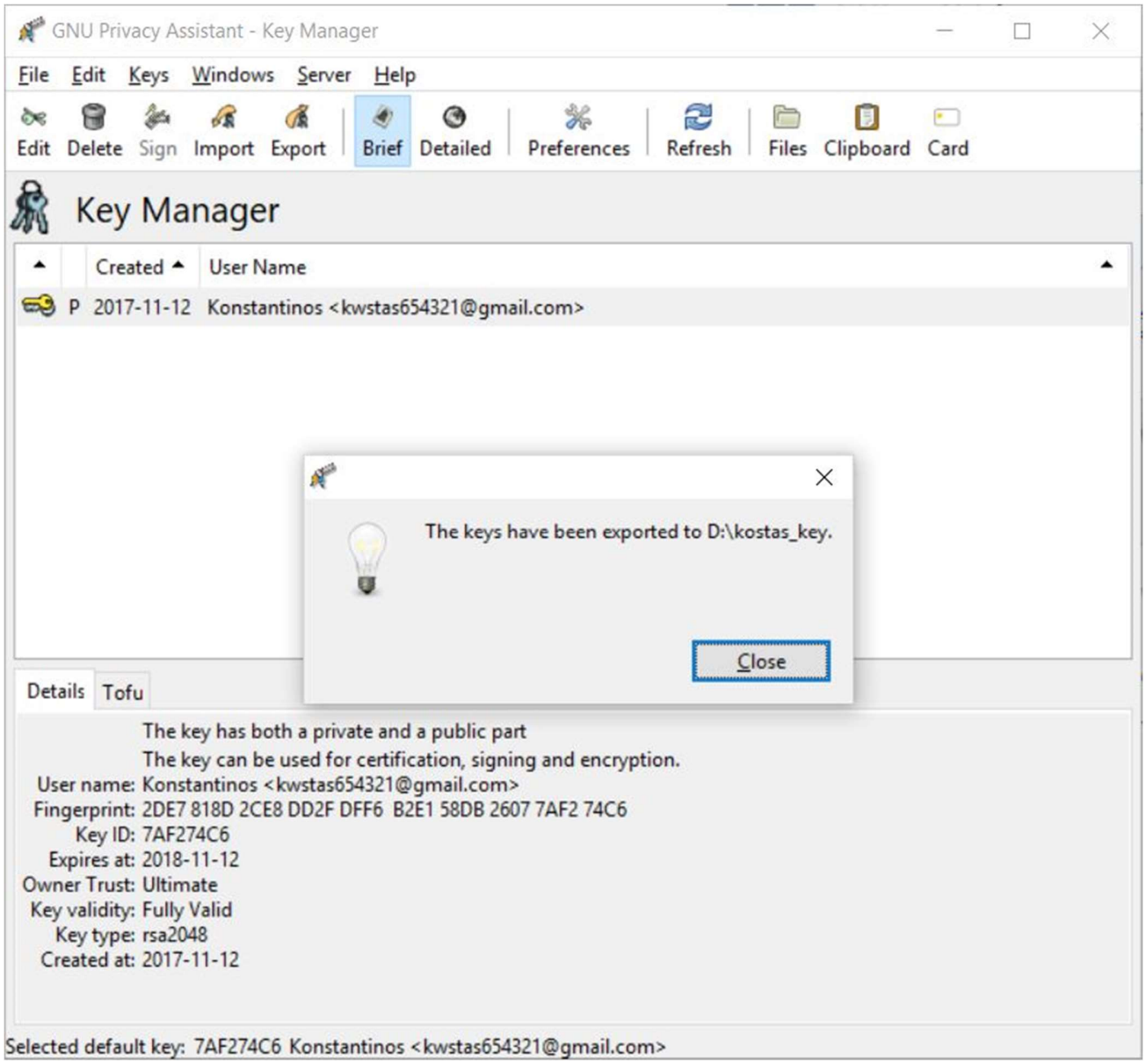
Φτιαχνω και ένα δεύτερο κλειδι για να στείλω μύνημα απο έναν αλλον υπολογίστη.
Το δευτερο κλειδι ονομάζεται Giorgos

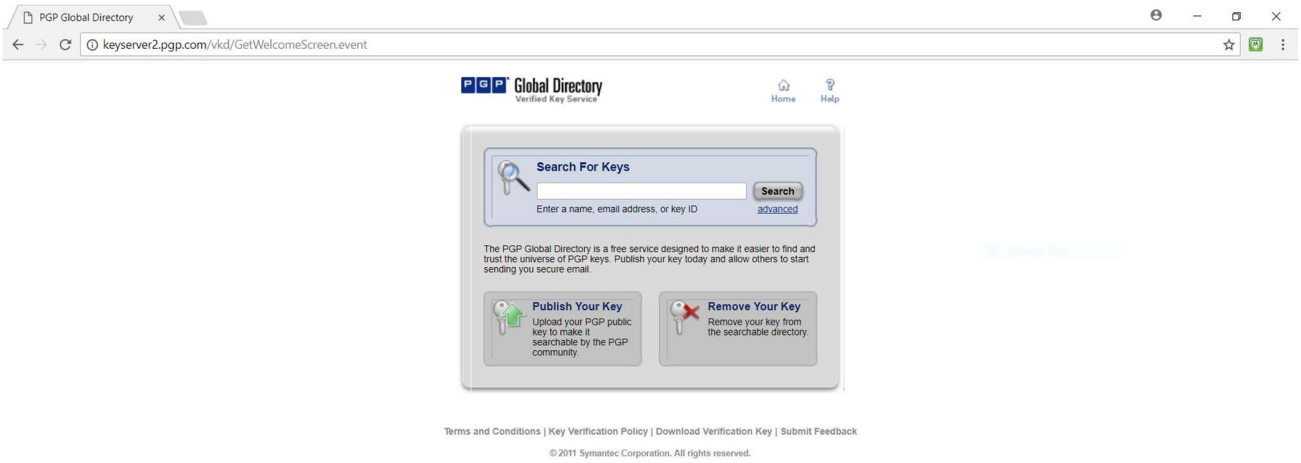


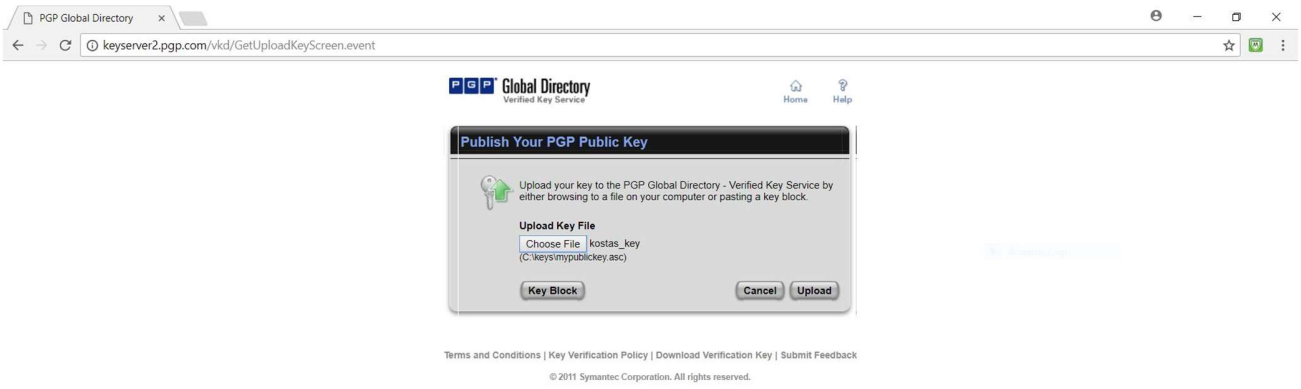
2. Ανεβάστε το κλειδί (πιστοποιητικό) σας σε κάποιον key server.

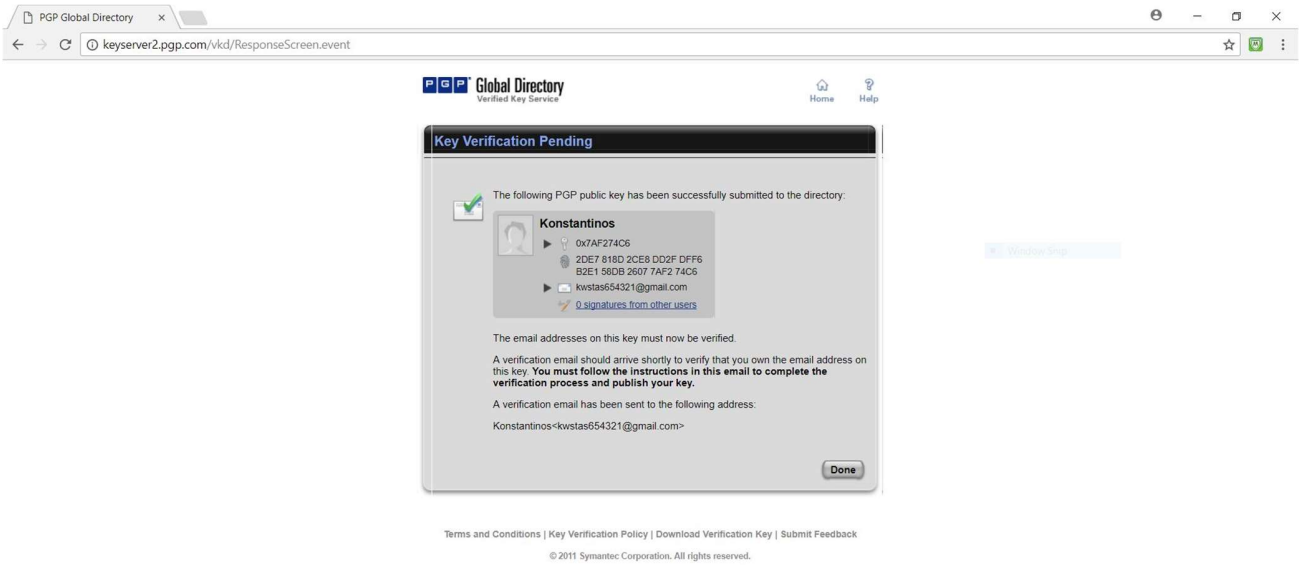
Ανεβάζω το κλειδί του Κώστα

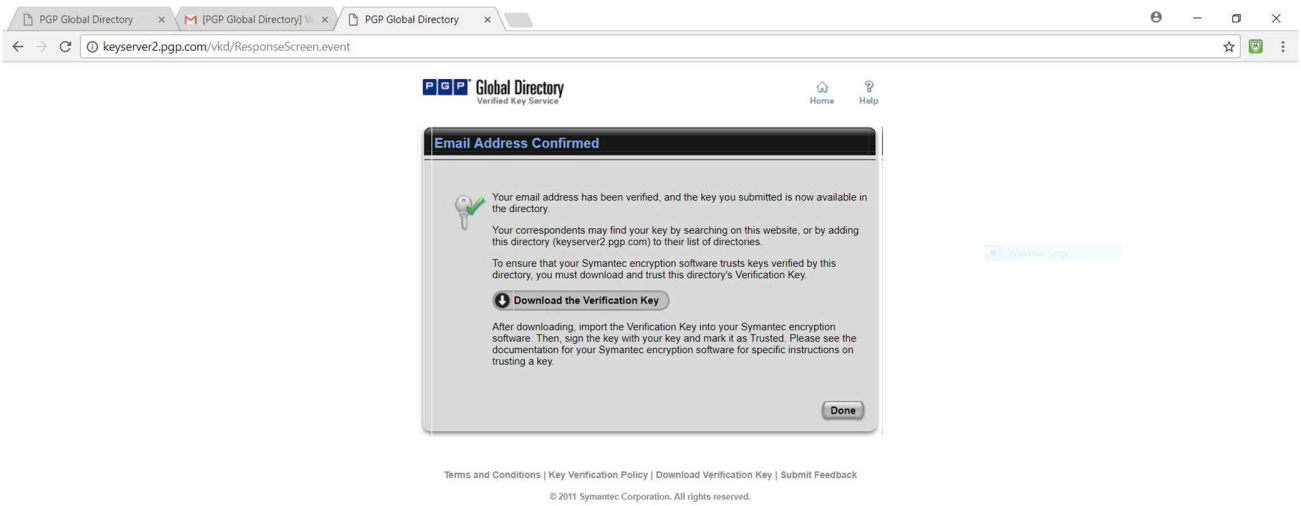

Export public keys to file
Name:
kostas_key
Save in folder:
\
Create Folder
Places
Search
Recently Used
kwnstantinos
Desktop
OS (C:)
DATA (D:)
Name
Size
Modified
music
Tuesday
photos
Yesterday at 13:49
pictures
10/2/2017
Program Files
Monday
Program Files (x86)
8/27/2017
Programmes
Friday
RemoteSystemsTempFiles
3/6/2017
SoftwareDistribution
11/15/2016
Users
Monday
WindowsApps
8/31/2017
WpSystem
10/18/2017
WUDownloadCache
9/2/2017
OIKONOMIKO
11/5/2017
αποδεικτικο στοιχειο
5/1/2017
παπει
Tuesday
Rijndael-Animation.zip
597.7 kB
Monday
Cancel
Save

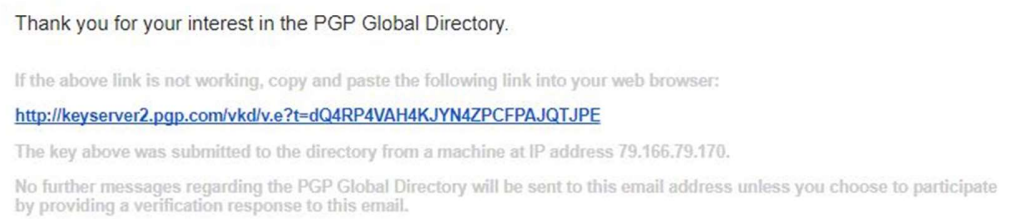

GNU Privacy Assistant - Key Manager
File Edit Keys Windows Server Help
Edit Delete Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card
Key Manager
Created
User Name
P 2017-11-12 Konstantinos <kwstas654321@gmail.com>
The keys have been exported to D:\kostas_key.
Close
Details Tofu
The key has both a private and a public part
The key can be used for certification, signing and encryption.
User name: Konstantinos <kwstas654321@gmail.com>
Fingerprint: 2DE7 818D 2CE8 DD2F DFF6 B2E1 58DB 2607 7AF2 74C6
Key ID: 7AF274C6
Expires at: 2018-11-12
Owner Trust: Ultimate
Key validity: Fully Valid
Key type: rsa2048
Created at: 2017-11-12
Selected default key: 7AF274C6 Konstantinos <kwstas654321@gmail.com>


PGP Global Directory
keyserver2.pgp.com/vkd/GetWelcomeScreen.event
Global Directory
Verified Key Service
Home
Help
Search For Keys
Search
Enter a name, email address, or key ID
advanced
The PGP Global Directory is a free service designed to make it easier to find and trust the universe of PGP keys. Publish your key today and allow others to start sending you secure email.
Publish Your Key
Upload your PGP public key to make it searchable by the PGP community.
Remove Your Key
Remove your key from the searchable directory.
Terms and Conditions | Key Verification Policy | Download Verification Key | Submit Feedback
© 2011 Symantec Corporation. All rights reserved.

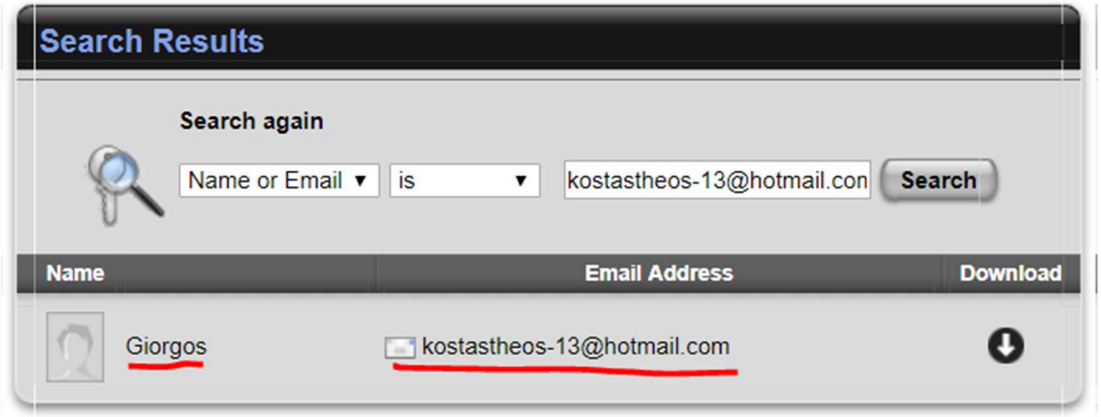

PGP Global Directory
keyserver2.pgp.com/vkd/GetUploadKeyScreen.event
Global Directory
Verified Key Service
Home
Help
Publish Your PGP Public Key
Upload your key to the PGP Global Directory - Verified Key Service by either browsing to a file on your computer or pasting a key block.
Upload Key File
Choose File
kostas_key
(C:\keys\mypublickey.asc)
Key Block
Cancel
Upload
Terms and Conditions | Key Verification Policy | Download Verification Key | Submit Feedback
© 2011 Symantec Corporation. All rights reserved.


PGP Global Directory
keyserver2.pgp.com/vkd/ResponseScreen.event
PGP Global Directory
Verified Key Service
Home
Help
Key Verification Pending
The following PGP public key has been successfully submitted to the directory:
Konstantinos
0x7AF274C6
2DE7 818D 2CE8 DD2F DFF6
B2E1 58DB 2607 7AF2 74C6
kwstas654321@gmail.com
0 signatures from other users
The email addresses on this key must now be verified.
A verification email should arrive shortly to verify that you own the email address on this key. You must follow the instructions in this email to complete the verification process and publish your key.
A verification email has been sent to the following address:
Konstantinos<kwstas654321@gmail.com>
Done
Terms and Conditions | Key Verification Policy | Download Verification Key | Submit Feedback
© 2011 Symantec Corporation. All rights reserved.





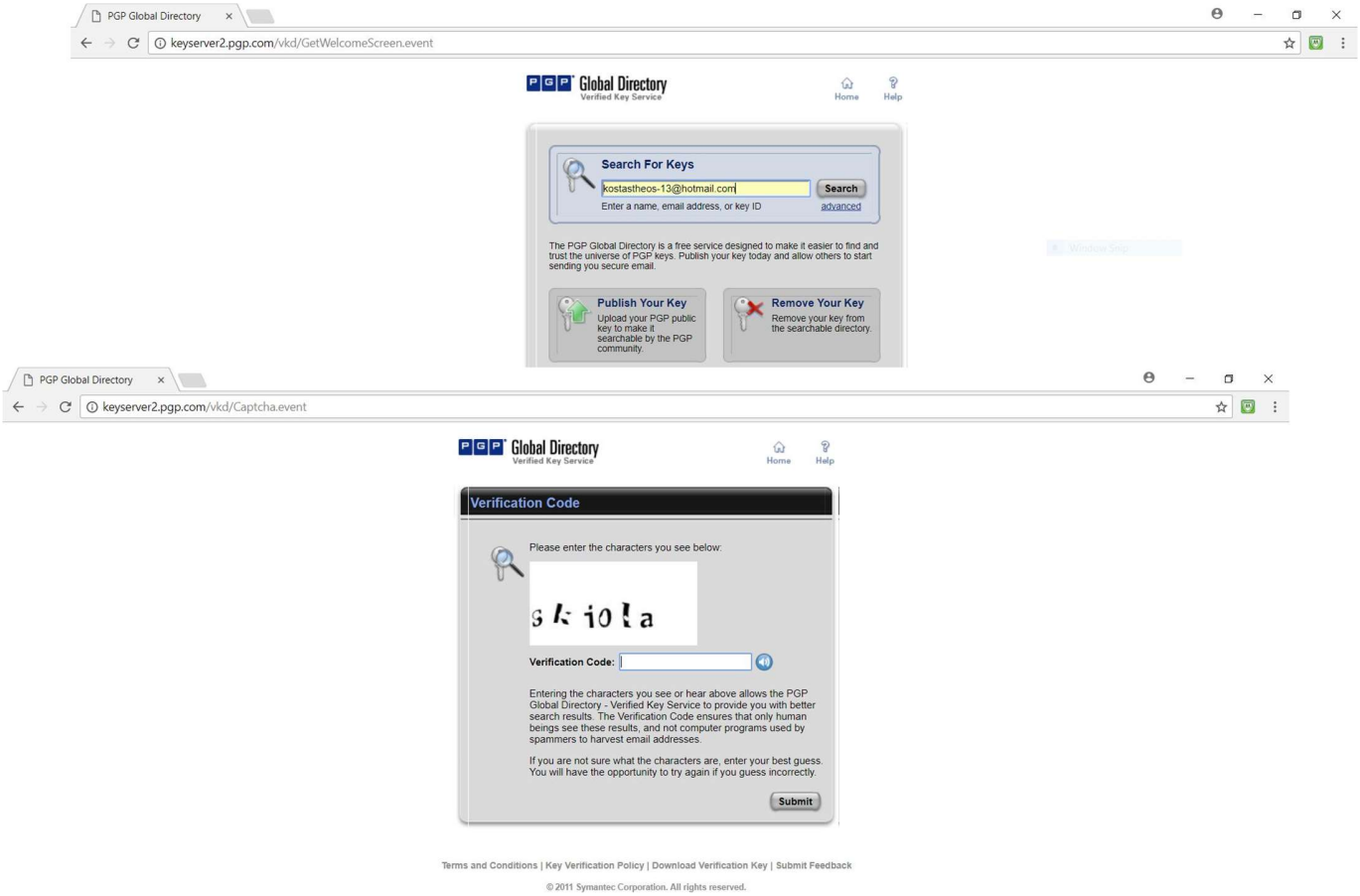
Την ίδια διαδικασία για τον Giorgo

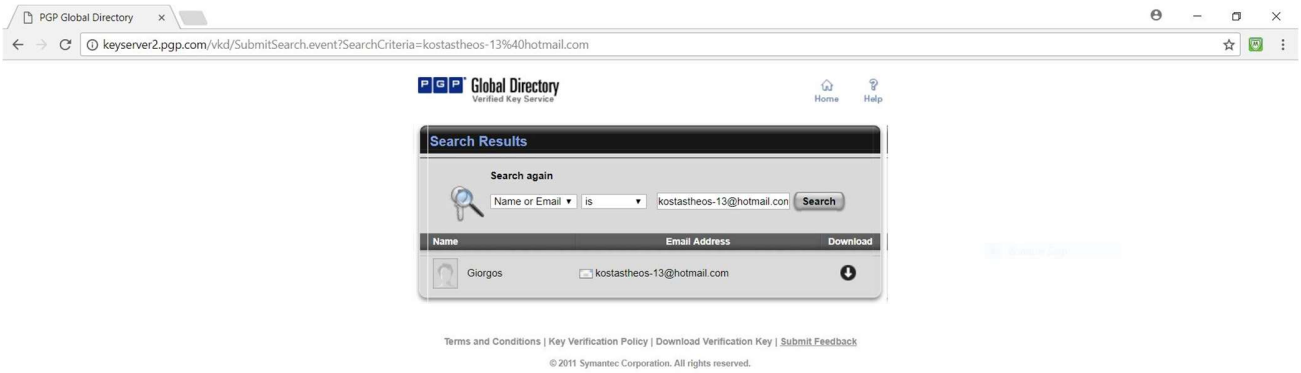


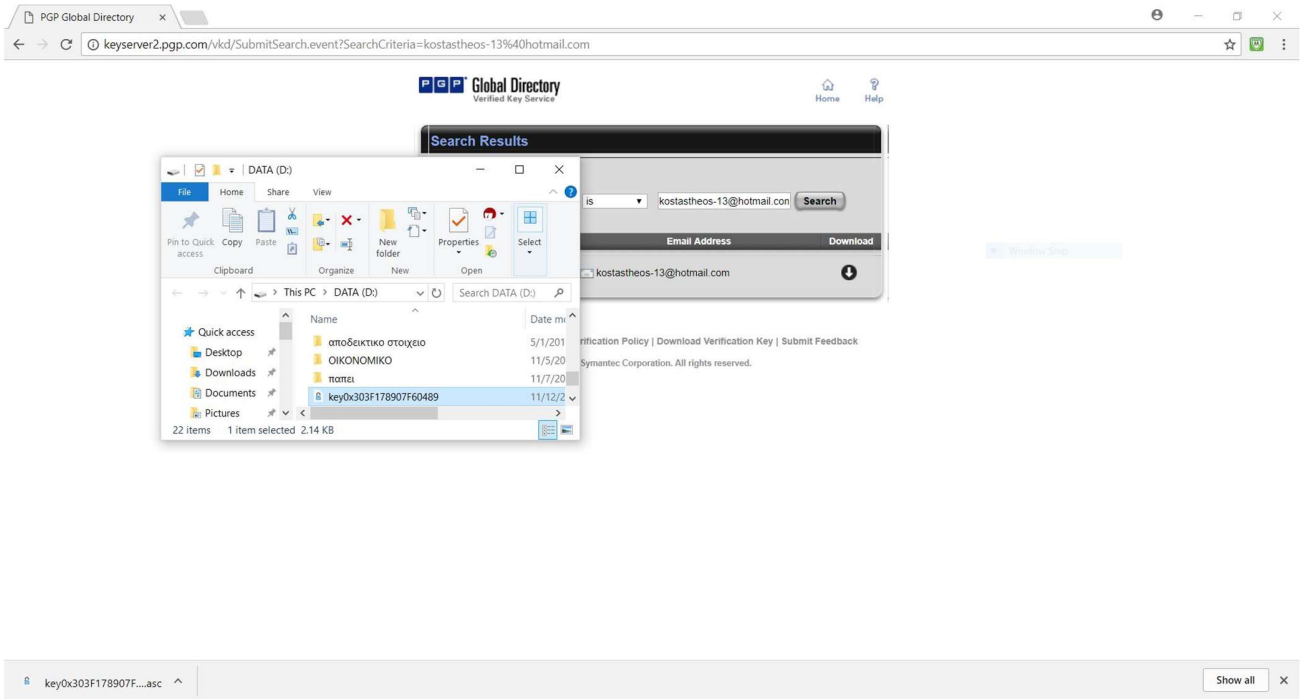
Εδω βλέπουμε οτι έχω ανεβάσει τον Giorgo στο pgp με την ιδια διαδικασία

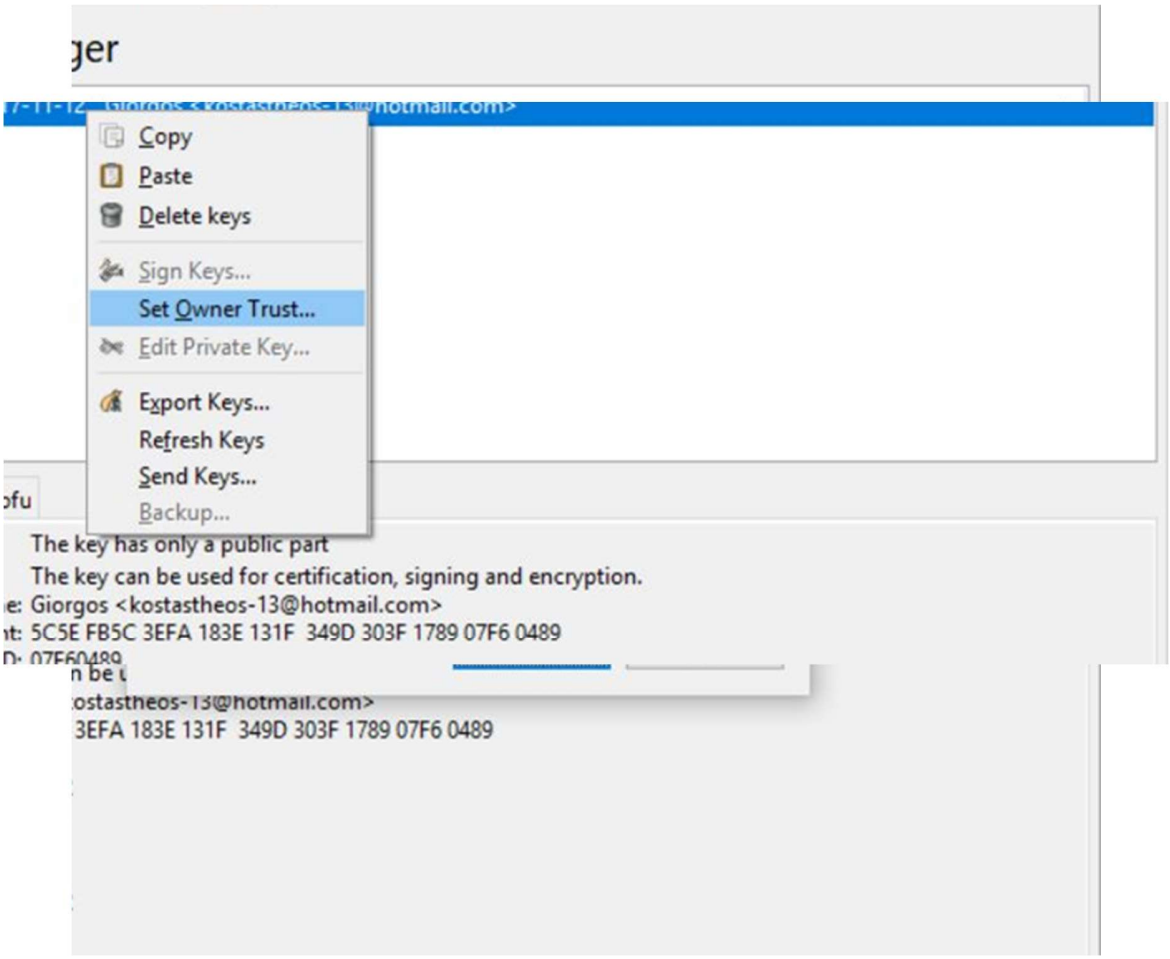
3. Αναζητήστε και εγκαταστήστε τα κλειδιά των άλλων μελών της ομάδας σας στον υπολογιστή σας (μέσω του GPG). Υπογράψτε τα κλειδιά των άλλων μελών της ομάδας σας με το δικό σας κλειδί. Αλλάξτε το επίπεδο εμπιστοσύνης των κλειδιών αυτών σε έμπιστα.

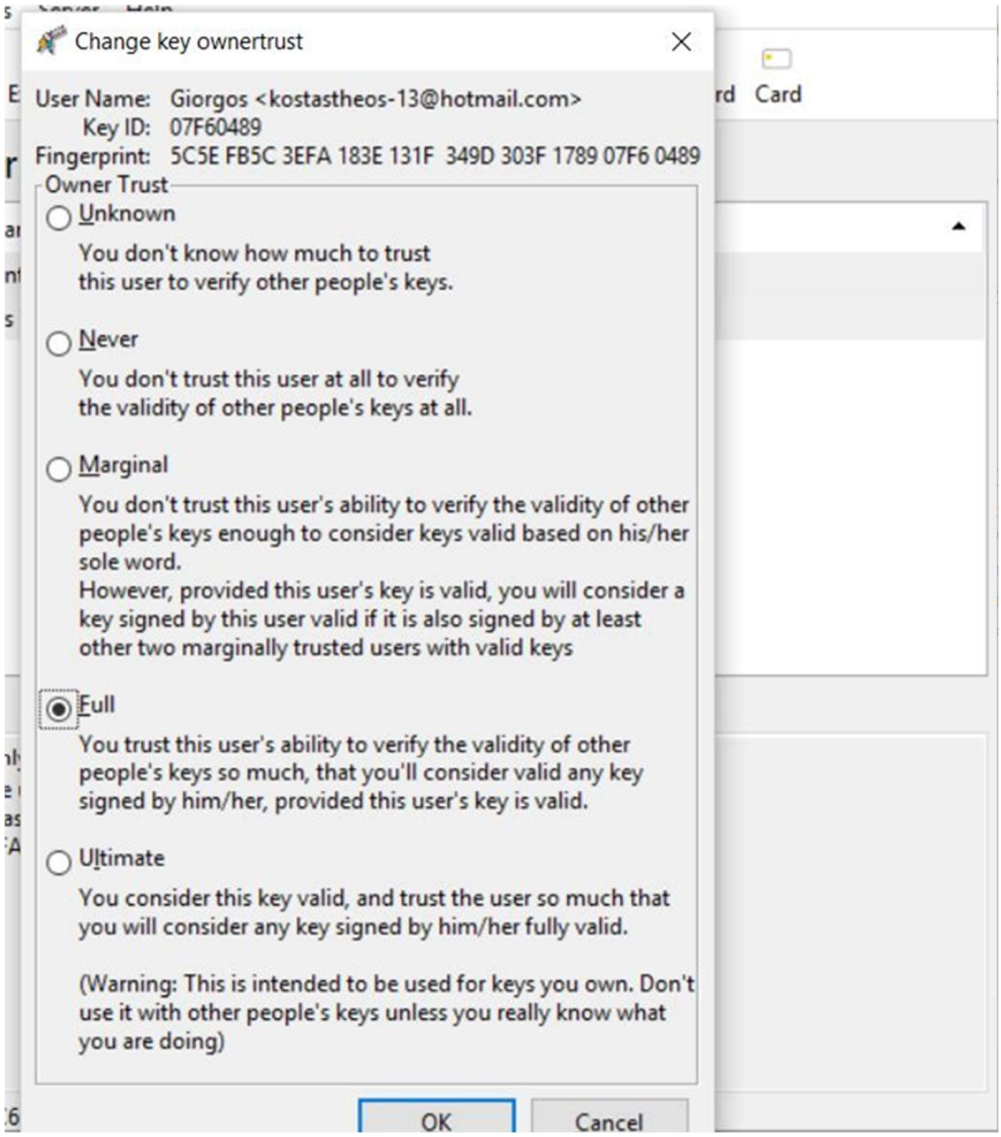
Αναζητηση το κλειδι του Γιωργου




PGP Global Directory
keyserver2.pgp.com/vkd/SubmitSearch.event?SearchCriteria=kostastheos-13%40hotmail.com
Global Directory
Verified Key Service
Home
Help
Search Results
Search again
Name or Email
is
kostastheos-13@hotmail.con
Search
Name
Email Address
Download
Giorgos
kostastheos-13@hotmail.com
Terms and Conditions | Key Verification Policy | Download Verification Key | Submit Feedback
© 2011 Symantec Corporation. All rights reserved.

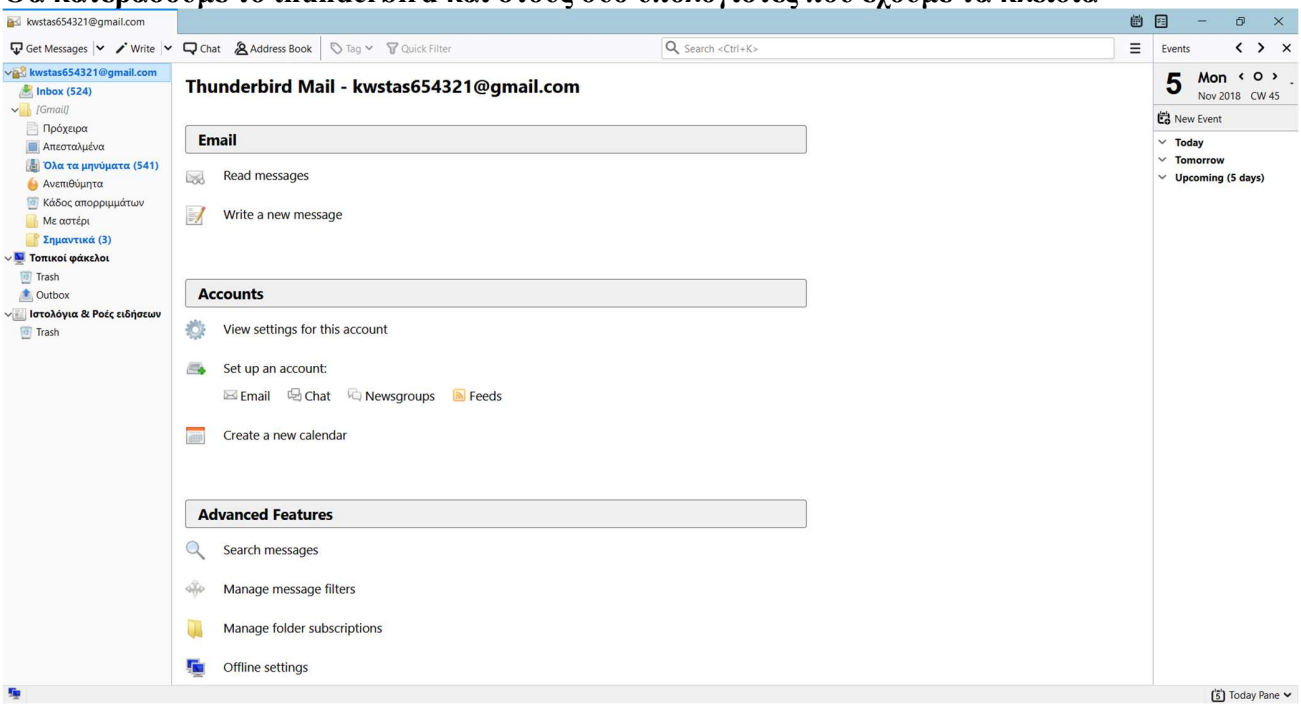

PGP Global Directory
keyserver2.pgp.com/vkd/SubmitSearch.event?SearchCriteria=kostastheos-13%40hotmail.com
Global Directory
Verified Key Service
Home
Help
Search Results
DATA (D:)
File
Home
Share
View
Pin to Quick access
Copy
Paste
Clipboard
New folder
Organize
New
Properties
Open
Select
This PC
DATA (D:)
Search DATA (D:)
Quick access
Desktop
Downloads
Documents
Pictures
Name
αποδεικτικο στοιχειο
ΟΙΚΟΝΟΜΙΚΟ
παπει
key0x303F178907F60489
22 items
1 item selected 2.14 KB
is
kostastheos-13@hotmail.com
Search
Email Address
Download
kostastheos-13@hotmail.com
Symantec Corporation. All rights reserved.
key0x303F178907F....asc
Show all


ger
Copy
Paste
Delete keys
Sign Keys...
Set Owner Trust...
Edit Private Key...
Export Keys...
Refresh Keys
Send Keys...
Backup...
The key has only a public part
The key can be used for certification, signing and encryption.
Giorgos <kostastheos-13@hotmail.com>
5C5E FB5C 3EFA 183E 131F 349D 303F 1789 07F6 0489
3EFA 183E 131F 349D 303F 1789 07F6 0489


Change key ownertrust
User Name: Giorgos <kostastheos-13@hotmail.com>
Key ID: 07F60489
Fingerprint: 5C5E FB5C 3EFA 183E 131F 349D 303F 1789 07F6 0489
Owner Trust
Unknown
You don't know how much to trust this user to verify other people's keys.
Never
You don't trust this user at all to verify the validity of other people's keys at all.
Marginal
You don't trust this user's ability to verify the validity of other people's keys enough to consider keys valid based on his/her sole word.
However, provided this user's key is valid, you will consider a key signed by this user valid if it is also signed by at least other two marginally trusted users with valid keys
Full
You trust this user's ability to verify the validity of other people's keys so much, that you'll consider valid any key signed by him/her, provided this user's key is valid.
Ultimate
You consider this key valid, and trust the user so much that you will consider any key signed by him/her fully valid.
(Warning: This is intended to be used for keys you own. Don't use it with other people's keys unless you really know what you are doing)
OK
Cancel
Card

4. Εγκαταστήστε σε έναν mail client της επιλογής σας το δικό σας πιστοποιητικό καθώς και τα πιστοποιητικά των άλλων χρηστών. Ανταλλάξτε μέσω email ένα κρυπτογραφημένο και υπογεγραμμένο μήνυμα.(Υπόδειξη: εγκαταστήστε κάποιο κατάλληλο plugin για τον mail client. Πχ. στον thunderbird μπορείτε να εγκαταστήσετε το πρόσθετο enigmail για τη διαχείριση κλειδιών του openPGP).

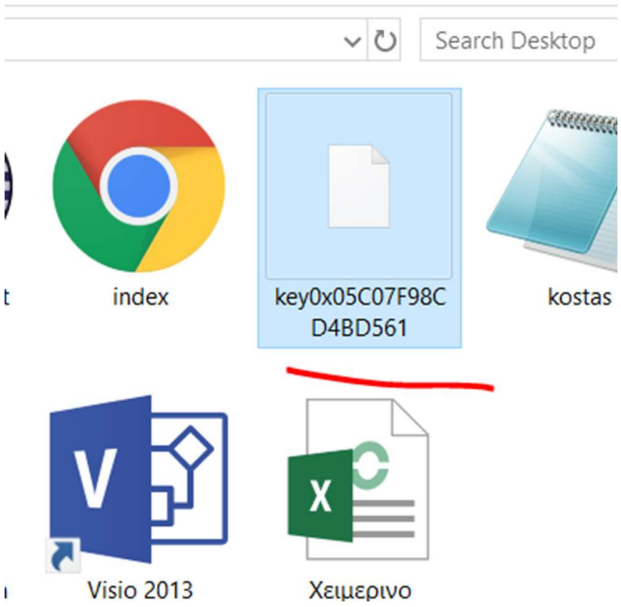
Θα κατέβασουμε το thunderbird και στους δυο υπολογιστές που έχουμε τα κλειδιά

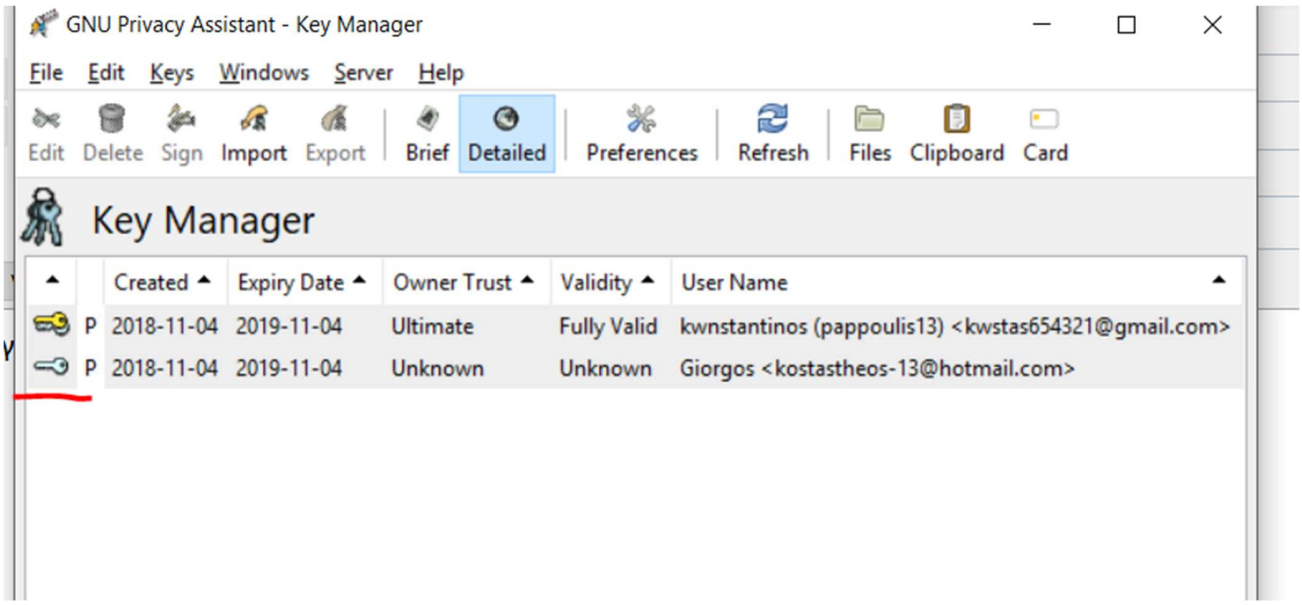


Εδω έχουμε το ενα mail το δικο μου που ονομάζεται κωστας kwstas654321@gmail.com

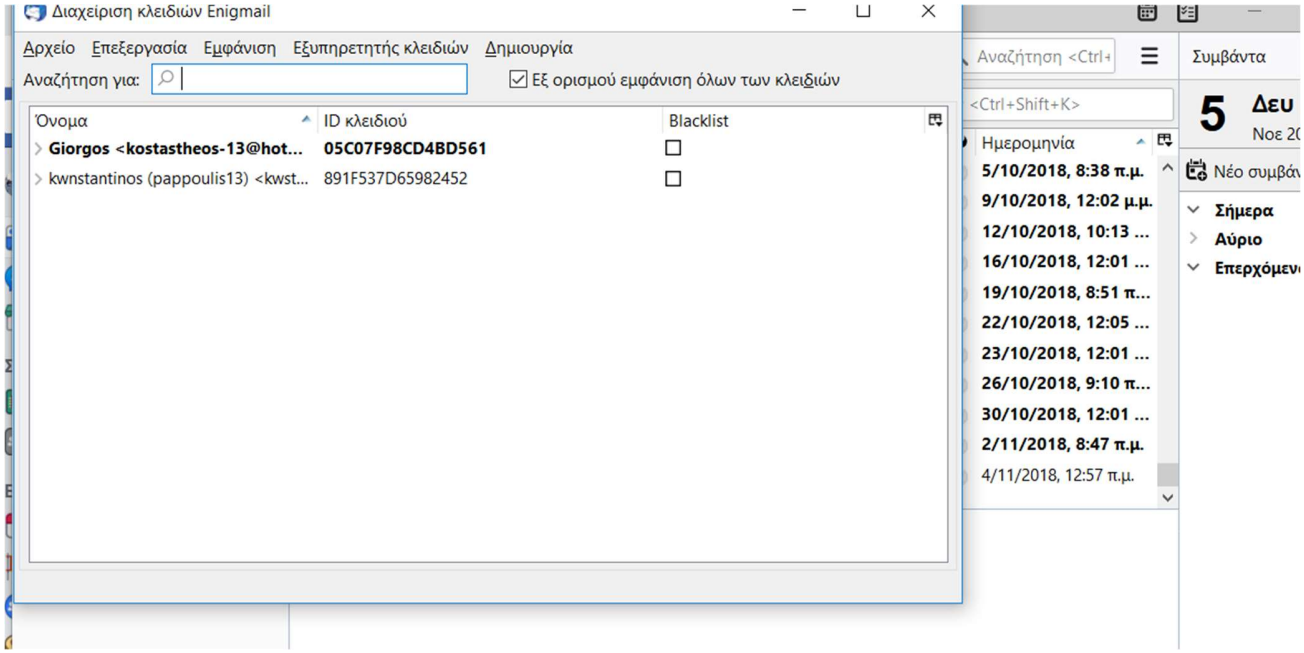
Κατεβαζω το κλειδι του Giorgou

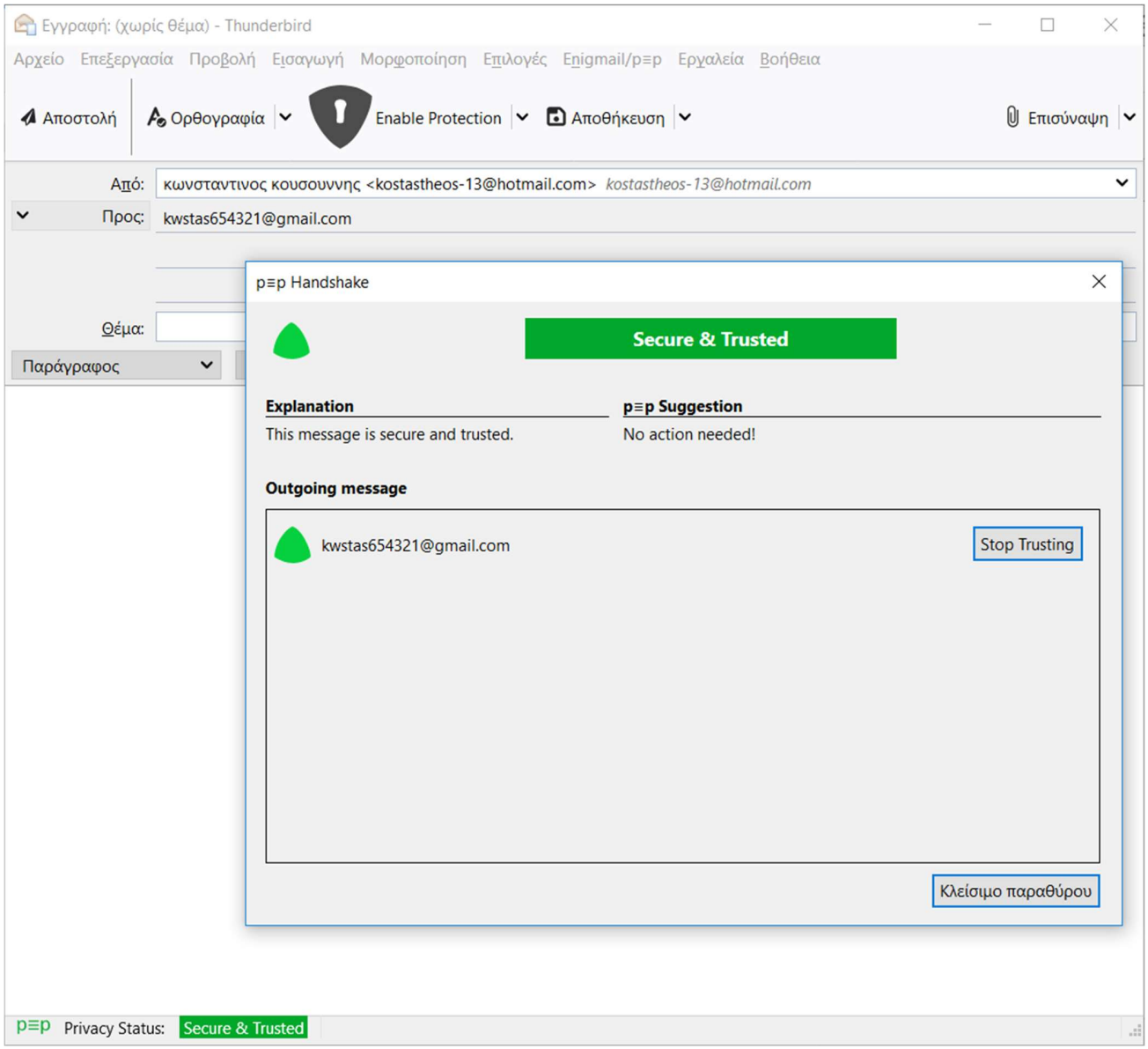
Το αποθηκευω καπου στον υπολογιστη μου

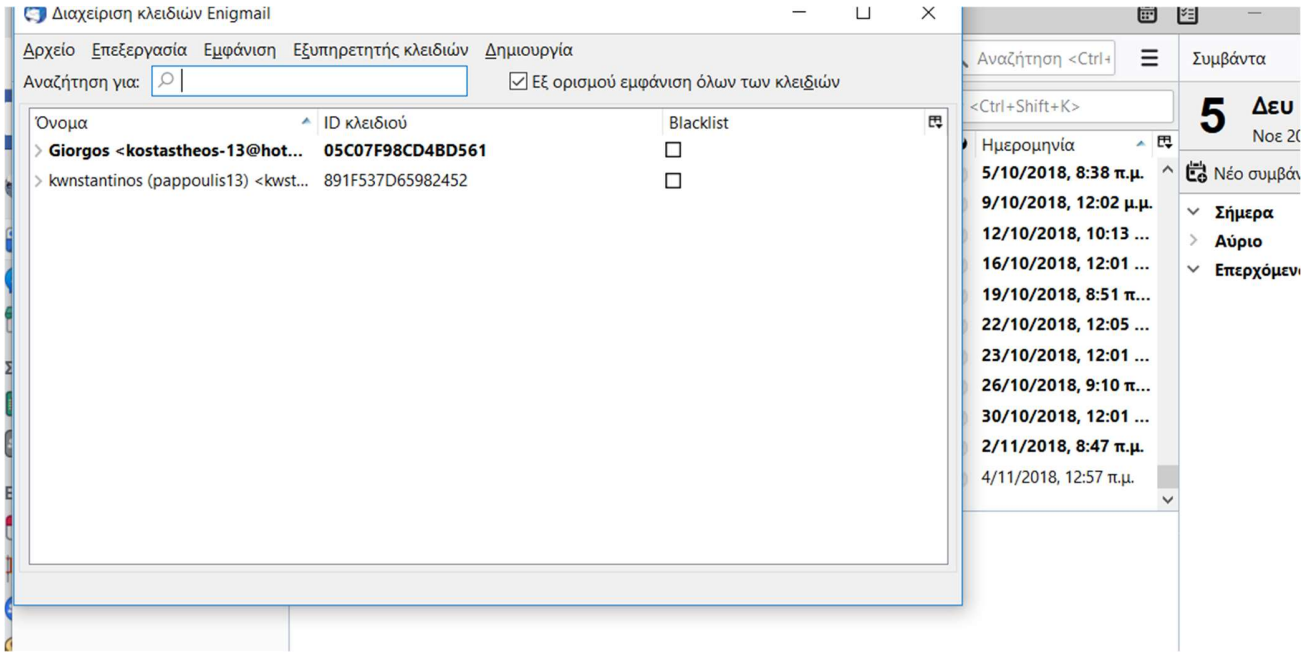




Και το κάνω import στο gpa οπως βλέπουμε ειναι το δημοσιο κλειδι του Giorgos


Διαχείριση κλειδιών Enigmail
Αρχείο Επεξεργασία Εμφάνιση Εξυπηρετητής κλειδιών Δημιουργία
Αναζήτηση για:
Εξ ορισμού εμφάνιση όλων των κλειδιών
Όνομα
ID κλειδιού
Blacklist
Giorgos <kostastheos-13@hot...
05C07F98CD4BD561
kwnstantinos (pappoulis13) <kwst...
891F537D65982452
Αναζήτηση <Ctrl+
<Ctrl+Shift+K>
Ημερομηνία
5/10/2018, 8:38 π.μ.
9/10/2018, 12:02 μ.μ.
12/10/2018, 10:13 ...
16/10/2018, 12:01 ...
19/10/2018, 8:51 π...
22/10/2018, 12:05 ...
23/10/2018, 12:01 ...
26/10/2018, 9:10 π...
30/10/2018, 12:01 ...
2/11/2018, 8:47 π.μ.
4/11/2018, 12:57 π.μ.
Συμβάντα
5
Δευ
Σήμερα
Αύριο


Εγγραφή: (χωρίς θέμα) - Thunderbird
Αρχείο Επεξεργασία Προβολή Εισαγωγή Μορφοποίηση Επιλογές Enigmail/p≡p Εργαλεία Βοήθεια
Αποστολή
Ορθογραφία
Enable Protection
Αποθήκευση
Επισύναψη
Από: κωνσταντινος κουσουννης <kostastheos-13@hotmail.com> kostastheos-13@hotmail.com
Προς: kwstas654321@gmail.com
Θέμα:
Παράγραφος
p≡p Handshake
Secure & Trusted
Explanation
This message is secure and trusted.
p≡p Suggestion
No action needed!
Outgoing message
kwstas654321@gmail.com
Stop Trusting
Κλείσιμο παραθύρου
p≡p Privacy Status: Secure & Trusted



Συντασουμε ενα κειμενο και το κρυπτογραφουμε με τα κλειδια που φτιαξαμε.

Το κειμενο μας έφτασε κρυπτογραφημενο.