Cvičení 8.4.2024

1. Nalezněte Eulerovo číslo pro n = 26, 29, 35, 49, 600, tj. nalezněte všechna m, 1≤m<n, která jsou nesoudělná s n.

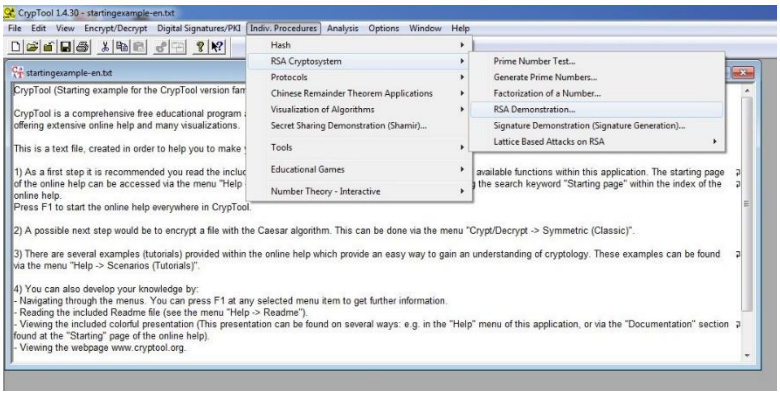
2. Nalezněte aditivní opačný prvek ke všem prvkům v množině celých čísel modulo m, kde m = 8, 11.

3. Nalezněte multiplikativní inverzní prvek ke všem prvkům v množině celých čísel modulo m, kde m = 8, 11.

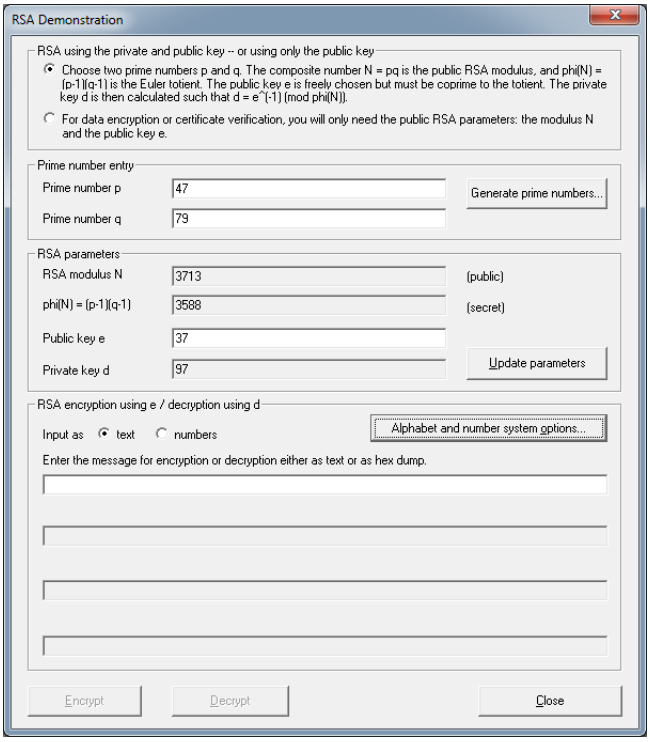
4. Simulujte šifrování a dešifrování pomocí RSA pokud jsou dány následující hodnoty:
   a) p=7, q=11, e=17, m=8,
   b) p=13, q=11, e=7, m=5,
   c) Pro určení multiplikativního inverzního (tedy soukromého klíče) prvku použijte EEA, např. https://planetcalc.com/3311/

Cryptool: Encryption or decryption of messages using the RSA key pair.

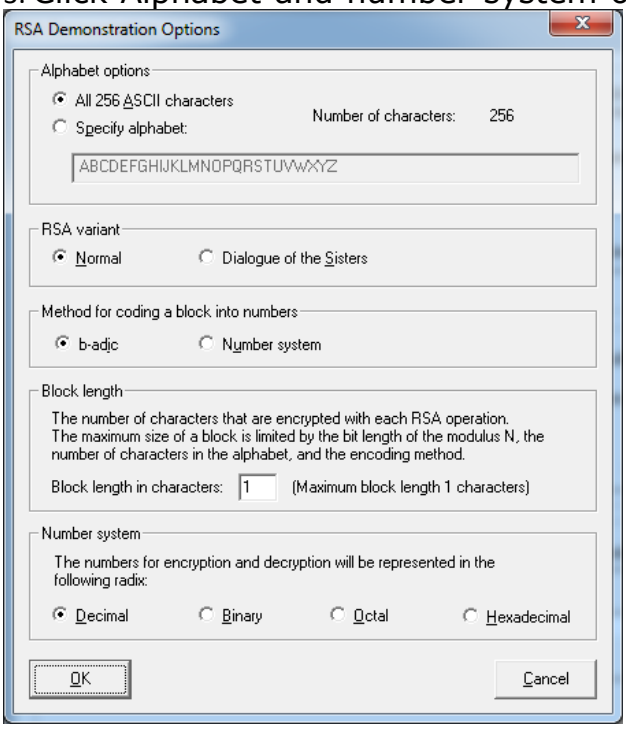
1. Select Individual Procedures/RSA Cryptosystem/RSA Demonstration



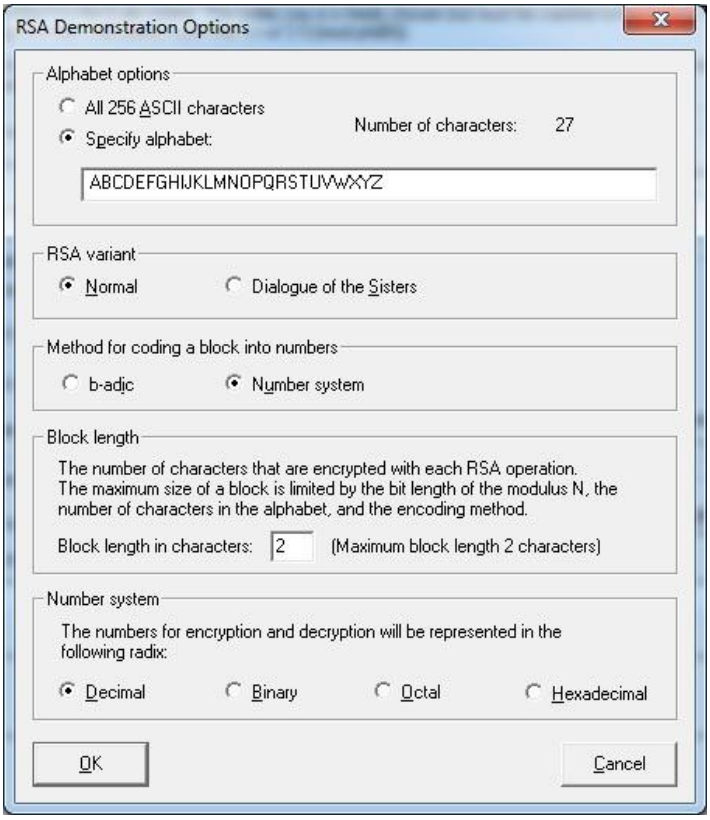
2. Enter the RSA key p=47, q=79, e=37. The parameters N = p*q=3713 and phi(N)=3588 and d=97 are calculated.



3. Click Alphabet and number system options



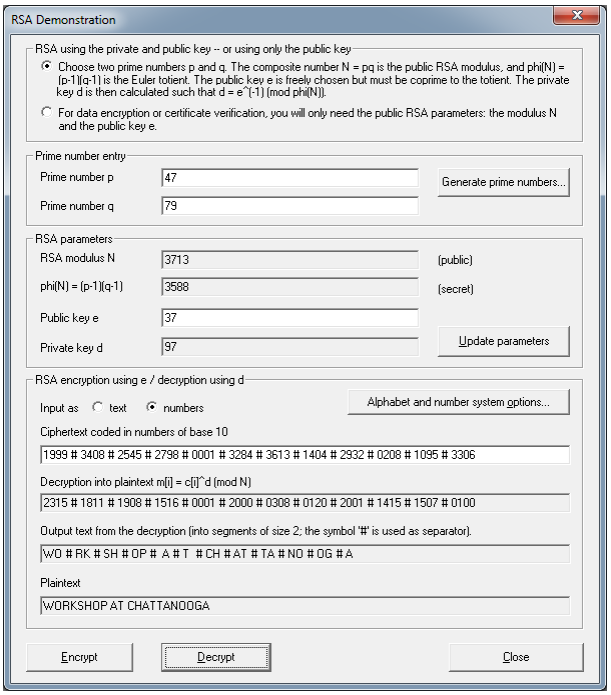
4. Choose specify alphabet under Alphabet Options and number system under Method for coding of text into number. Enter 2 in Block length in characters.



5. To confirm your entries, click on OK. You can now enter the input the text, "WORKSHOP AT CHATTANOOGA", in the input line and click on the Encrypt button.

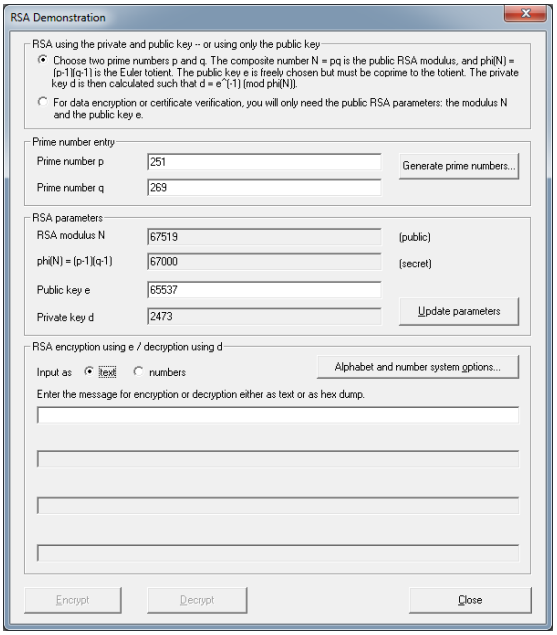
6. To decrypt, copy text in Encryption into ciphertext 1999 # 3408 # 2545 #

2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306 to input text area. And click Decrypt button.



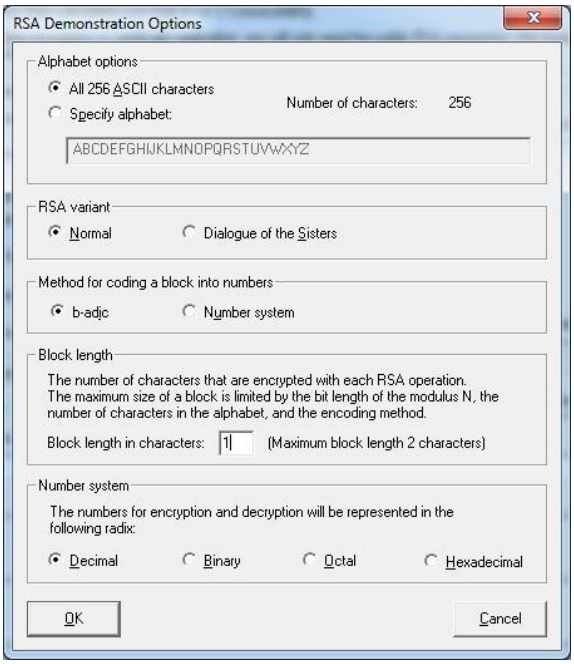
Cryptool: Encryption of the message with block length 1 v.s. encryption of the message with block length 2.

1. Create the RSA key p=251, q=269, e=65537.

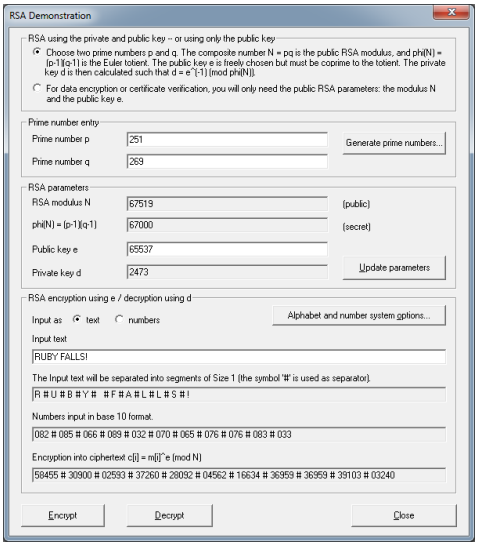


2. Click Alphabet and number system options

Choose All 256 ASCII characters under Alphabet options, b-adic under Method for coding and a block into numbers and 1 in Block length in characters.

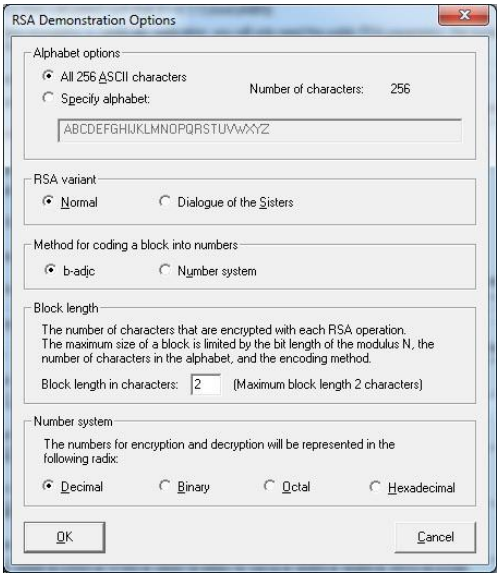


3. To confirm your entries, click on OK. You can now enter the input the text, “RUBY FALLS!”, in the input line and click on the Encrypt button.

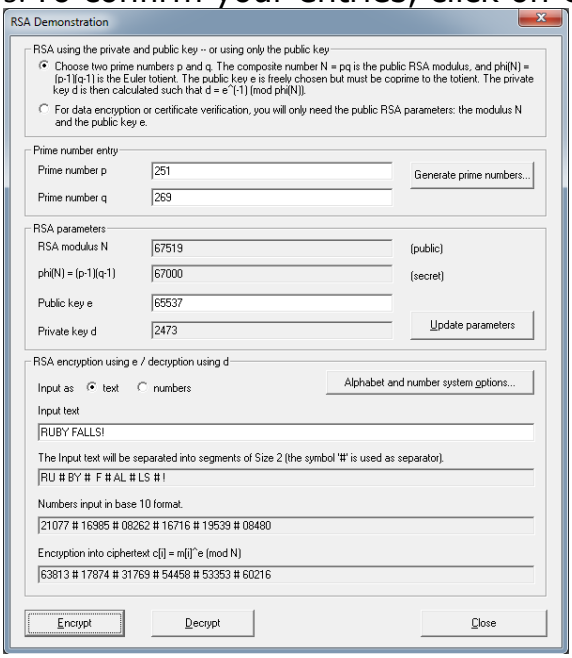


The number “#” serves here to visually split up the individual numbers. If you insert these numbers into the input line and then choose Decrypt, the original plaintext will be restored.

4. Click Alphabet and number system optionsChoose All 256 ASCII characters under Alphabet options, b-adic under Method for coding and a block into numbers and 2 in Block length in characters.



5. To confirm your entries, click on OK.



6. You will receive a cipher text that is only half as long:

Cryptool: Attack on RSA encryption with short RSA modulus

The analysis is performed in two stages: first of all the prime factorization of the RSA modulus is calculated using factorization, and then in the second

stage the secret key for encryption of the message is determined. After this, the cipher text can be decrypted with the cracked secret key.

We will figure out plaintext given

RSA modulus n = 639784868795271438588314150 41

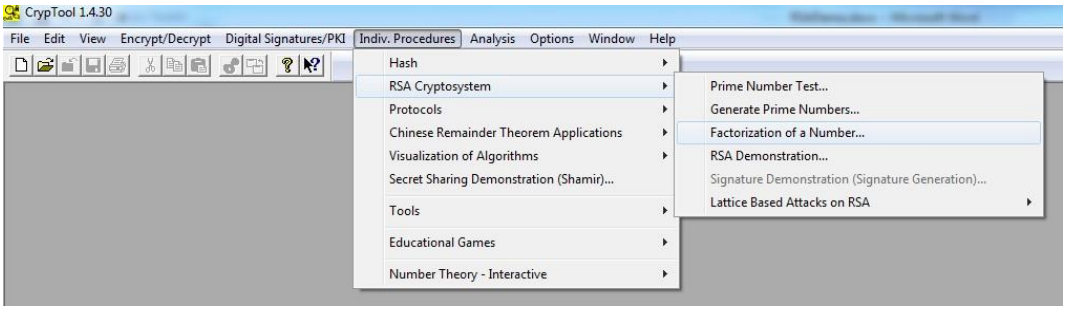
Public exponent e = 17579

Cipher text = 45411667895024938209259253423, 165970916214320200763115522 01,

4646897927975035473263763 1044, 3287016754590374133981967 1379

1. Factorization of the RSA modulus with the aid of prime factorization.

To break down the natural number, select menu sequence Indiv. Procedure/RSA Cryptosystem / Factorization of a Number.

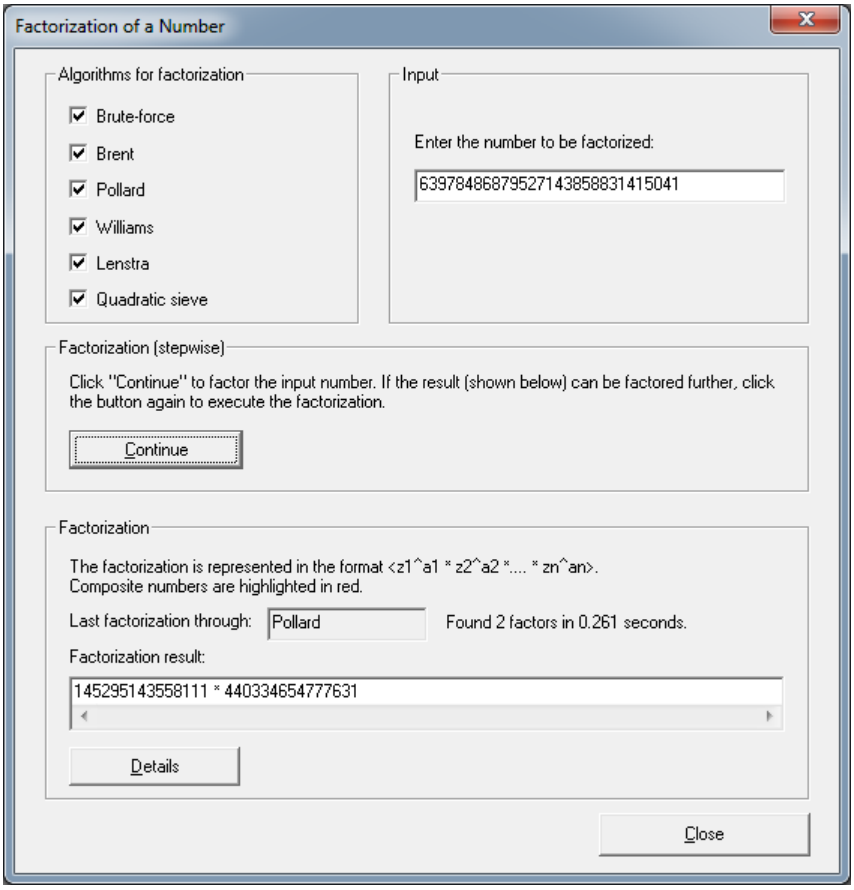


2. The two components of the public key is

RSA modulus n = 639784868795271438588314150 41

Public exponent e = 17579

Enter n=639784868795271438588314150 41 as input and click Continue.



It is interesting to see which procedure broke down the RSA modulus the fastest.

2. Calculate the secret key d from the prime factorization of n and the public key e:

With the knowledge of the prime factors p = 145295143558111 and q = 440334654777631 and the public key e = 17579, we are in a position to decrypt the ciphertext.

3. Open the next dialog box via menu selection Indiv. Procedure/RSA Cryptosystem/RSA Demonstration:.

4. Enter p = 145295143558111 and q = 440334654777631 and the public key e = 17579.

5.Click on Alphabet and number system options and make the following settings:

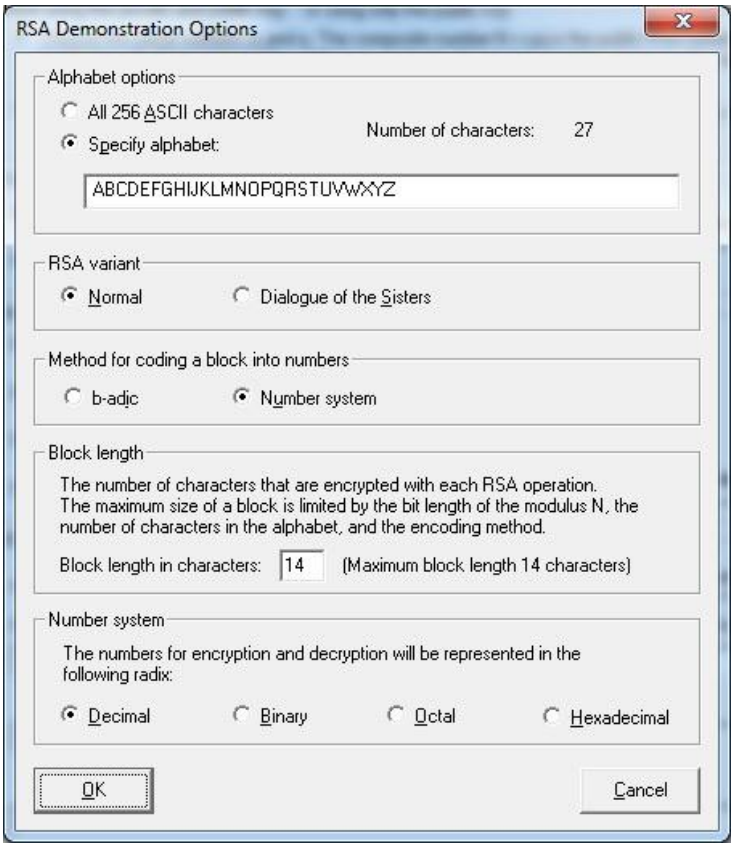
Alphabet options: Specify alphabet

RSA variant: Normal

Method for coding a block into number: Number system

Block length: 14

Number system: Decimal



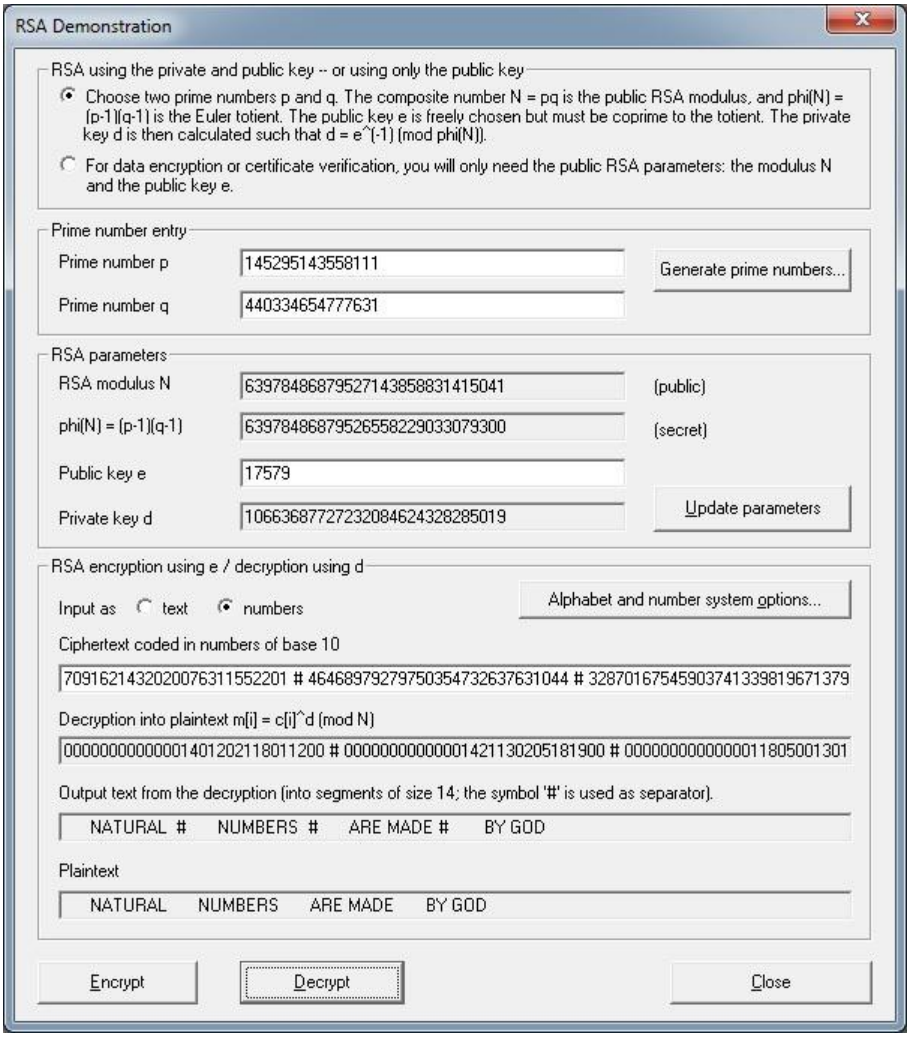
5. Enter the following cipher text in the input text field. And click Decrypt button.

45411667895024938209259253423,

16597091621432020076311552201,

46468979279750354732637631044,

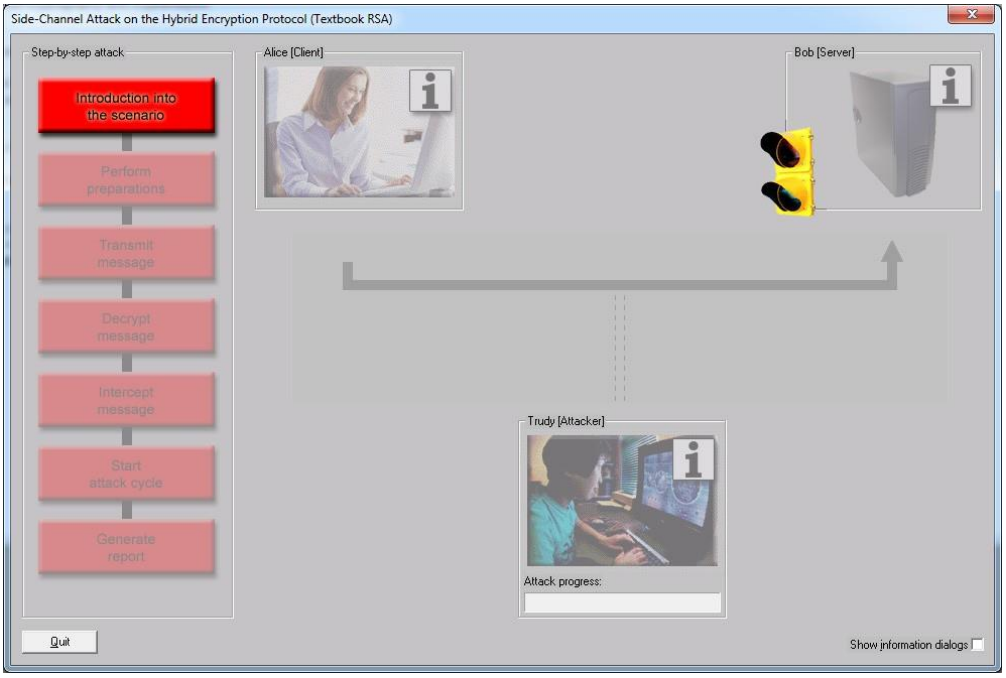
32870167545903741339819671379



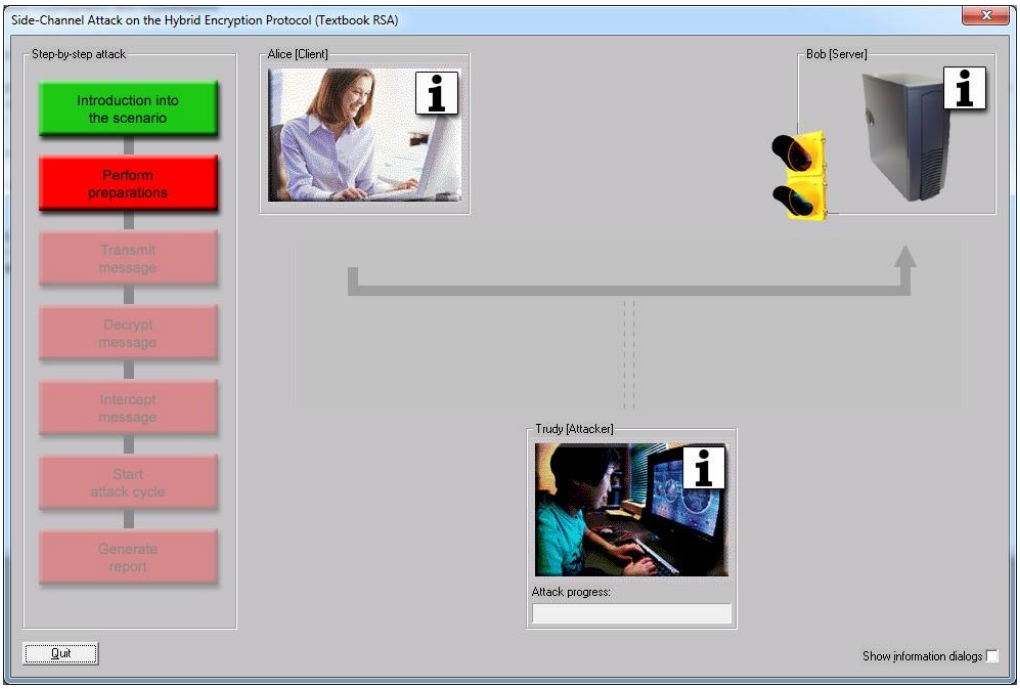
Check your results: “NATURAL NUMBERS ARE MADE BY GOD”

Side Channel Attack to RSA:

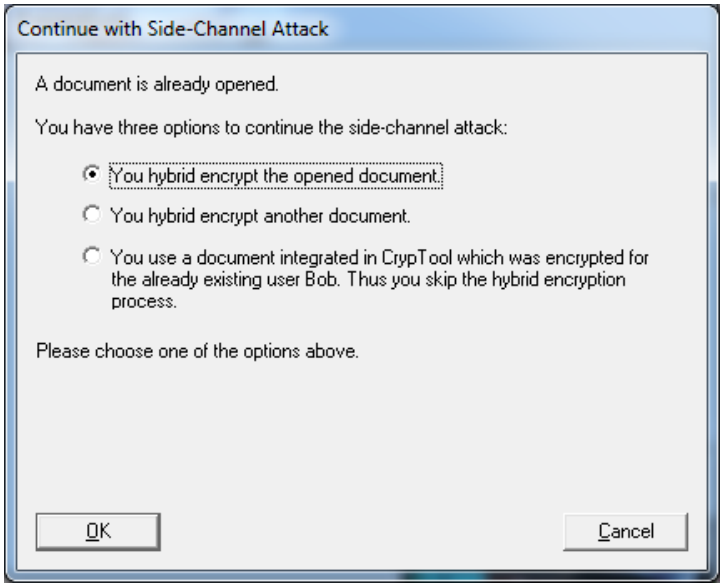
Select from menu: “Analysis” \“Asymmetric Encryption” \“Side-Channel Attack on Textbook RSA”



Click “Introduction to the scenario”.

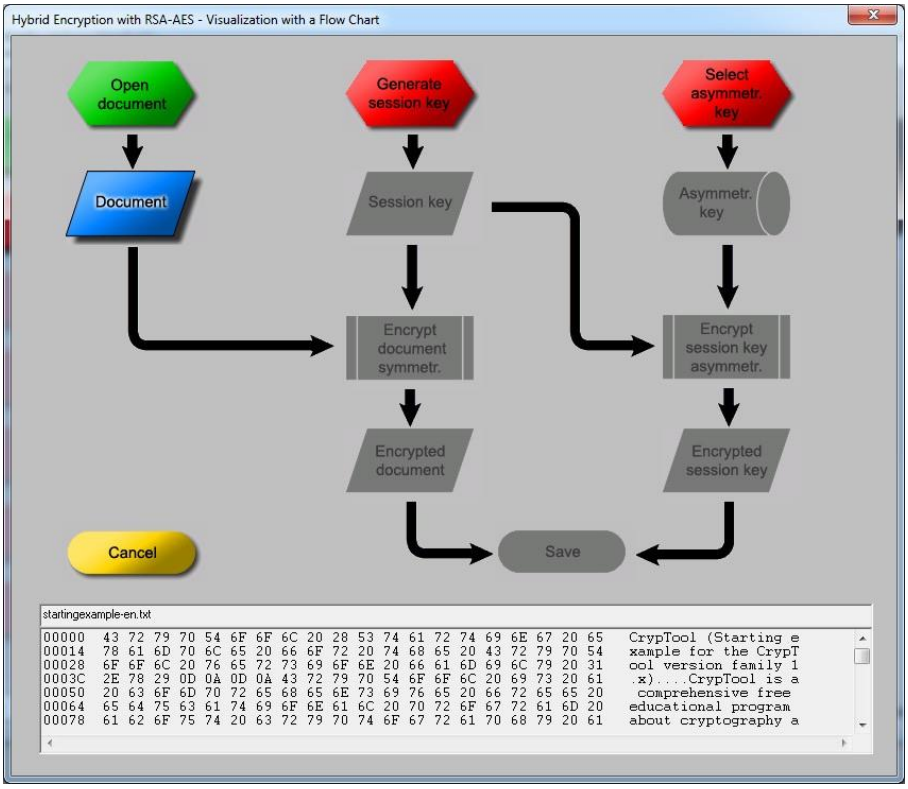


Click “Perform preparation” and click “OK”

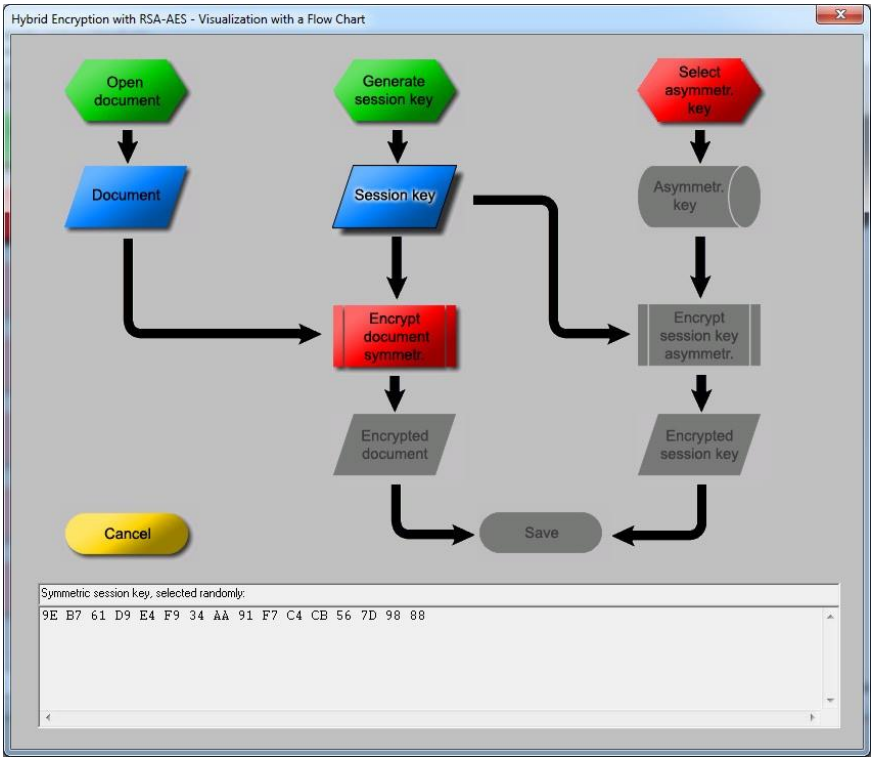


Click “OK” again.

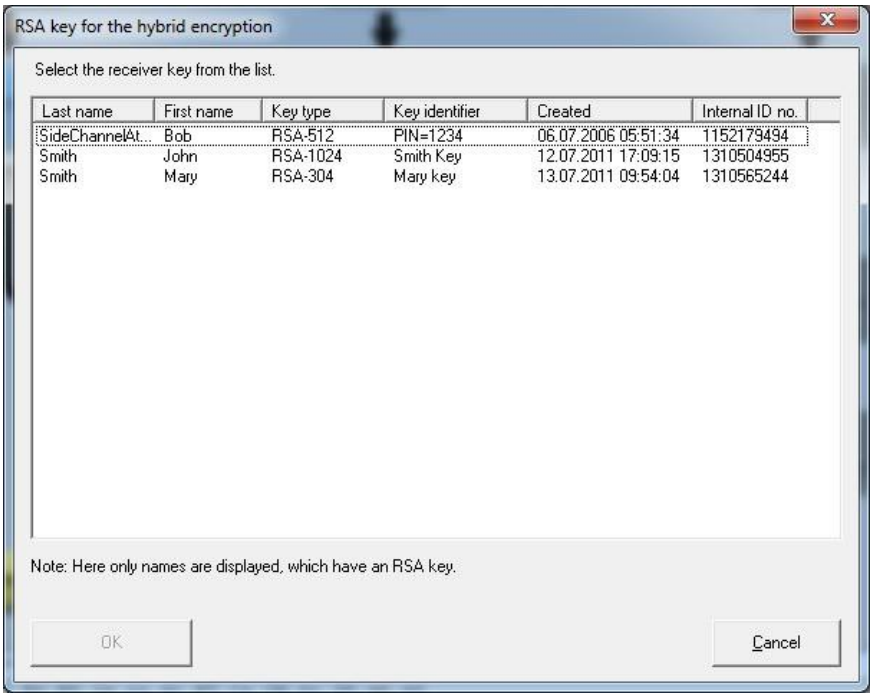
Hybrid cryptosystem see https://en.wikipedia.org/wiki/Hybrid_cryptosystem



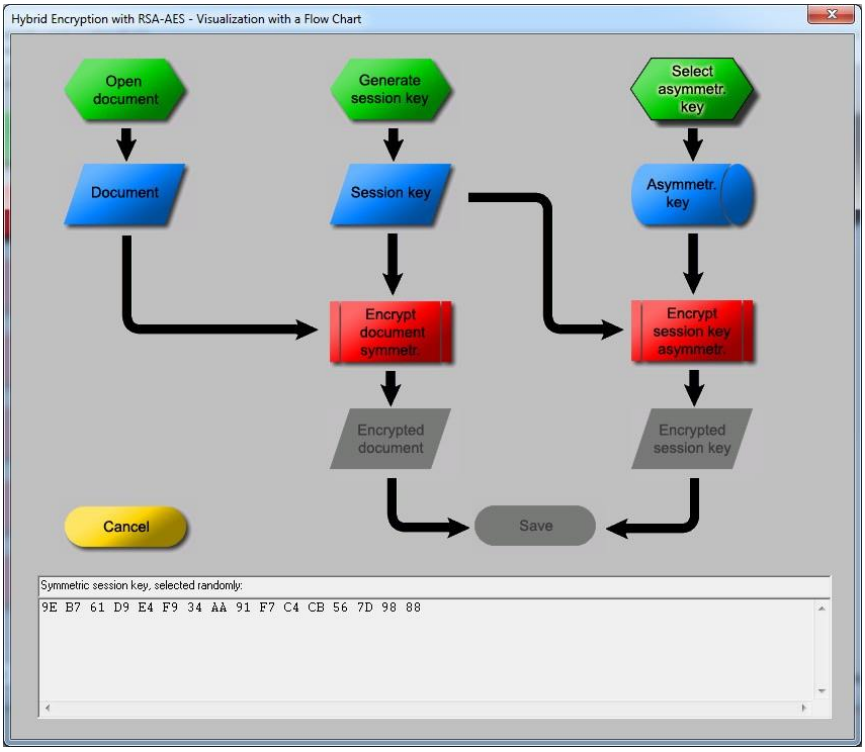
Click “Generate session key” and “Session Key”. The generated session key is e.g. “9E B7 61 D9 E4 F9 34 AA 91 F7 C4 CB 56 7D 98 88”. You may obtain different key!



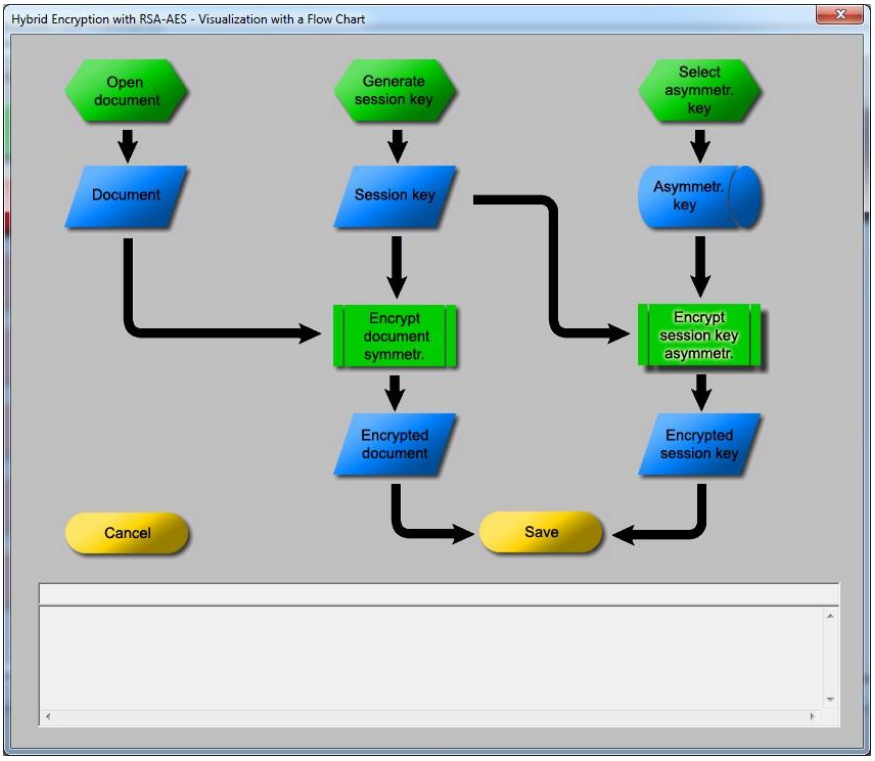
Click “Select asymmetr. key”.



Select Bob’s key and click “OK”.

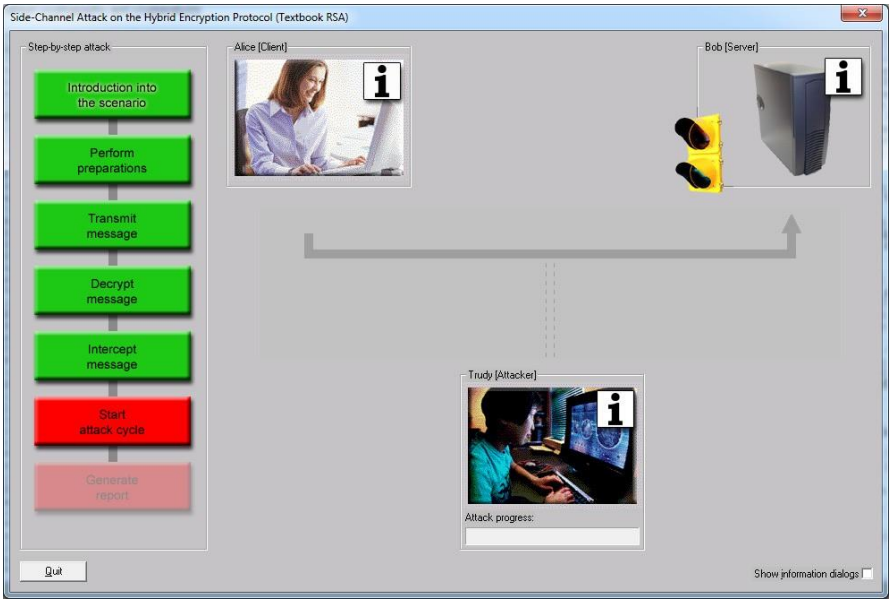


Click “Encrypt document symmetry.”, “Encrypt session key asymmetry.” and “Save”.

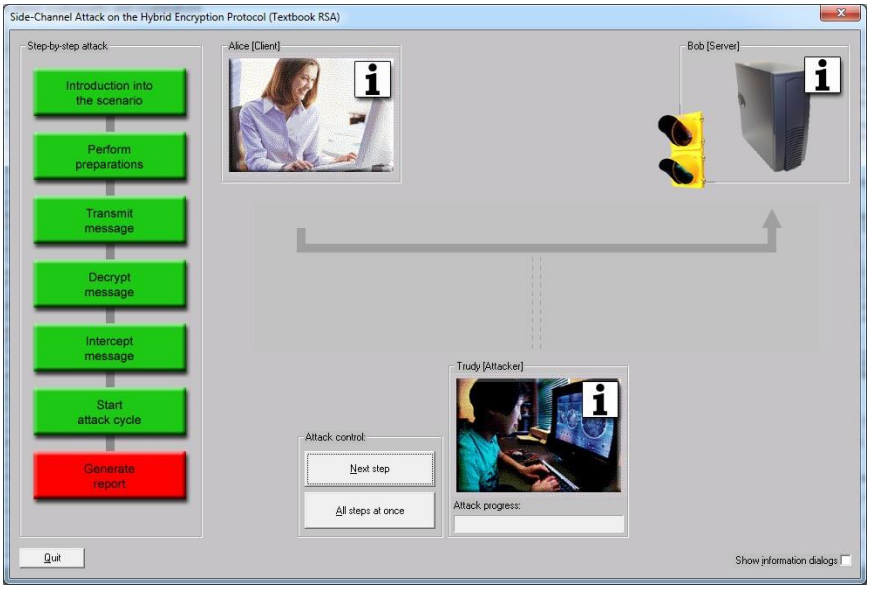


Click “Transmit message” and “Decrypt message”.

Enter 1234 and click “OK”.

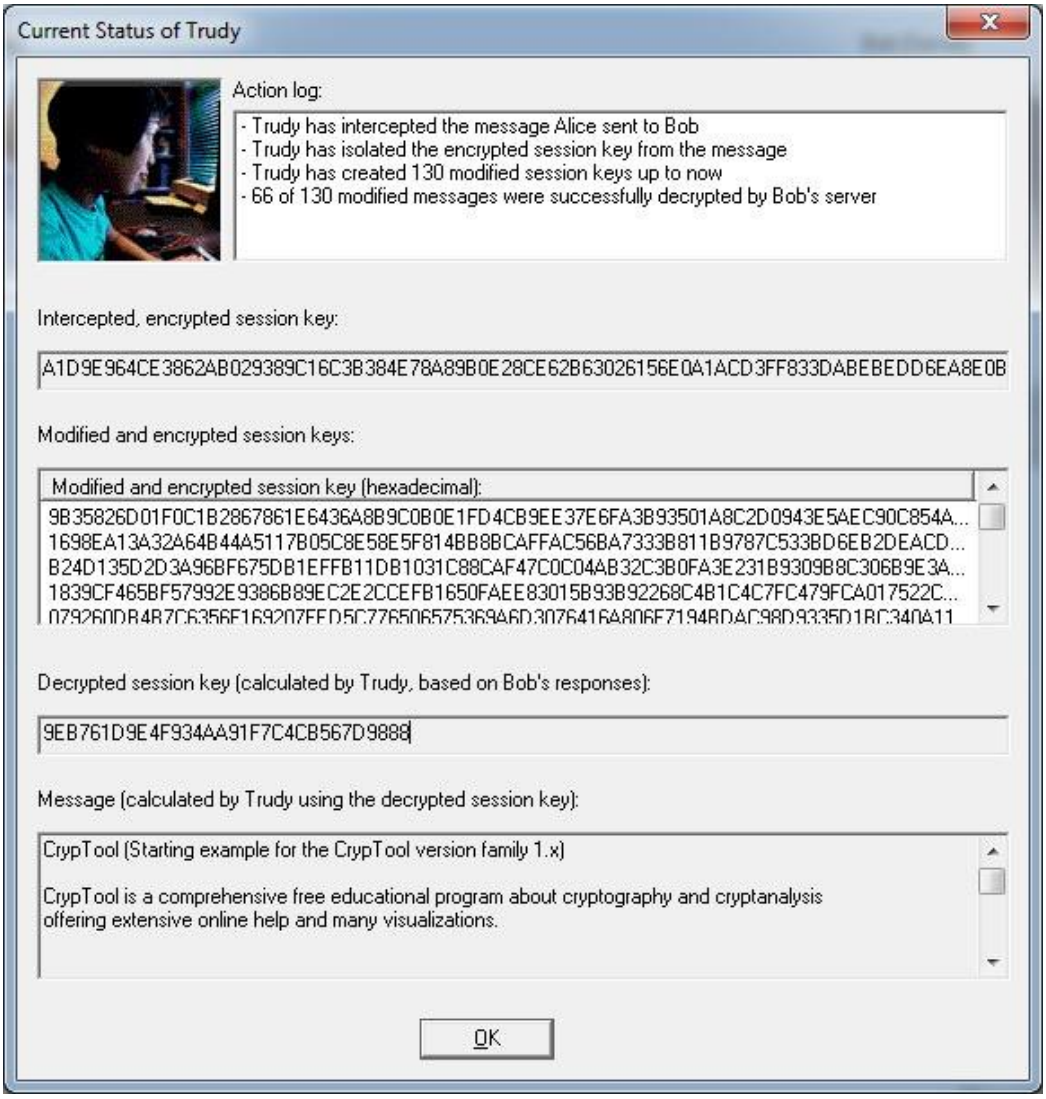


Click “Intercept message” and “Start attack cycle”.



Click “All steps at once” button.

Click “OK” and icon of Trudy (Attacker).



The session key is 9EB761D9E4F934AA91F7C4CB567D9888 which matches the one generated in Step 5.