

End of Encryption/Decryption (RSA Algorithm)

Introduction

This lab will guide you through the installation and initial use of a cryptographic tool called CrypTool. It focuses on encryption, decryption, and key generation using the RSA algorithm.

Learning objectives

- Install **CrypTool 2.1 (Stable Build 9778.2)** on your system
- Generate RSA keys and encrypt/decrypt a message

Part 1: Installing CrypTool 2.1

Step 1: Download CrypTool 2.1

- **CrypTool 2.1** is the current version available as a desktop application.
- Go to the official CrypTool website: <https://www.cryptool.org/en/>.
(*Note: To open the links, right-click (or long-press) on the links and select "Open in new tab." Avoid clicking the link directly, as this might block it.*)

Step 2: Install CrypTool 2.1 on Windows

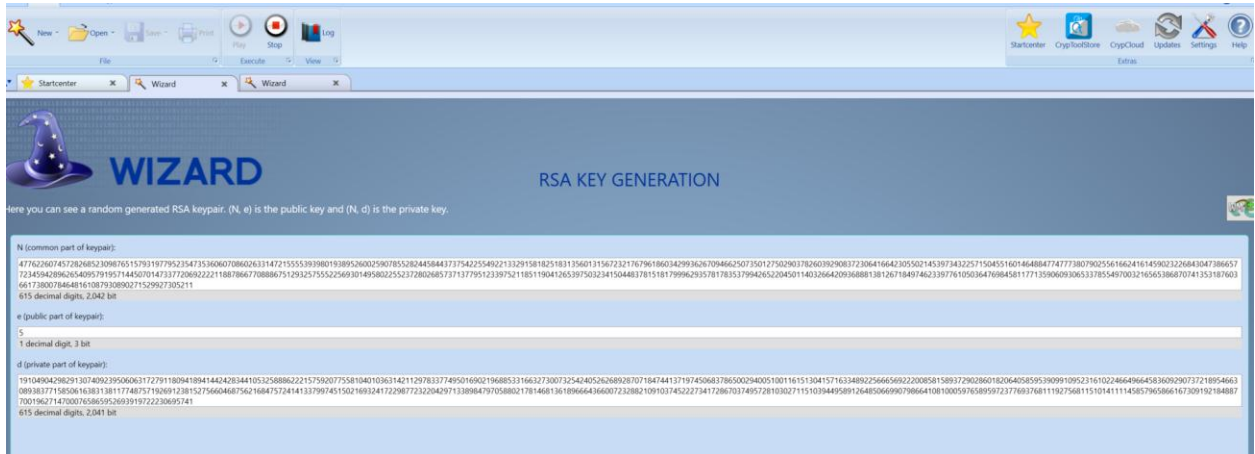
- Download **CrypTool 2.1 (Stable Build 9778.2)** from the official website:
 - Go to [CrypTool 2 Download Page](#).
(*Note: To open the links, right-click (or long-press) on the links and select "Open in new tab." Avoid clicking the link directly, as this might block it.*)
 - Select the version compatible with your operating system (typically a .exe file for Windows).
- Run the installer by double-clicking the downloaded file.
 - Follow the prompts and accept the default installation options.

Part 2: Using RSA algorithm for encryption/decryption

Step 1: Generating an RSA key pair

- Open **CrypTool 2.1**.
- Select the **New** option.
- Select **Encryption/Decryption** from the list of options. Click **Next**.
- Select **Modern Encryption/Decryption**. Click **Next**.

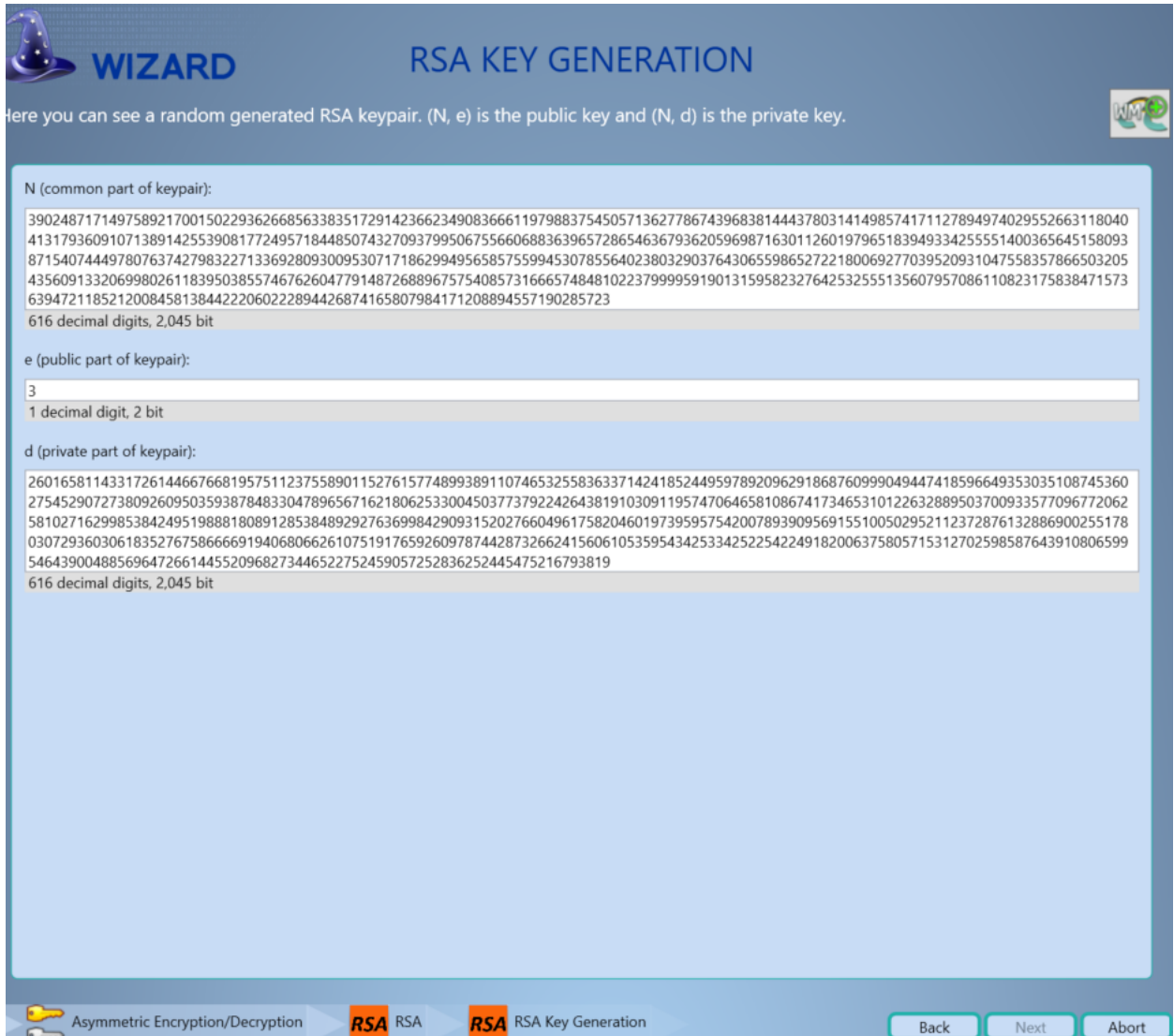
- Select **Asymmetric Encryption/Decryption**. Click **Next**.
- Select **RSA** and click **Next**.
- Select **RSA Key Generation**. Click **Next**.
- The RSA key pair is generated. **(N,e) is the public key, and (N,d) is the private key.**



- Select **Next**.

Step 2: Encryption using public key generated using RSA algorithm

- Click **New** to open a new wizard. Select **RSA Encryption** from the list of options. Click **Next**
- Copy the value of **N** and **e** generated in *Step 1* and paste in the **N** and **e** text box respectively. Type some text in *Text Message to Encrypt*. Click **Next**.



WIZARD RSA KEY GENERATION

Here you can see a random generated RSA keypair. (N, e) is the public key and (N, d) is the private key.

N (common part of keypair):

```
3902487171497589217001502293626685633835172914236623490836661197988375450571362778674396838144437803141498574171127894974029552663118040
4131793609107138914255390817724957184485074327093799506755660688363965728654636793620596987163011260197965183949334255551400365645158093
8715407444978076374279832271336928093009530717186299495658575599453078556402380329037643065598652722180069277039520931047558357866503205
4356091332069980261183950385574676260477914872688967575408573166657484810223799995919013159582327642532555135607957086110823175838471573
639472118521200845813844222060222894426874165807984171208894557190285723
```

616 decimal digits, 2,045 bit

e (public part of keypair):

3

1 decimal digit, 2 bit

d (private part of keypair):

```
2601658114331726144667668195751123755890115276157748993891107465325583633714241852449597892096291868760999049447418596649353035108745360
2754529072738092609503593878483304789656716218062533004503773792242643819103091195747064658108674173465310122632889503700933577096772062
5810271629985384249519888180891285384892927636998429093152027660496175820460197395957542007893909569155100502952112372876132886900255178
0307293603061835276758666691940680662610751917659260978744287326624156061053595434253342522542249182006375805715312702598587643910806599
546439004885696472661445520968273446522752459057252836252445475216793819
```

616 decimal digits, 2,045 bit

Asymmetric Encryption/Decryption RSA RSA RSA Key Generation Back Next Abort

- The **Ciphertext (in Hex)** is generated.
- Select **Next**.

Step 3: Decryption using private key generated using RSA algorithm

- Select **New** to open a new wizard and select **RSA Decryption** from the list of options shown in the left pane. Select **Next**.
- Copy the Value of **N** and **d** generated in *Step 1* and paste in the *N* and *d* text box respectively. Similarly, copy the **Ciphertext (in Hex)** generated in *Step 2* and paste in the *Text Message to Decrypt* box. Click on **Next**.



- The decrypted message is generated.

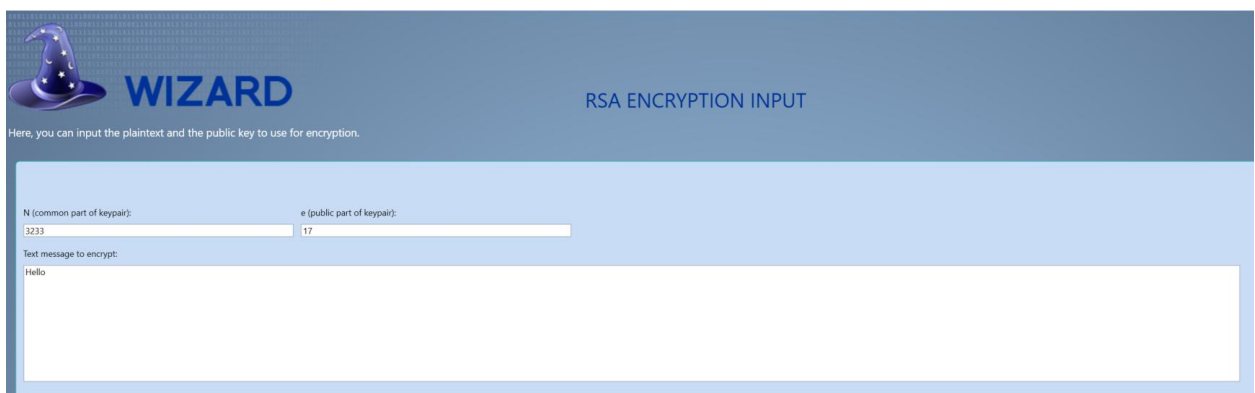
Exercise

- Here are two sets of (N), (e), and (d) values for an RSA experiment. These values represent the modulus ((N)), the public exponent ((e)), and the private exponent ((d)). (N,e) is the public key and (N,d) is private key. Encrypt and decrypt the message using these key pairs.

Set 1:

- (N = 3233)

- (e = 17)



- (d = 2753)



WIZARD


RSA ENCRYPTION OUTPUT

Here, you can see the RSA encryption output.

Ciphertext (in Hex):
88 08 21 05 E9 02 E9 02 89 08
29 characters, 1 line

Set 2:

- (N = 2773)
- (e = 13)



WIZARD

RSA DECRYPTION INPUT

Here, you can input the plaintext and the private key to use for decryption.

N (common part of keypair): 3233 d (private part of keypair): 2753

Text message to decrypt (in Hex):
88 08 21 05 E9 02 E9 02 89 08

- (d = 937)



WIZARD

RSA DECRYPTION OUTPUT

Here, you can see the RSA decryption output.

Plaintext:
Hello
5 characters, 1 line

Decrypted Text:

Summary

In this reading, you have learned to successfully install **CrypTool 2.1 (Stable Build 9778.2)**, generate RSA keys, and perform encryption and decryption tasks. This reading provides a solid foundation for more advanced cryptographic experiments.

My Reflection

This lab provided hands-on experience with the RSA algorithm using CrypTool. It reinforced my understanding of public/private key encryption, the structure of RSA key pairs, and the

conversion of plaintext to ciphertext using mathematical operations. I also practiced inputting key values manually and interpreting the results, which helped deepen my grasp of asymmetric cryptography.