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

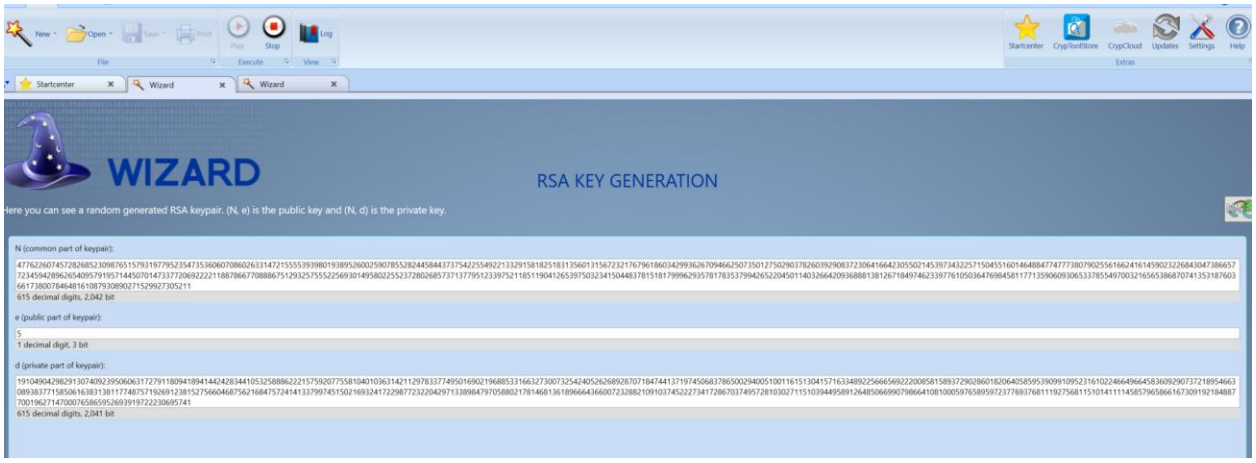
- Download **CrypTool 2.1 (Stable Build 9778.2)** from the official website:
  - Go to CrypTool 2 Download Page.
    *(**Note**: To open the links, right-click (or long-press) on the links and select "Open in new tab." Avoid clicking the link directly, as this might block it.)*
  - Select the version 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**.

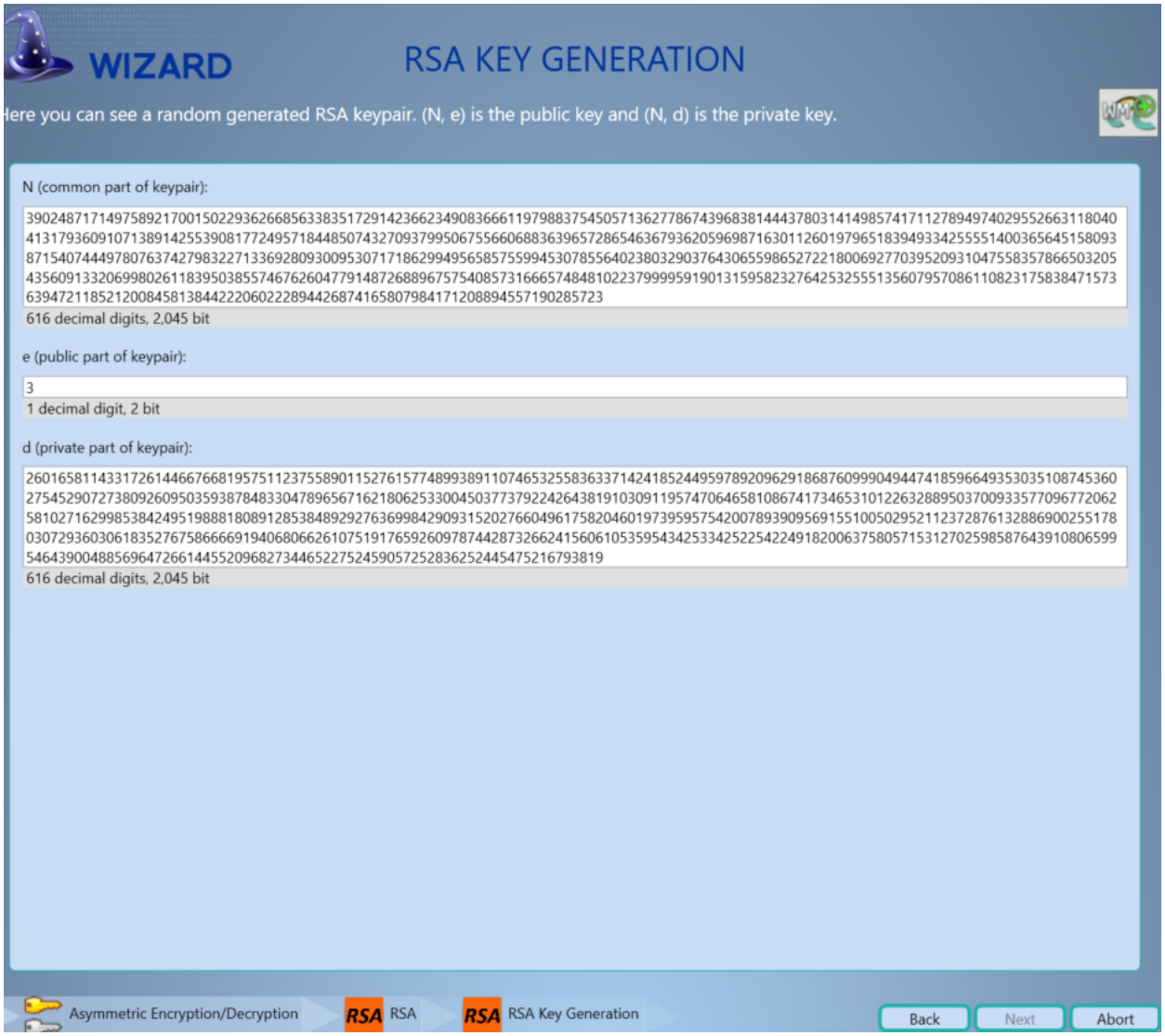
- Select **Asymmetric Encryption/Decryption**. Click **Next**.
- Select **RSA** and click **Next**.
- Select **RSA Key Generation**. Click **Next**.
- The RSA key pair is generated. **(N,e) is the public key, and (N,d) is the private key**.



- 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**.



- 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**.

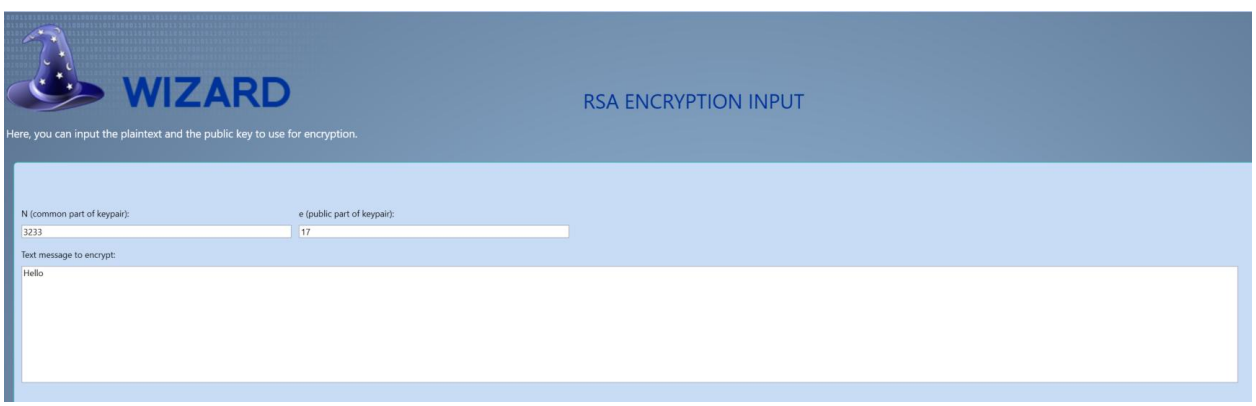
- The decrypted message is generated.

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:

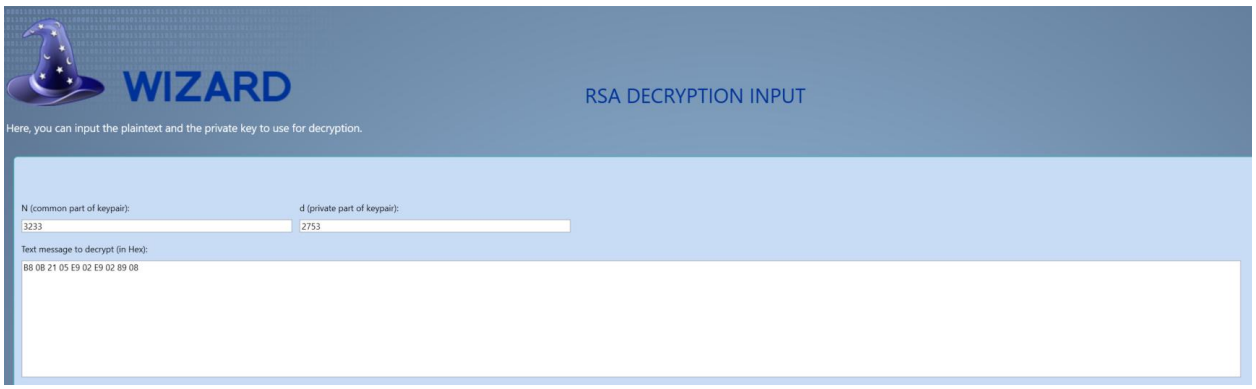
- (N = 3233)
- (e = 17)



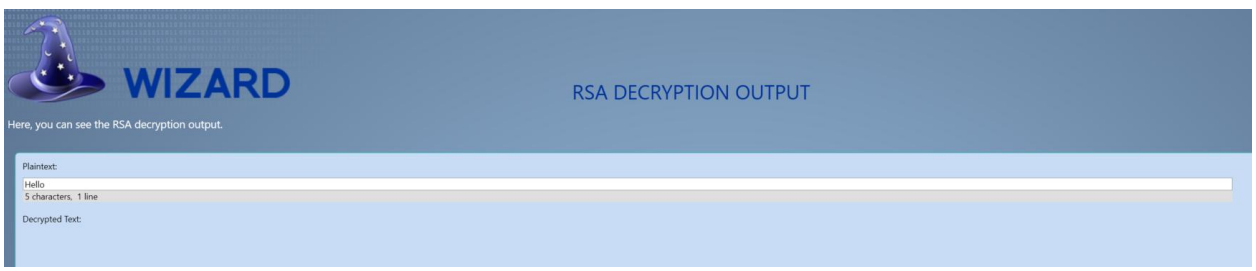
- (d = 2753)

Set 2:

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



- (d = 937)



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.