Assignment6

Lab on Short Message RSA Attacks and Padding (100 points)

In **short message attack of RSA**, if it is known that Alice is sending a four-digit number to Bob, Eve can easily try plaintext numbers from 0000 to 9999 to find the plaintext. Therefore, short message must be padded with random bits. **If you are Eve, show that you are able to find the plaintext containing four digit numbers given ciphertext.**

Optimal asymmetric encryption padding (OAEP) is recommended when short messages are encrypted with RSA algorithms. The following is the encryption and decryption processes of OAEP.

- Encryption
  - Pad the message to make m-bit message M, if M is less than m-bit
  - Choose a random number r
  - User one-way function G that inputs r-bit integer and outputs m-bit integer. This is the mask.
  - P1 = M ⊕ G®
  - P2 = H(P1) ⊕ r, function H inputs m-bit and outputs k-bit
  - C = E(P1 || P2). User RSA encryption here
- Decryption
  - P = D (P1 || P2)
  - Bob first recreates the value of r:

    H(P1) ⊕ P2 = H(P1) ⊕ H(P1) ⊕ r = r

  - Bob recreates msg:

    G(r) ⊕ P1 = G(r) ⊕ G(r) ⊕ M = M

Pad your message with OAEP padding and then encrypt by RSA.

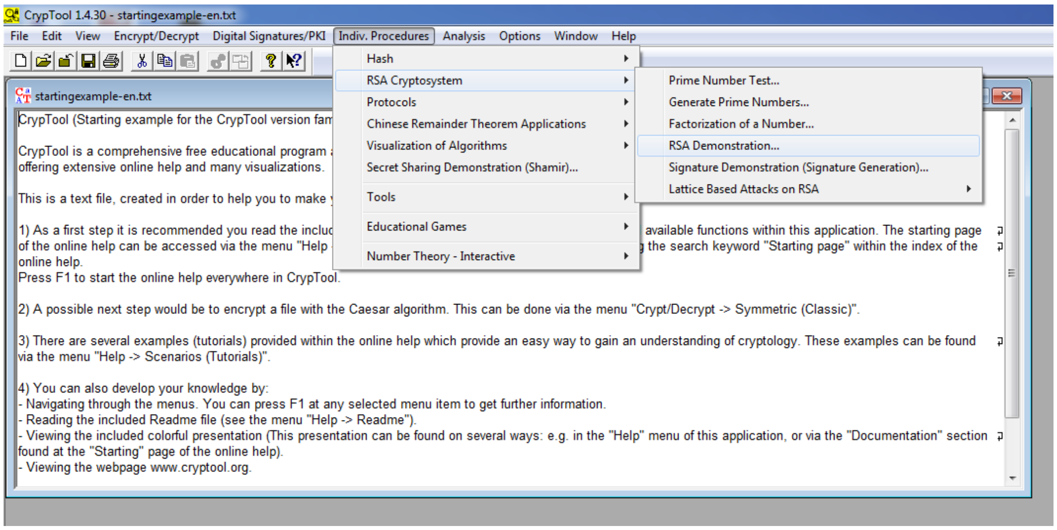
What to submit:

A report describes how you find the unpadded short plaintext (30 points), describes what you have observed after you apply OAEP padding (30 points), and discusses feasibility of short message attack after padding (10 points).

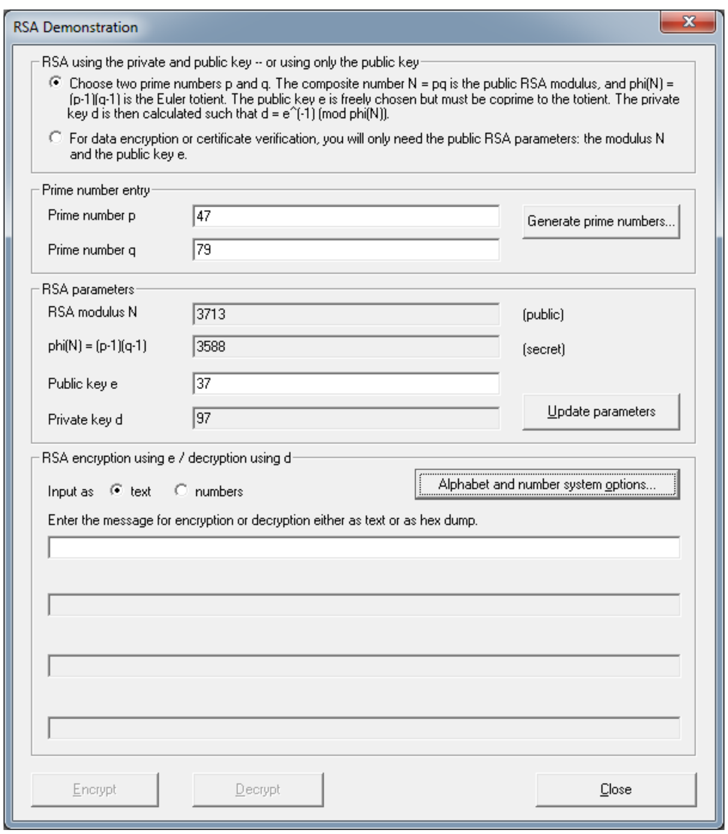
Lab on RSA Encryption and Factorization Attacks (practice)

Encryption or decryption of messages using the RSA key pair.

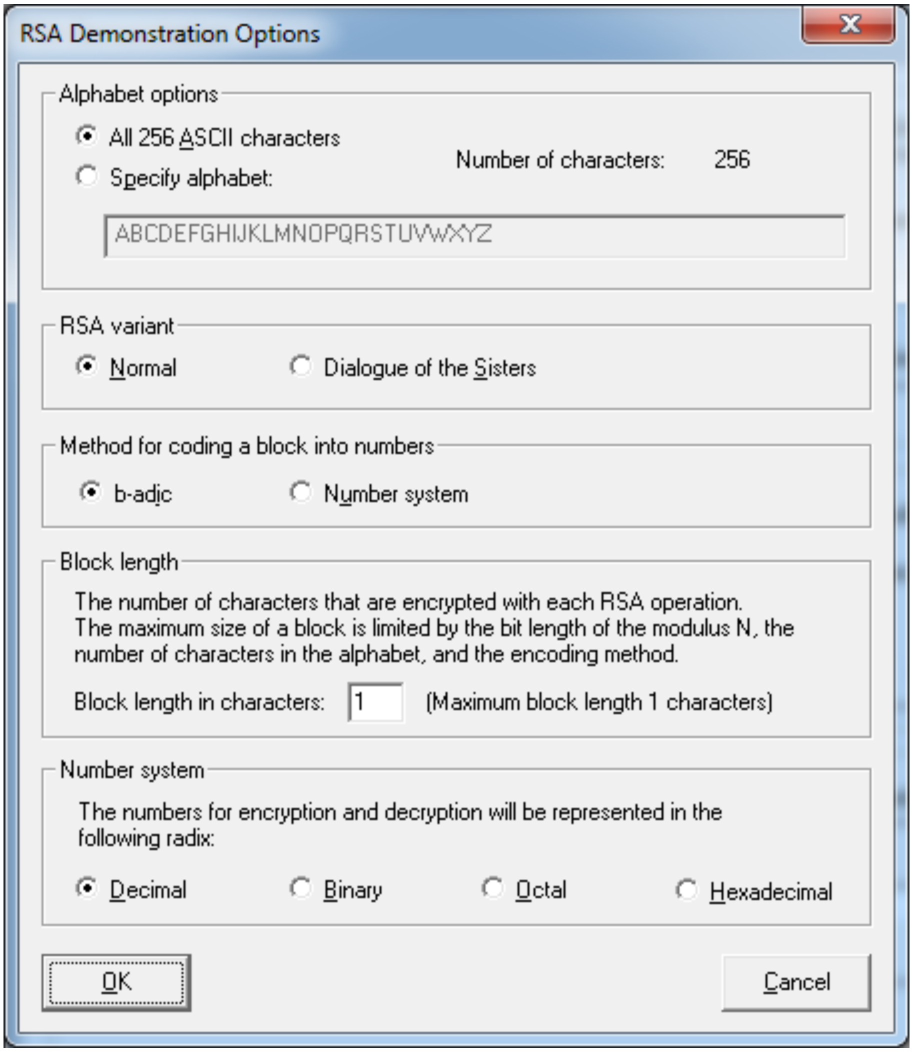
1. Select **Individual Procedures/RSA Cryptosystem/RSA Demonstration**



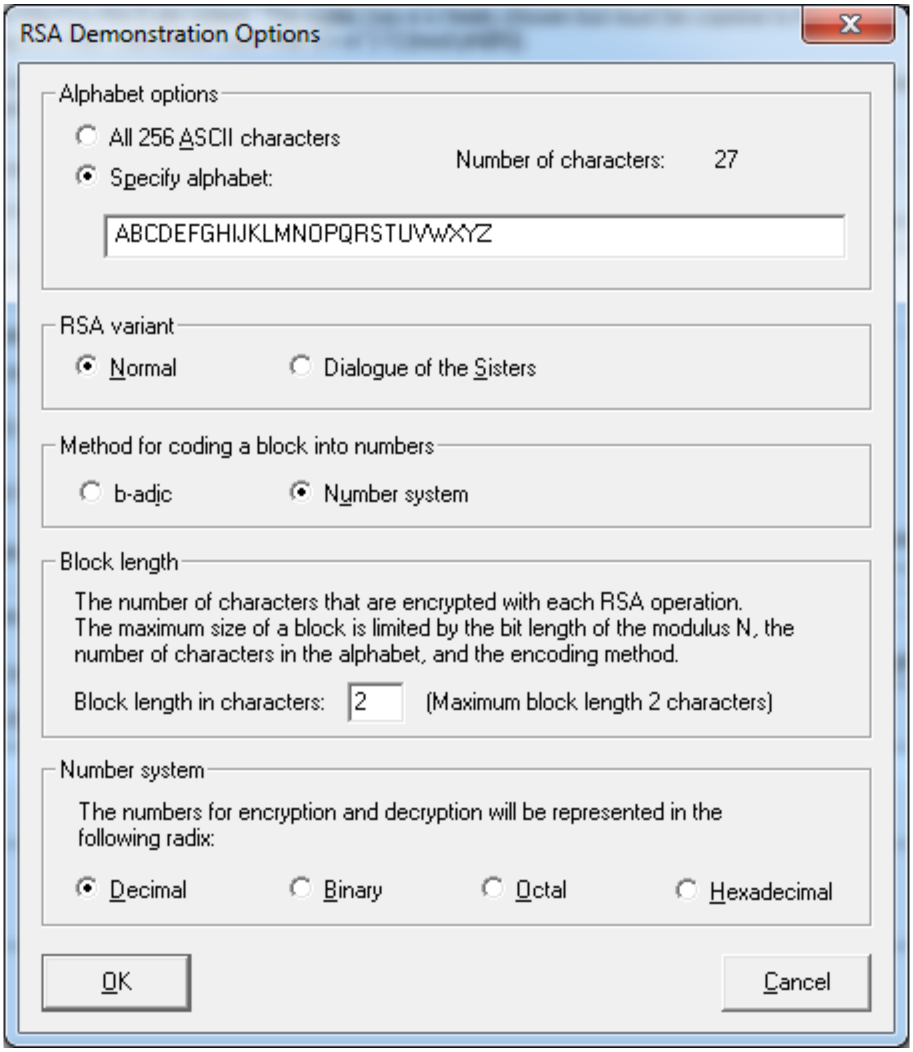
2. Enter the RSA key **p=47, q=79, e=37**. The parameters N = p*q=3713 and phi(N)=3588 and d=97 are calculated.



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.

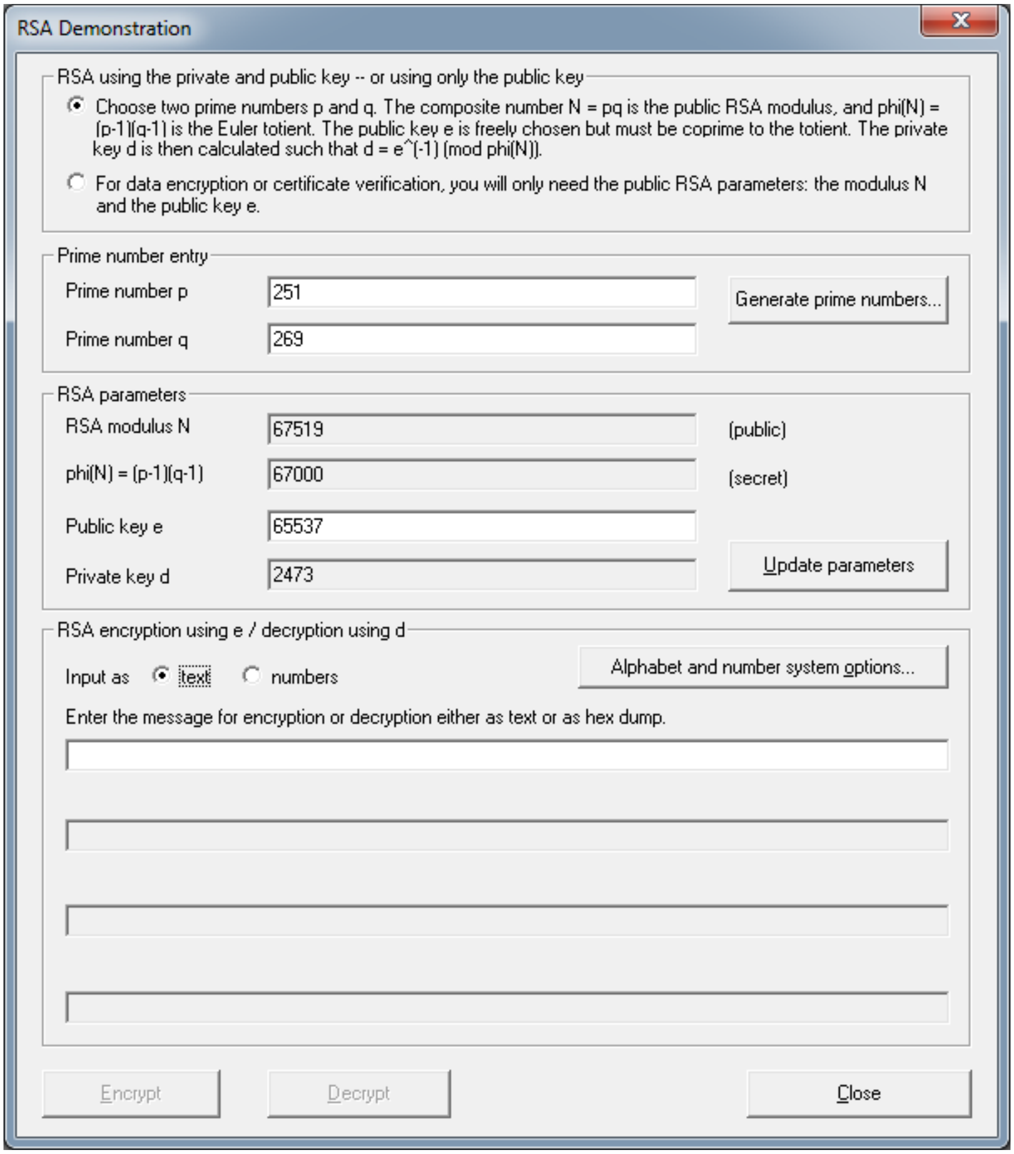


5. To confirm your entries, click on OK. You can now enter the input the text, "**WORKSHOP AT CHATTANOOGA**", in the input line and click on the **Encrypt** button.

6. To decrypt, copy text in <u>Encryption into ciphertext</u> **1999 # 3408 # 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 #** 3306 to <u>input text</u> area. And click **Decrypt** button.

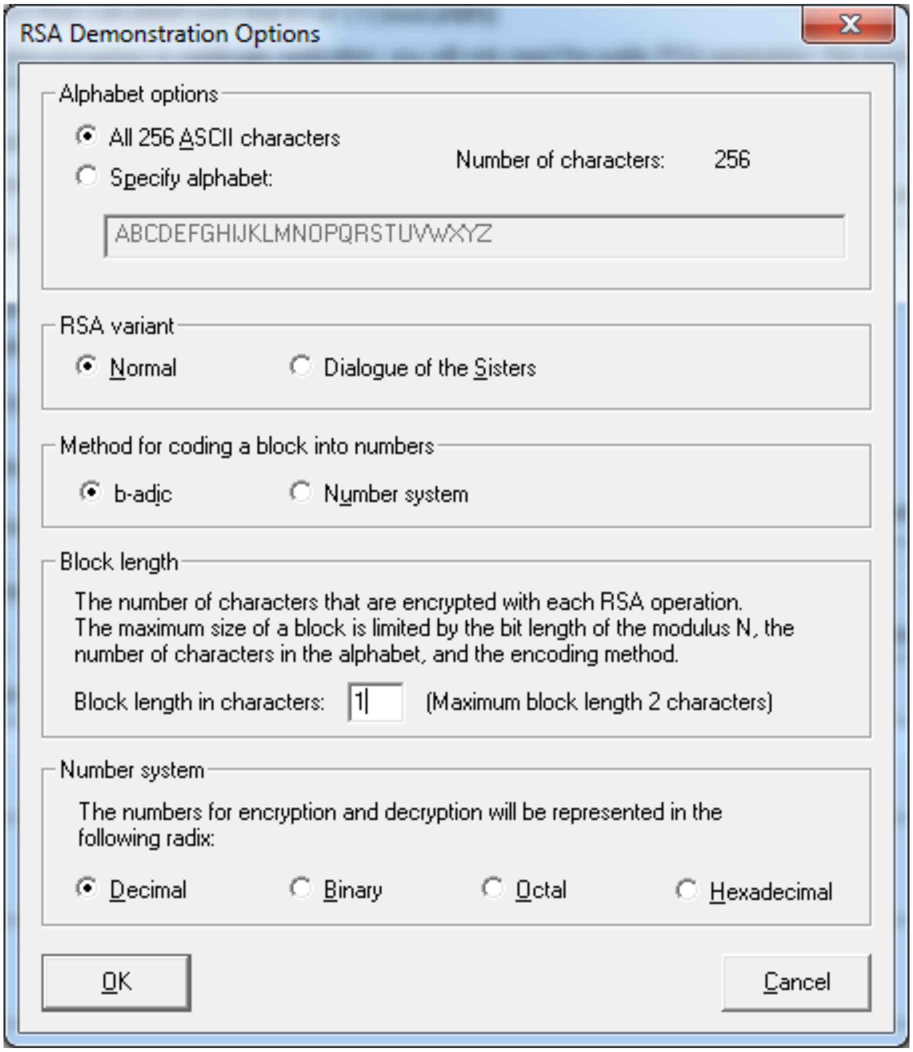
Encryption of the message with block length 1 v.s. encryption of the message with block length 2.

1. Create the RSA key p=251, q=269, e=65537. The value of N is ______________, the value of phi(N) is__ ______________, the value of private key d is__________.

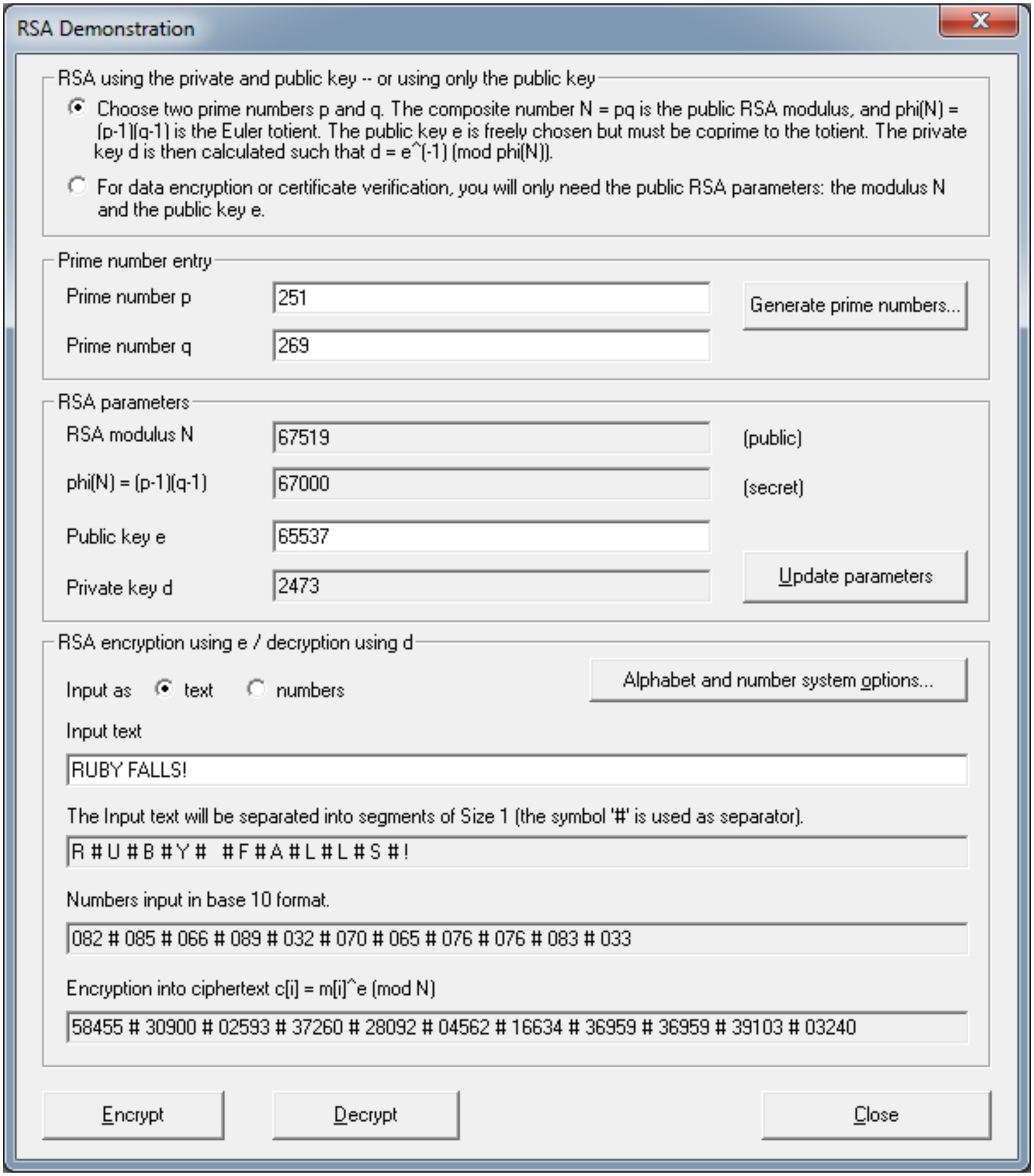


2. Click **Alphabet and number system options**

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



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.



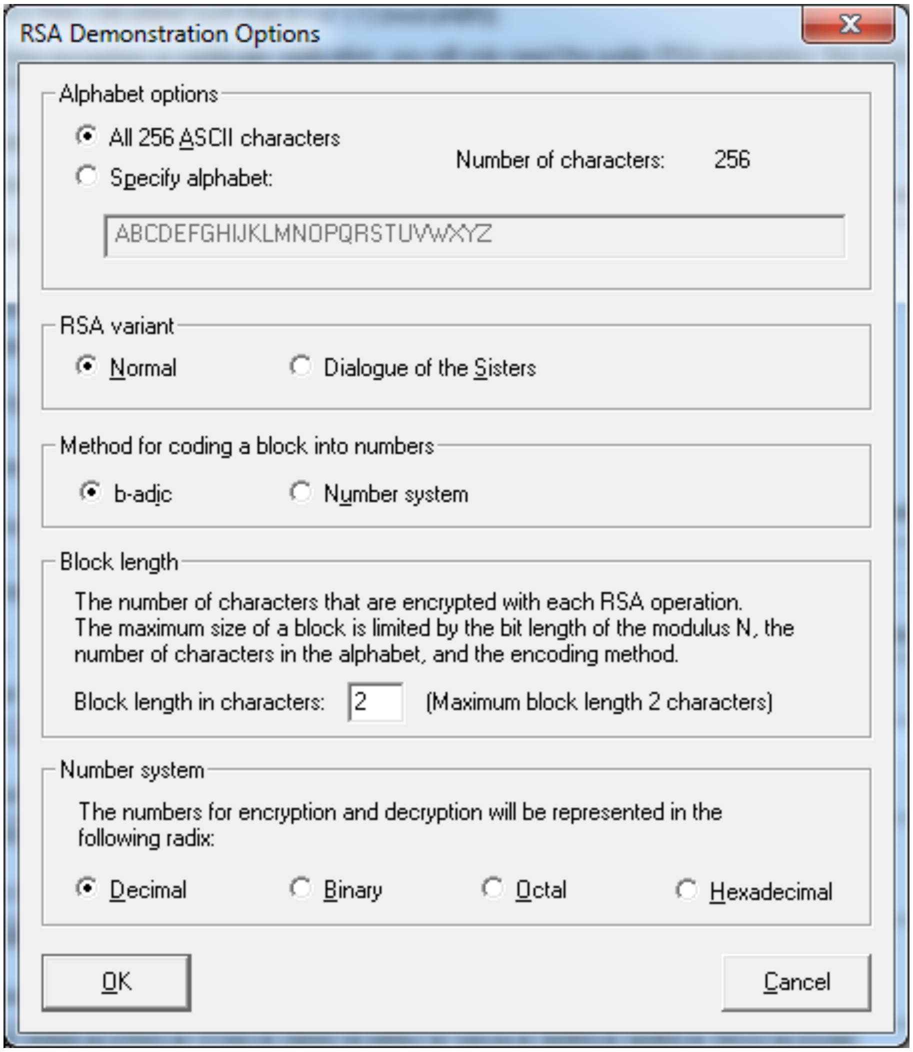
The encrypted version of this is the number sequence is ____

____

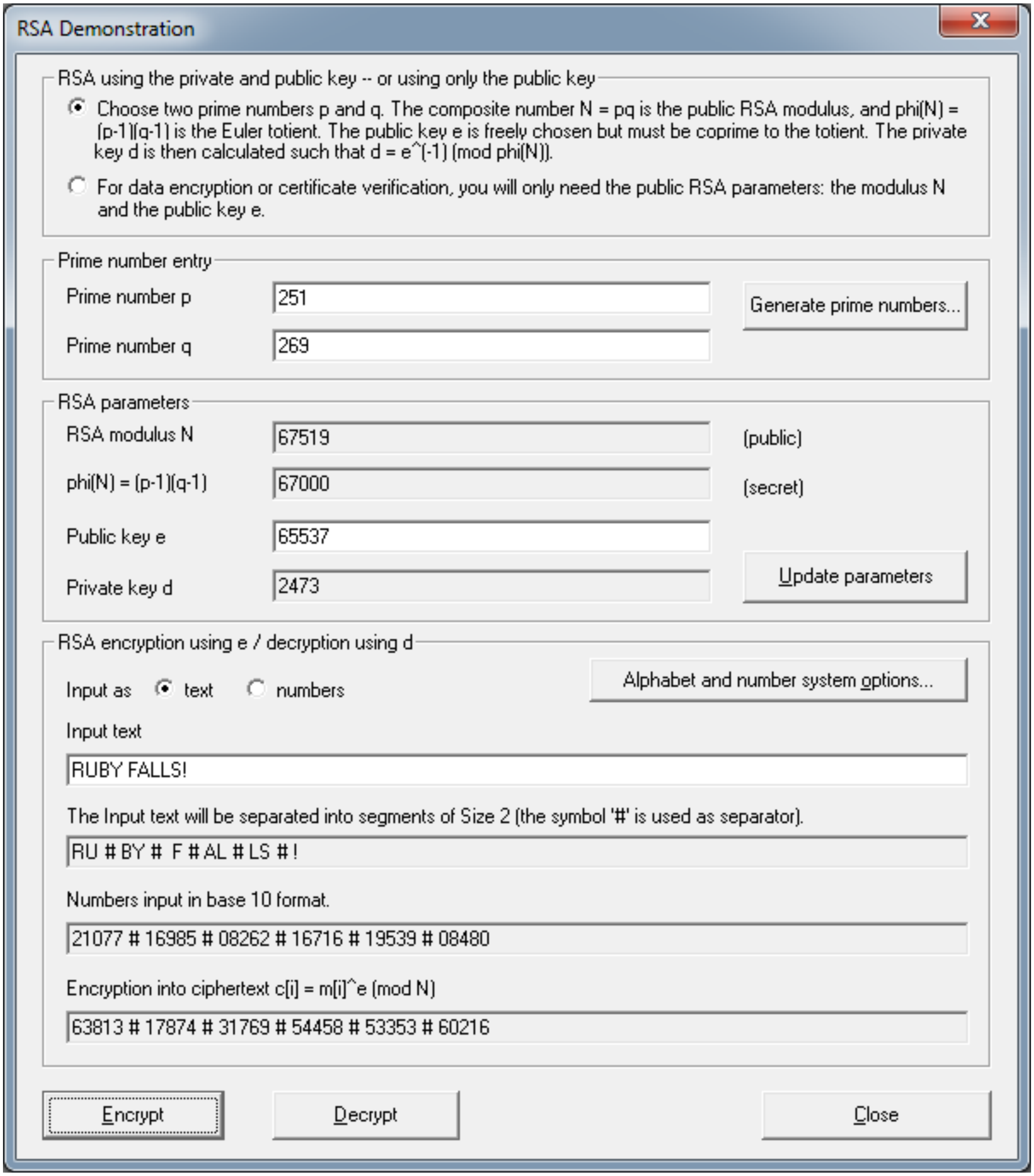
The number "#" serves here to visually split up the individual numbers. If you insert these numbers into the input line and then choose **Decrypt**, the original plaintext will be restored.

4. Click **Alphabet and number system options**

Choose **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:

Attack on RSA encryption with short RSA modulus (practice)

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

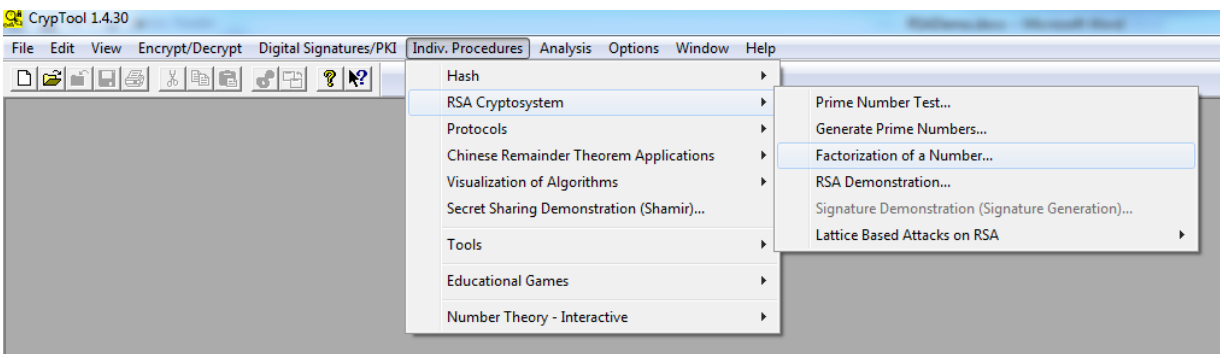
RSA modulus n = 63978486879527143858831415041

Public exponent e = 17579

Cipher text = 45411667895024938209259253423, 16597091621432020076311552201, 46468979279750354732637631044, 32870167545903741339819671379

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**.

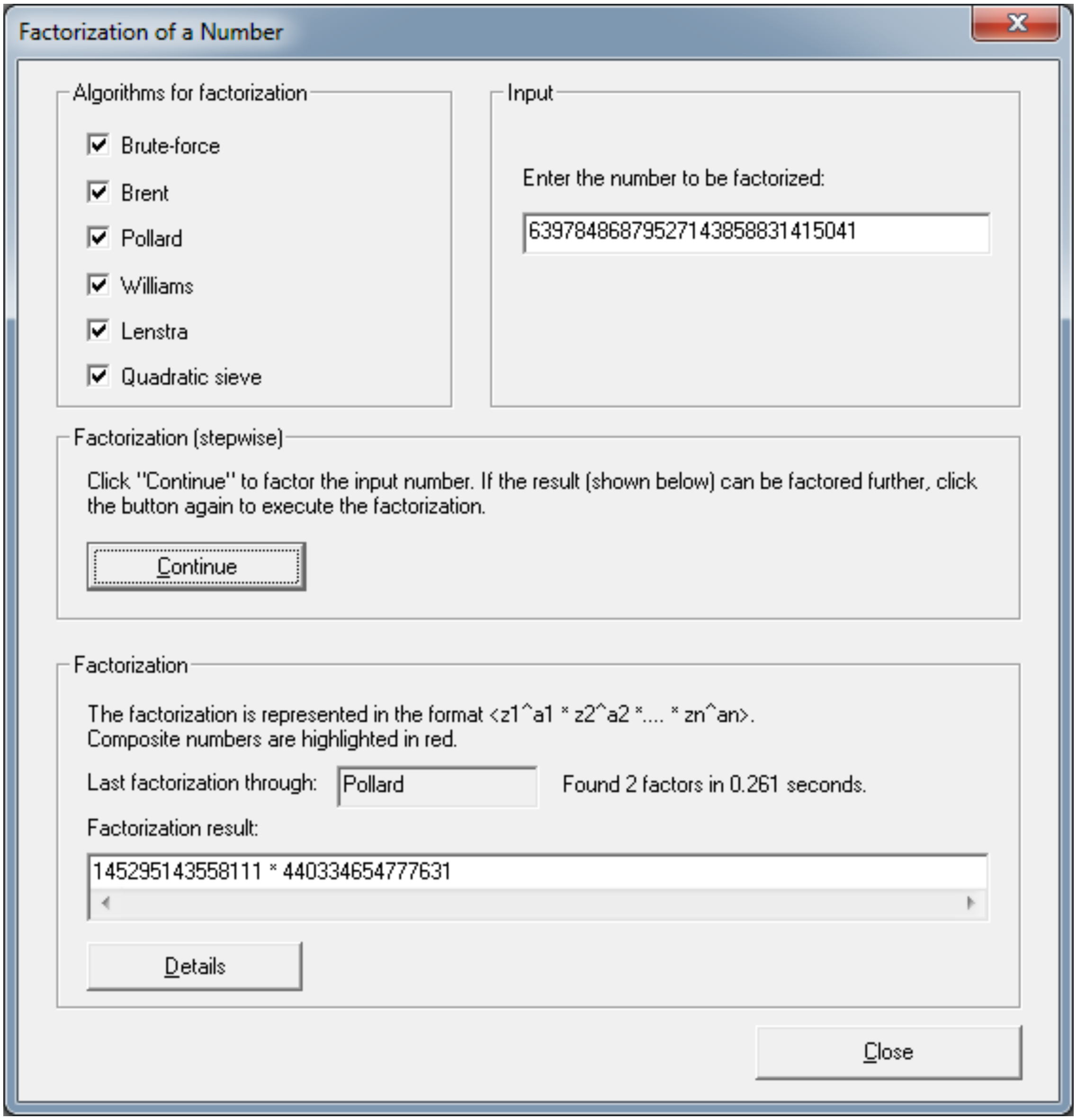


2. The two components of the public key is

RSA modulus n = 63978486879527143858831415041

Public exponent e = 17579

Enter n=**63978486879527143858831415041** 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:

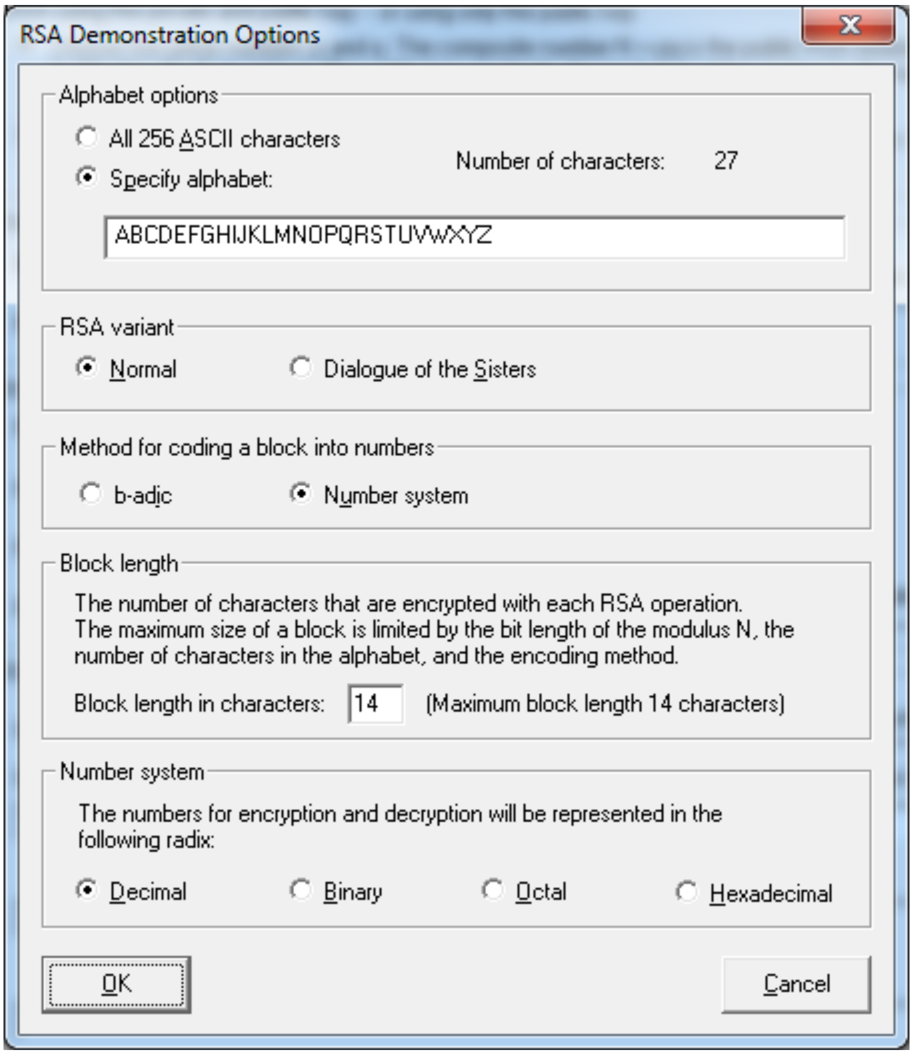
Alphabet options: **Specify alphabet**

RSA variant: **Normal**

Method for coding a block into number: **Number system**

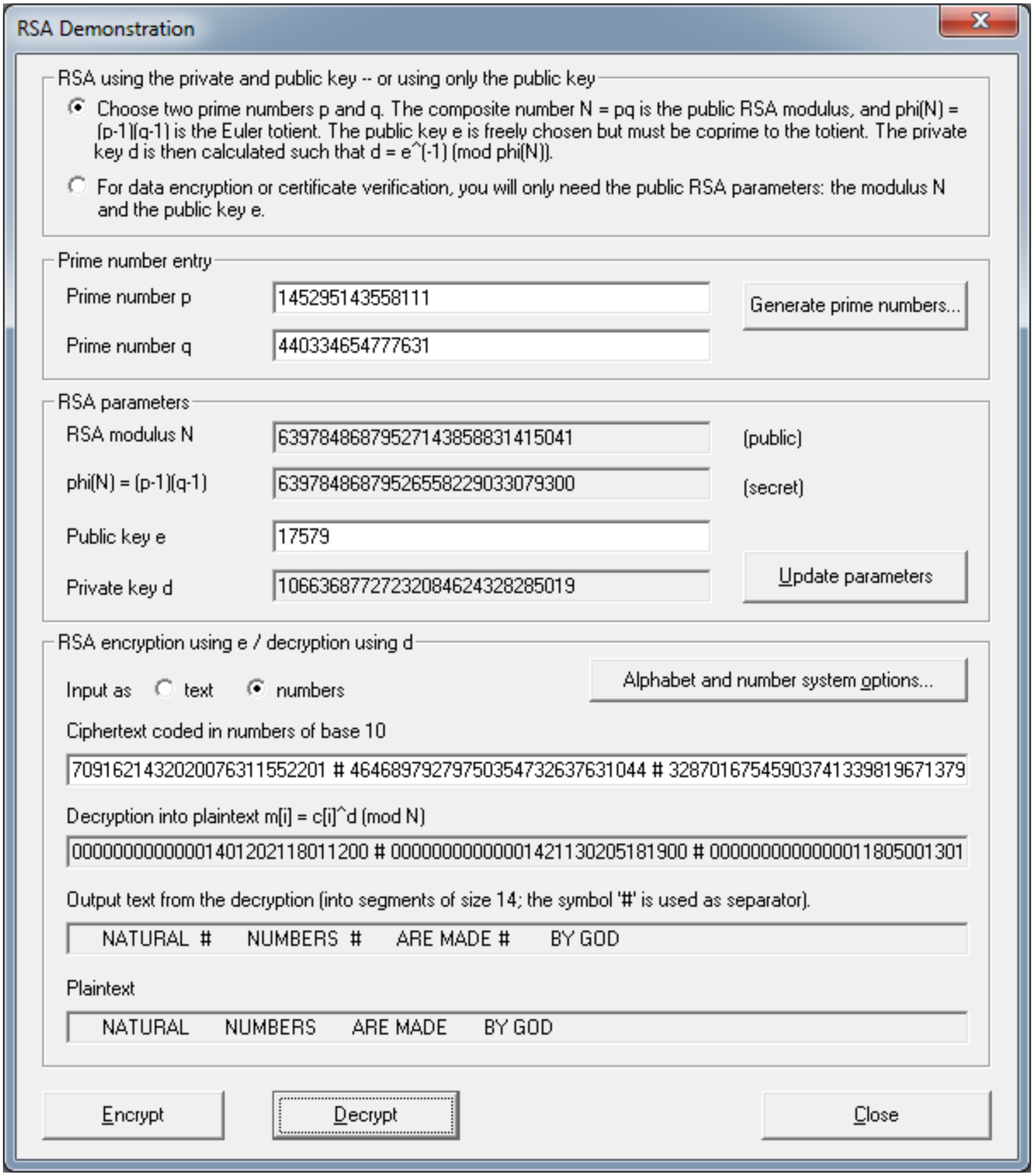
Block length: **14**

Number system: **Decimal**



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

45411667895024938209259253423,
16597091621432020076311552201,
46468979279750354732637631044,
32870167545903741339819671379

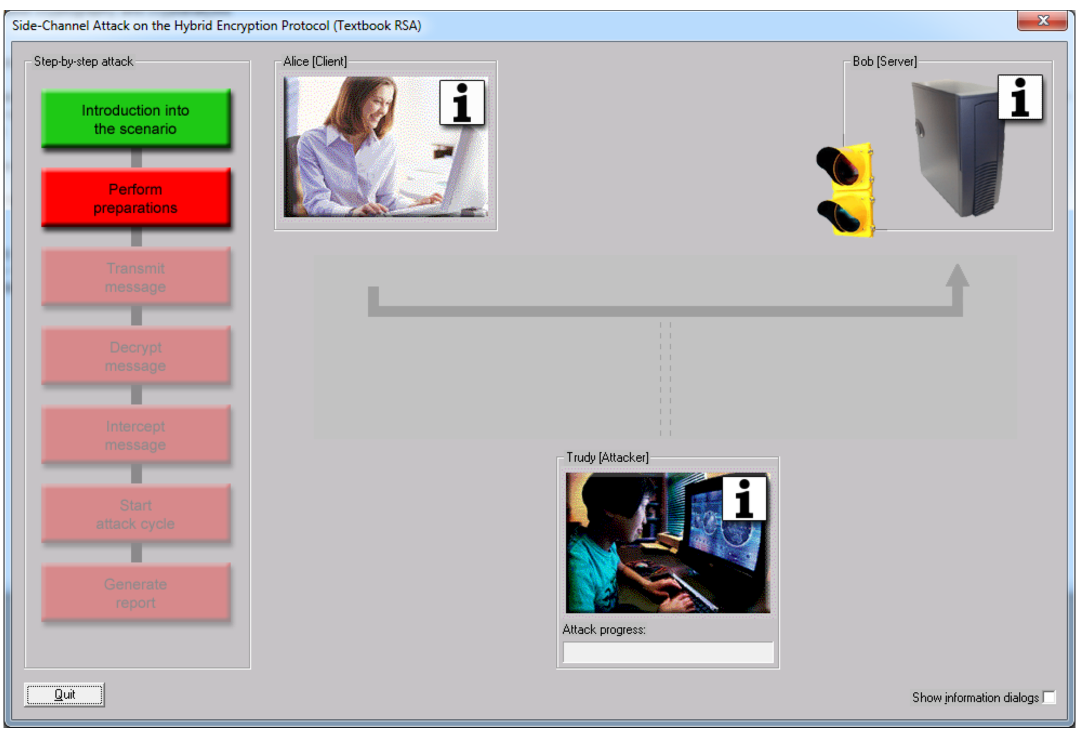


Check your results: “**NATURAL NUMBERS ARE MADE BY GOD**”

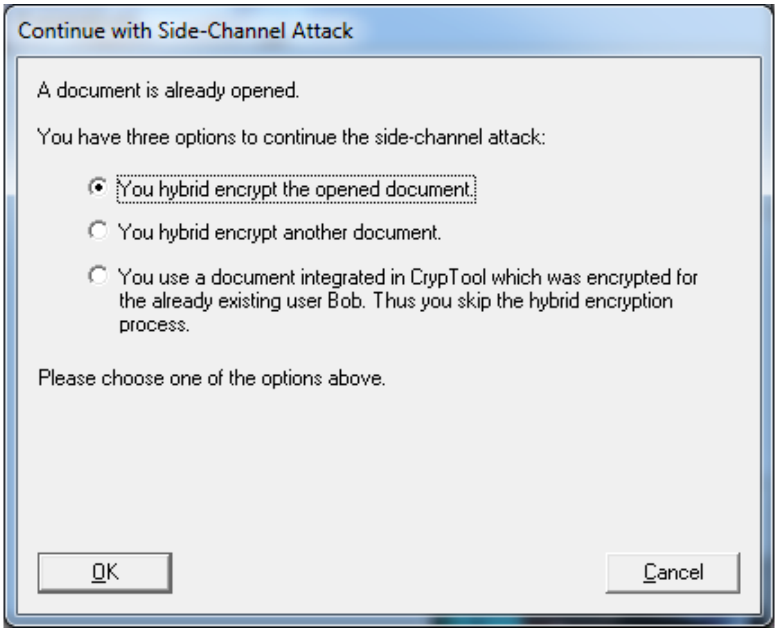
Side Channel Attack to RSA: (10 points)

1. Select from menu: "**Analysis" \"Asymmetric Encryption" \"Side-Channel Attack on Textbook RSA**"

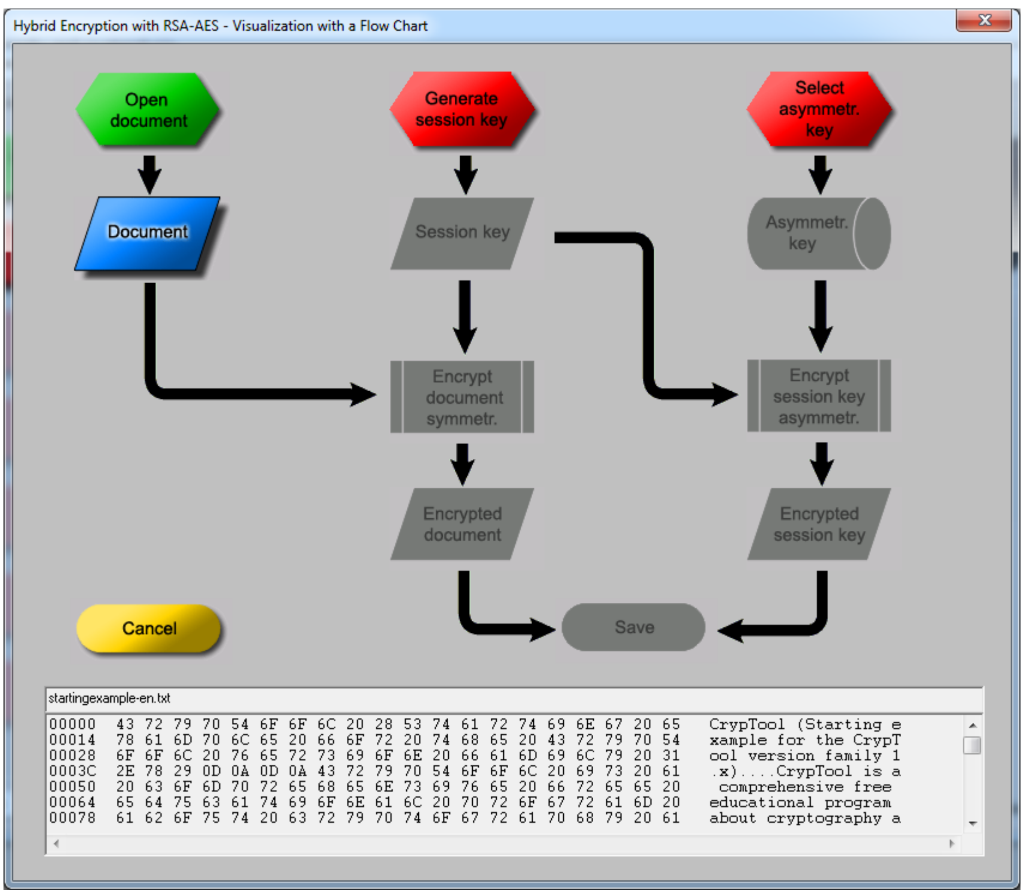
2. Click "**Introduction to the scenario**".



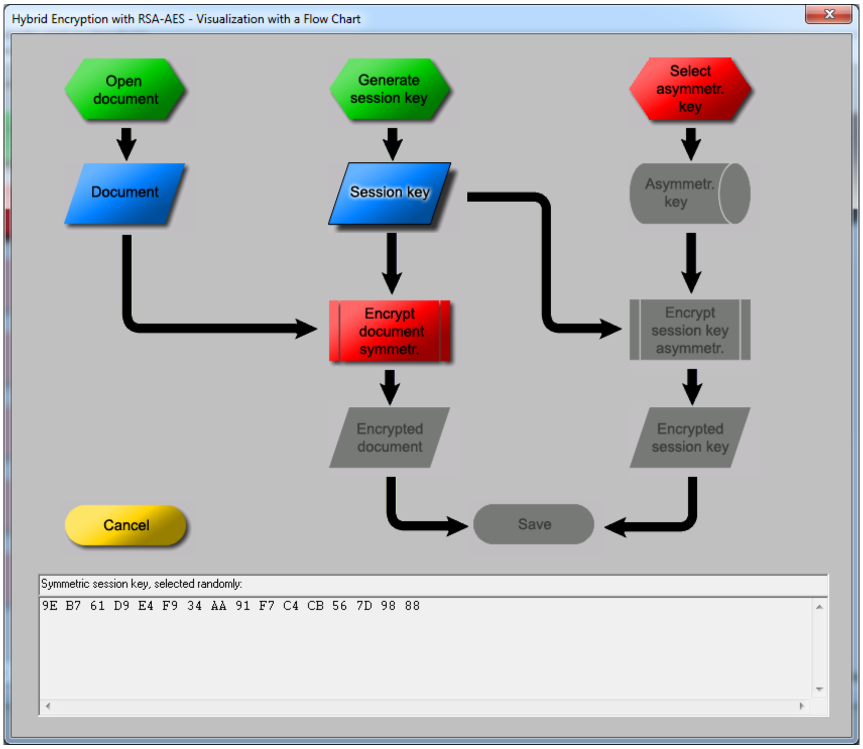
3. Click “**Perform preparation**” and click “**OK**”



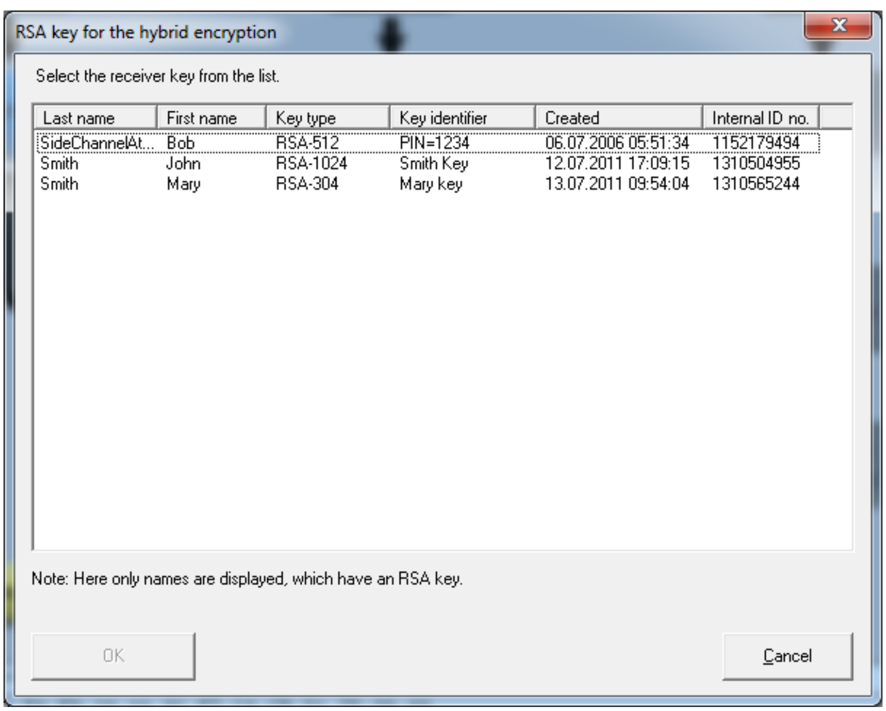
4. Click “**OK**” again.



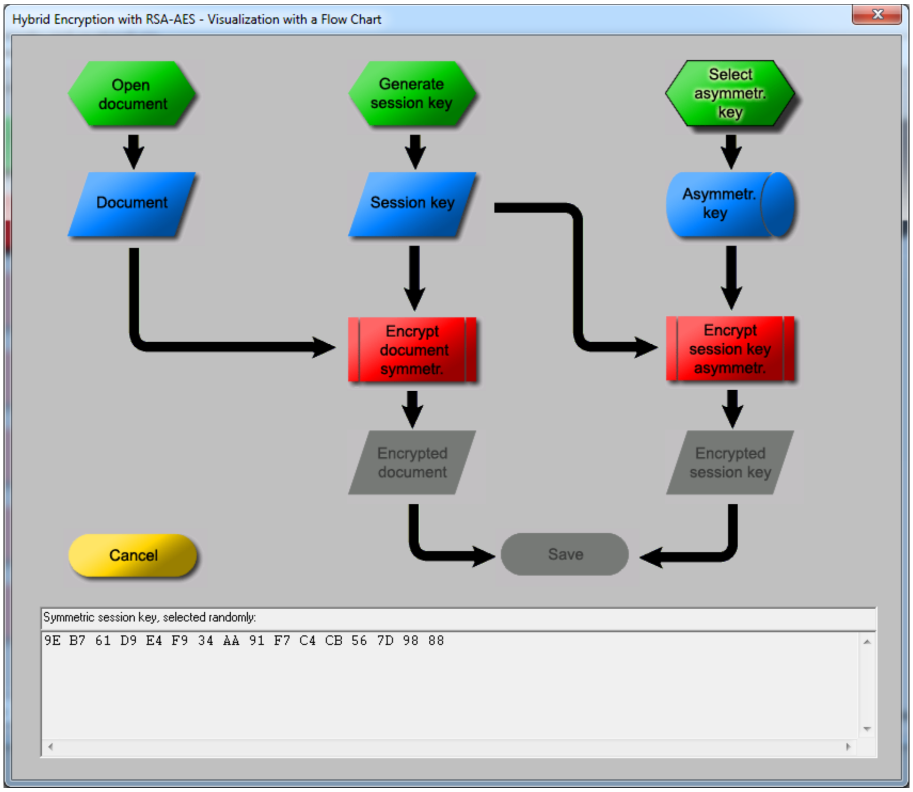
5. Click “**Generate session key**” and “**Session Key**”. The generated session key is “9E B7 61 D9 E4 F9 34 AA 91 F7 C4 CB 56 7D 98 88”.



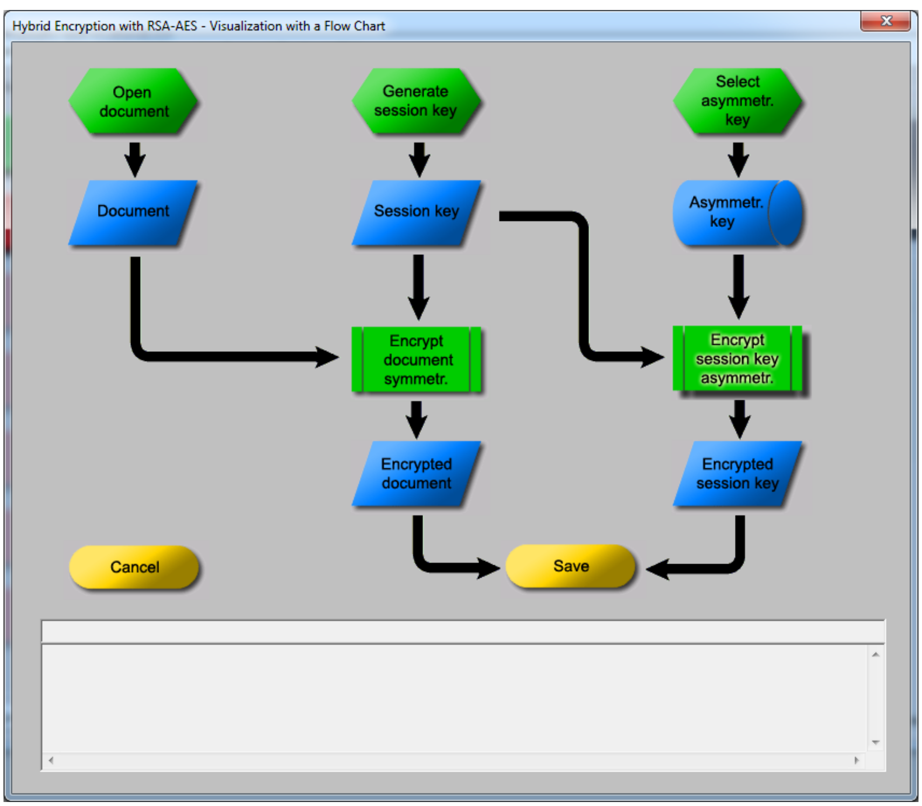
6. Click “**Select asymmetr. key**”.



7. Select Bob’s key and click “**OK**”.

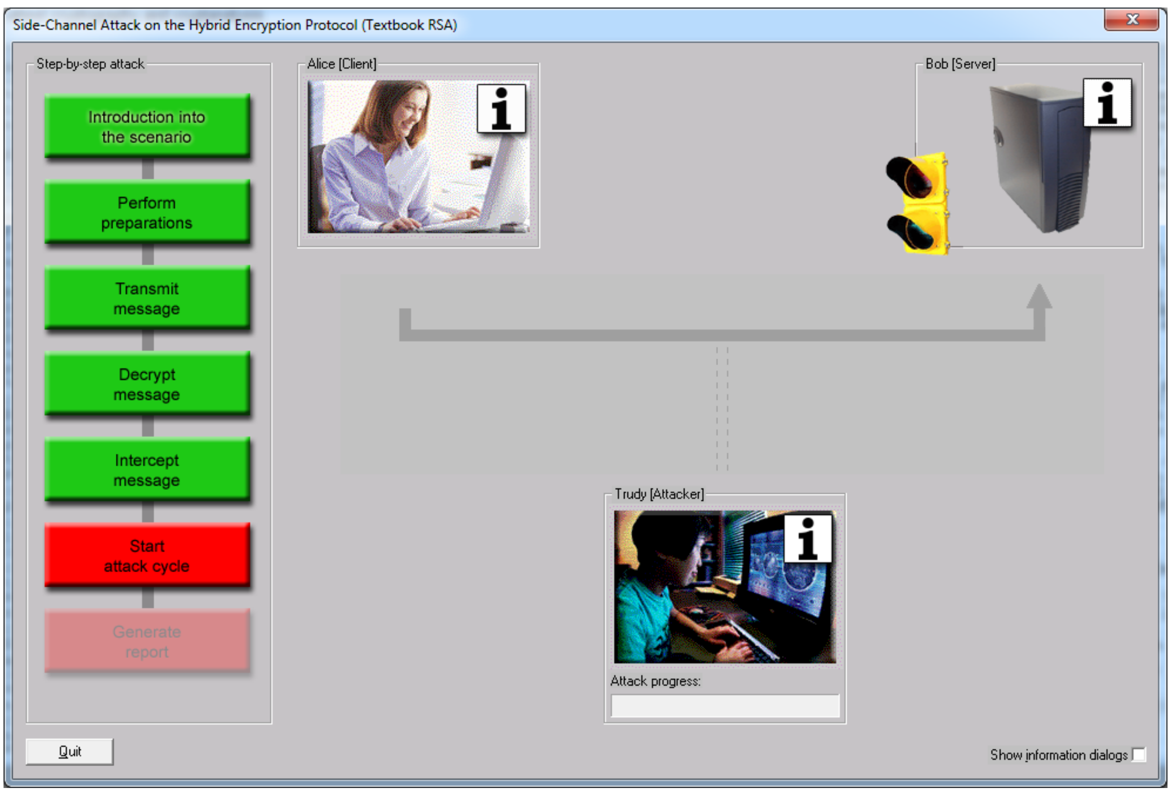


8. Click “**Encrypt document symmetry**.”, “**Encrypt session key asymmetry**.” and “**Save**”.

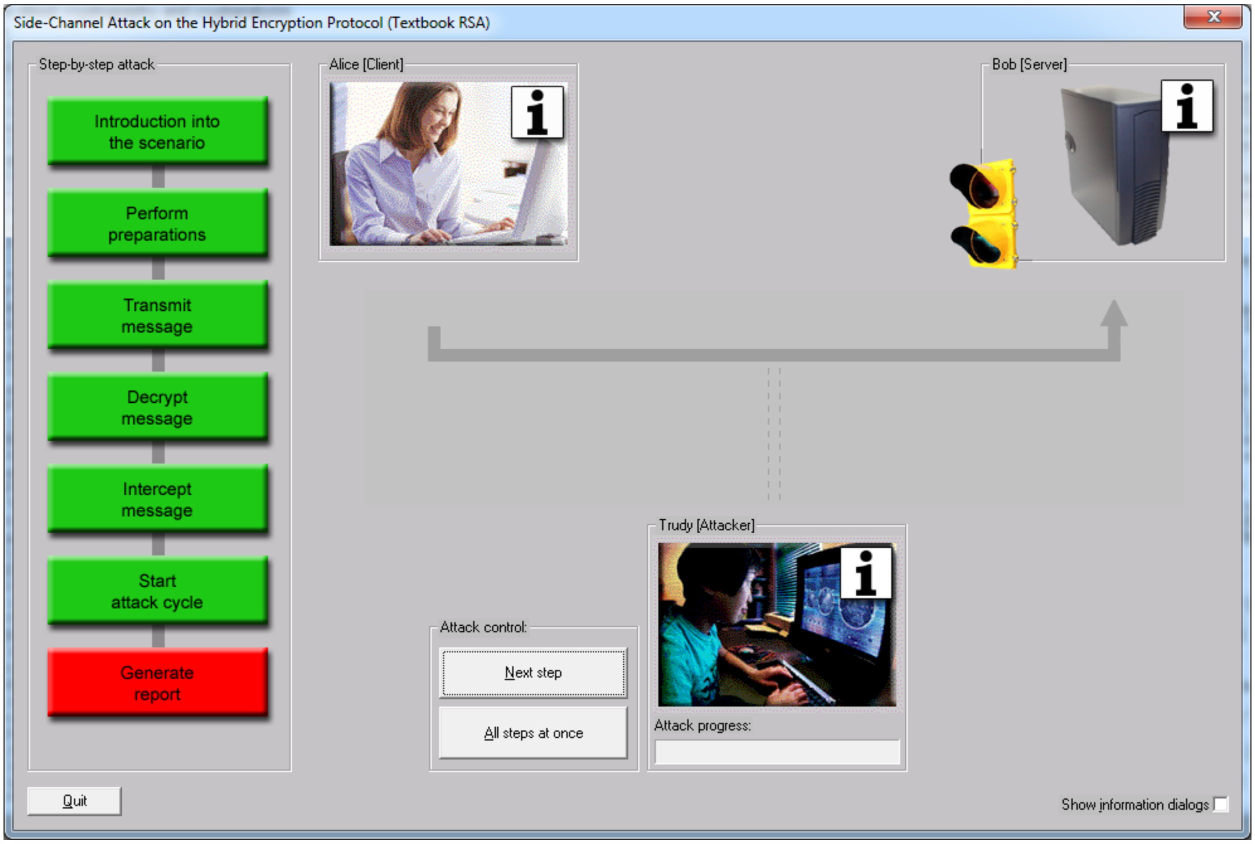


9. Click “**Transmit message**” and “**Decrypt message**”.

10. Enter **1234** and click “**OK**”.

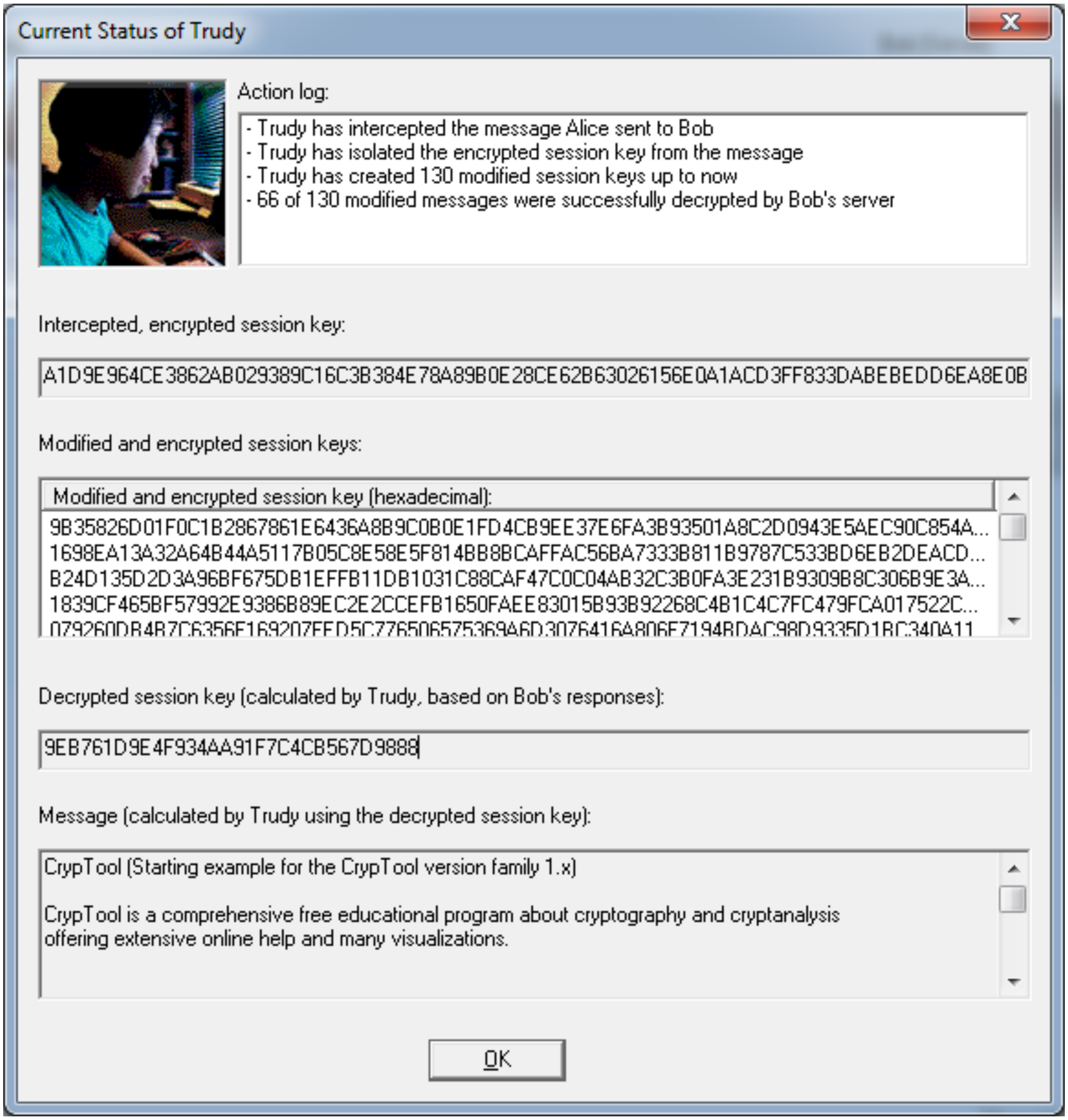


11. Click “**Intercept message**” and “**Start attack cycle**”.



12. Click “**All steps at once**” button.

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



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