Lab 2: Public-Key Cryptography

ITCS461: Computer and Communication Security

Mahidol University

Agenda

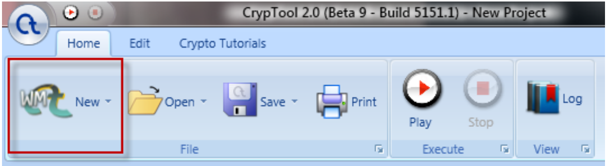
1 Part I: RSA Key Generation

2 Part II: RSA Encryption/Decryption

3 Part III: Attack to Break RSA

Part I: RSA Key Generation

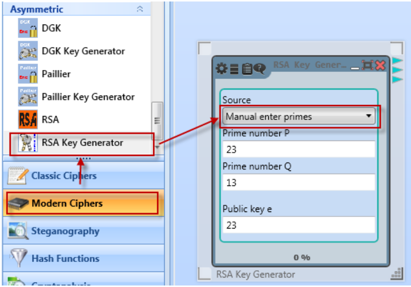
1. Open “**Cryptool 2**” program
2. Create a new worksheet by clicking at “New” button.



CrypTool 2.0 (Beta 9 - Build 5151.1) - New Project

Part I: RSA Key Generation

3. using RSA key generator by:
   - 3.1. Select “**Modern Ciphers**” under the Components block.
   - 3.2. Click “**RSA Key Generator**”.
   - 3.3. Drag and drop it on the workspace.
   - 3.4. Enlarge the “RSA Key Generator” block.
   - 3.5. Select the type of source to be “**Enter primes manually**”.



Source: Manual enter primes

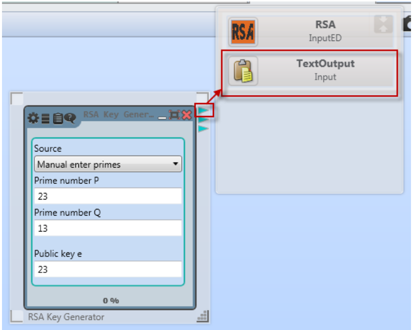
Prime number P: 23

Prime number Q: 13

Public key e: 23

Part I: RSA Key Generation

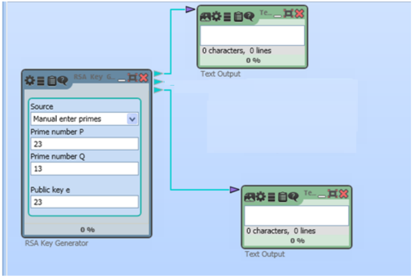
4. Display “N” value by:
    4.1. Move pointer over the 3 blues arrows, look for the one which is the output of “N”.
    4.2. Click on that output blue arrow, drag and release next to the RSA Key Generator block.
    4.3. Then select “TextOutput”.
    4.4. This block is used to display the value “N”, the global modulus number of RSA, which is a part of public key, $PU = \{e, N\}$ and private key, $PR = \{d, N\}$.



Source
Manual enter primes
Prime number P
23
Prime number Q
13
Public key e
23

Part I: RSA Key Generation

5. Display “**d**” value by doing the same as step 4.
   5.1. but now look for arrow of output “**d**”
   5.2. drag and drop
   5.3. select “**textOutput**”



Source: Manual enter primes
Prime number P: 23
Prime number Q: 13
Public key e: 23

Part I: RSA Key Generation

6. Select prime number $P = 7$, prime number $Q = 11$, and public key $e = 17$, then click “**Play**”. Observe the outputs (i.e. “**N**” and “**d**”) for the given values.

Part I: RSA Key Generation

Question 1: What are the values of "N" and "d"?

- value of N = ______________
- value of d = ______________
- calculate $\phi(N) = (P-1)(Q-1) =$ ______________
- Verify that $N = P \times Q$?______________ (Y/N)
- Verify that $e \times d \equiv 1 \bmod \phi(N)$?______________ (Y/N)

  If No, why? ____

Part I: RSA Key Generation

7. Click “**Stop**” and change public key “**e**” to **13**, then “**Play**” again.

Question 2:

- What is the value of private key “**d**”? ______________
- Verify $e \times d \equiv 1 \bmod \phi(N)$?______________(Y/N)

  If No, why? ____

Part I: RSA Key Generation

8. Click “**Stop**” and change public key “**e**” to **5**, then “**Play**” again.

Question 3:

- What is the value of private key “**d**”? ______________
- Verify $e \times d \equiv 1 \bmod \phi(N)$?______________(Y/N)

  If No, why? ____

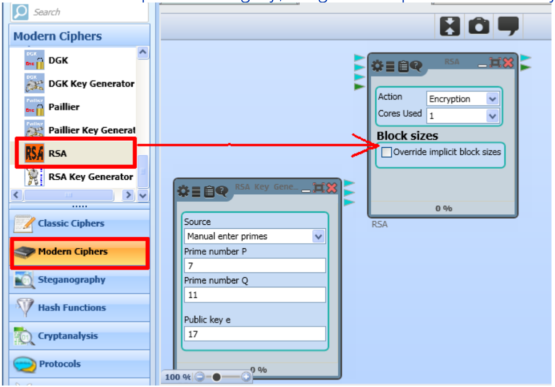
9. “**Stop**” the execution, Delete the two text output blocks but leave the RSA key generator block.

Part II: RSA Encryption/Decryption

Encryption

10. Now, let's do the encryption using the generated Public key, as $(e, N) = (17, 77)$ (Because P=7 and Q=11, So we get $N = P \times Q = 7 \times 11 = 77$).

    10.1. From "Modern Ciphers" category, drag and drop "**RSA**" block to your workspace



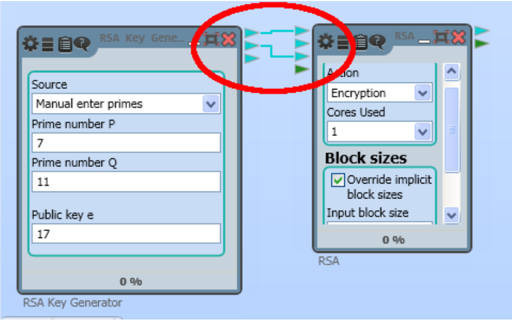
Action: Encryption
Cores Used: 1
Block sizes
☐ Override implicit block sizes

Source: Manual enter primes
Prime number P: 7
Prime number Q: 11
Public key e: 17

Part II: RSA Encryption/Decryption

10.2. Connect output “**N**” and “**e**” connectors of “**RSA Key Generator**” block to the “**RSA**” block accordingly by clicking on output arrow of **RSA key generator** block, drag and release on input arrow of **RSA** block.

(Make sure that the connections are correct by moving mouse pointer over the blue arrows of both blocks.)



RSA Key Generator

Source: Manual enter primes

Prime number P: 7

Prime number Q: 11

Public key e: 17

0 %

RSA

Action: Encryption

Cores Used: 1

Block sizes

☑ Override implicit block sizes

Input block size

0 %

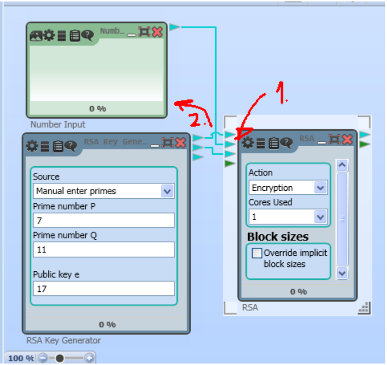
Part II: RSA Encryption/Decryption

10.3. Configure RSA block as following:

- Action=**“Encryption”**
- Core Used=1 (or other number for multi-core CPU)
- Block size= (uncheck, for default block size)

Part II: RSA Encryption/Decryption

11. Create input plaintext block by
    - 11.1. clicking on the blue arrow of “**Message M**” connector on the left of the RSA block
    - 11.2. drag-and-drop on any empty space in the worksheet
    - 11.3. then select “**NumberInput**”

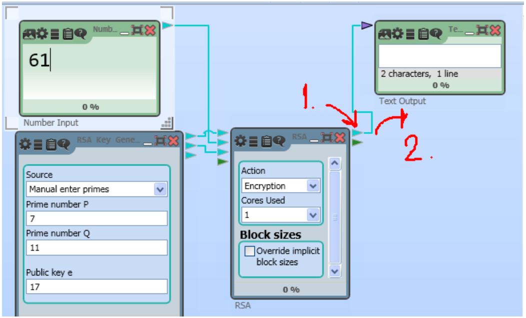


Source: Manual enter primes
Prime number P: 7
Prime number Q: 11
Public key e: 17
0 %
RSA Key Generator

Action: Encryption
Cores Used: 1
Block sizes
☐ Override implicit block sizes
0 %
RSA

Part II: RSA Encryption/Decryption

12. Create output ciphertext block by:
    - 12.1. clicking on the blue arrow of **"Ciphertext C/Message M output (as number)"** connector on the right of the RSA block
    - 12.2. drag-and-drop anywhere on the right
    - 12.3. Then select **"TextOutput"**



Number Input: 61 — 0 %

RSA Key Generator:
- Source: Manual enter primes
- Prime number P: 7
- Prime number Q: 11
- Public key e: 17

RSA:
- Action: Encryption
- Cores Used: 1
- Block sizes: □ Override implicit block sizes
- 0 %

Text Output: 2 characters, 1 line — 0 %

Part II: RSA Encryption/Decryption

13. Type **61** in the “**Number Input**” block. Then click “**Play**” to execute the encryption and “**Stop**”.

Question 4:

- What is the ciphertext (C)? ______________
- What is the encryption key (e)? ______________
- Is it correct ? ______________ (Y/N) *(by using calculator)*

Part II: RSA Encryption/Decryption

14. Type **2** in the “**Number Input**” block.

    Then click “**Play**” to execute the encryption and “**Stop**”.

Question 5:

- What is the ciphertext (C)? ______________
- Is it correct ? ______________ (Y/N) *(by using calculator)*

15. Type **79** in the “**Number Input**” block.

    Then click “**Play**” to execute the encryption and “**Stop**”.

Question 6:

- What is the ciphertext (C)? ______________
- Is it equal to the same output number as Question 5? _______(Y/N)

Part II: RSA Encryption/Decryption

Decryption

16. Now, let's decrypt the ciphertext back using the private key (d, N). We can do this by

    16.1. Deleting the connection of public key **e** between **RSA key generator** and **RSA** blocks (right click on the connecting line want to delete).

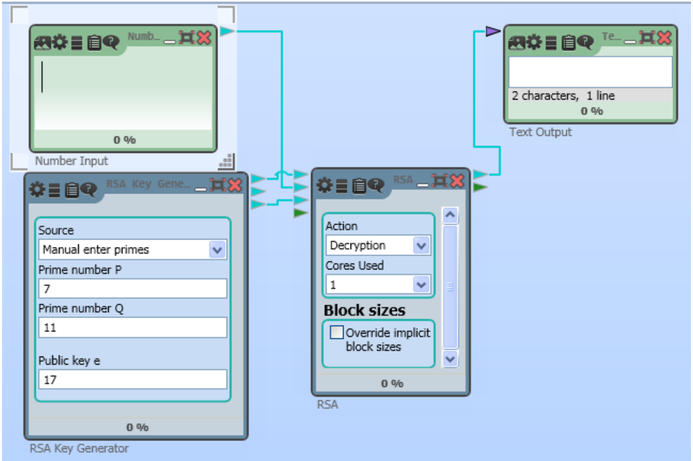
    16.2. Then connect output private key **d** of **RSA key generator** to input private key **d** of **RSA** (same position as input public key e).

    16.3. Change **RSA**'s **Action** to **"Decryption"**

    16.4. Keep the remaining in the same setting as encryption.

Part II: RSA Encryption/Decryption

The workspace now should look similar to the figure below.



Number Input
0 %

RSA Key Generator
Source: Manual enter primes
Prime number P: 7
Prime number Q: 11
Public key e: 17
0 %

RSA
Action: Decryption
Cores Used: 1
Block sizes
□ Override implicit block sizes
0 %

Text Output
2 characters, 1 line
0 %

Part II: RSA Encryption/Decryption

17. Type in the **ciphertext** you got in **Question 4** in the **"Number Input"** block. Then click **"Play"** to execute the decryption.

Question 7:

- What is the message output (M)? ______________________________
- Verify that the decrypted value (plaintext) is identical to the input message of Question 4. ______(Y/N)

  *(check for **P**,**C**,**e** and **d**. If you cannot get "yes", try again.)*

Part II: RSA Encryption/Decryption

18. Repeat Step 17 again but using ciphertext (the output) from **Question 5.**

Question 8:

- What is the message output (M)? ________________________________
- Verify that the decrypted value (plaintext) is identical to the input message of **Question 5.** _______(Y/N)

  *(check for **P**,**C**,**e** and **d**. If you cannot get "yes", try again.)*

Part II: RSA Encryption/Decryption

19. Repeat Step 17 again but using ciphertext of **Question 6**.

Question 9:

- What is the message output (M)? ______________________________
- Verify that the decrypted value is identical to the input message of **Question 6**. ____________(Y/N)
- If no, what do you think the reason is: ______________________________
  ____

Question 10: What is the maximum value of plaintext that will get a successful decryption? ______________________________

Part III: Attack to Break RSA

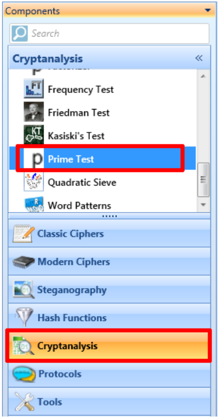
Introduction

We can come up with small prime numbers by ourselves, e.g. **2**, **3**, **5**, **7** and these can be used in RSA (i.e. **P** and **Q**) to generate keys very easily.

However, small prime numbers are not advised to be used in real world because the attackers can easily factorize the public value **N** (i.e. $P \times Q$) back to reveal P and Q values (which supposed to be secret).

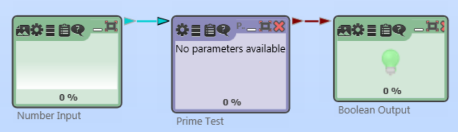
Part III: Attack to Break RSA

20. Create a new workspace
21. CrypTool provides a function to check if a number is a prime or not. Find “**Prime Test**” block under the “**Cryptanalysis**” menu and add it in the workspace.



Part III: Attack to Break RSA

22. Click the **“TextInput”** connector of the **Prime Generator block**. Drag-and-drop the “Number Input” block anywhere on the workspace. Do the same for the **“Boolean Output”** connector.

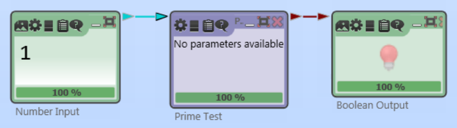


Part III: Attack to Break RSA

23. Type "**1**" in the Number Input block. The **Boolean Output** block will show red color bulb indicating that 1 is not a prime number.

    If you enter a prime number, e.g. "**7**" it will change to green bulb because it is a prime number.

    Also try for other numbers, e.g. 13, 15, 17, 21, 23, …



Part III: Attack to Break RSA

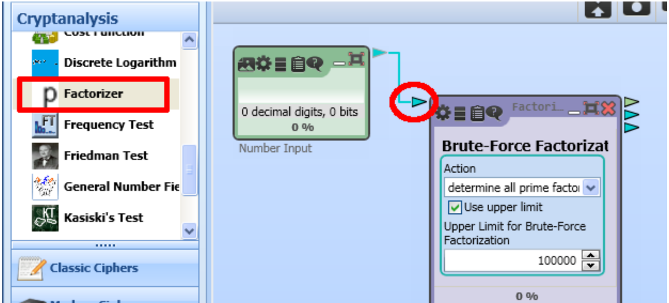
Question 11: Is “33478071698956898786044169848212690817704794983713768 568912431388982883793878002287614711652531743087737814467999489” a prime number ? ______________ (Y/N)

Question 12: Use this workspace to find two prime numbers (i.e. P and Q) in the range of 900 - 1000 and calculate N and $\phi(N)$

- P = ______________
- Q = ______________
- Calculate $N = P \times Q$ = ______________
- Calculate $\phi(N) = (P - 1) \times (Q - 1)$ = ______________

Part III: Attack to Break RSA

24. Stop execution
25. Create another workspace
26. Select “**Factorizer**” block under Cryptanalysis menu. Add it in the new workspace.
27. Click at input connector on the top-left corner, drag and drop somewhere on the left hand side. Then select “**NumberInput**”.

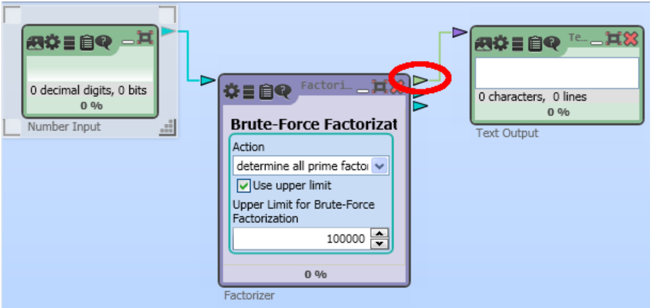


0 decimal digits, 0 bits
0 %

Action
determine all prime factoi
☑ Use upper limit
Upper Limit for Brute-Force Factorization
100000
0 %

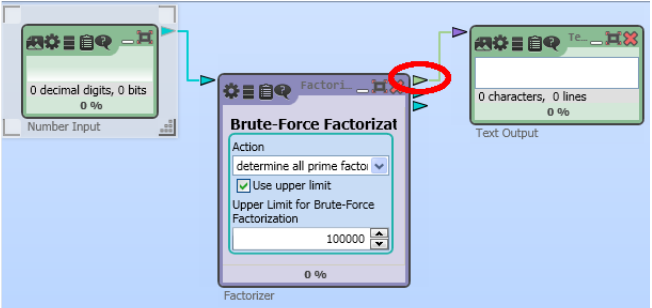
Part III: Attack to Break RSA

28. Click the first output connector on the top-right corner of the "**Factorizer**" block, drag and drop it anywhere on the workspace and choose "**TextOutput**"



Part III: Attack to Break RSA

29. Now you are ready to factorize a product of prime.
    - 29.1. Input the calculated **N** from **Question 1** in the **"Text Input"** block and click **"Play"**.
    - 29.2. Verify the factorized prime numbers shown at the **"Text Output"** blocks.
      (They should be the same as P and Q that you selected in Step 6.)
    - 29.3. Then try other numbers in Question 12. Try until you get correct answers, in order to check that it is working correctly.



Number Input: 0 decimal digits, 0 bits, 0 %

Factorizer: Brute-Force Factorizat
Action: determine all prime factoı
☑ Use upper limit
Upper Limit for Brute-Force Factorization: 100000
0 %

Text Output: 0 characters, 0 lines, 0 %

Part III: Attack to Break RSA

Question 13: Factorize N = 3992003

- P = ______________
- Q = ______________

(check your answer by using a calculator)

Question 14: Factorize N = 98448473560141

If it shows warning (yellow icon) and no result, try increasing the upper limit.

- P = ______________
- Q = ______________

(check your answer by using a calculator)

Part III: Attack to Break RSA

Question 15: Attack to RSA by trying to derive private key (d). Suppose, public-key (e) of Alice is **6007** and global modulus number (N) is **43562419**. Find the corresponding private-key(d) of Alice.

- $N = P \times Q$
- $P =$ ______________
- $Q =$ ______________
- $\phi(N) = (P-1) \times (Q-1) =$ ______________
- $e =$ ______________
- $d = e^{-1} \; mod \; \phi(N) =$ ______________

(check your answer by using a calculator, verify that $e \times d = 1 \; mod \; \phi(N)$*? If not, try again.)*

Before you leave...

Before you leave...

- Don't forget to submit the answer file to ~~the e-learning system.~~MyCourses website
- ~~Delete all workspaces that are opened (click at X on tab menu) and click at Trash Can on Startcenter tab before closing CrypTool.~~
- ~~Delete all files, folders and everything you created.~~
- ~~Shutdown the computer.~~