2.1 Lab on RSA Encryption and Factorization Attacks

Encryption or decryption of messages using the RSA key pair.

1. Select Individual Procedures/RSA Cryptosystem/RSA Demonstration

2. Enter the RSA key \( p=47, \quad q=79, \quad e=37 \). The parameters \( N = p\times q=3713 \) 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 processed into ciphertext: 1999 # 3408 # 2545 # 2798 # 0001 # 3284 # 3613 # 1404 # 2932 # 0208 # 1095 # 3306 to input text 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 \( \text{______________} \), the value of \( \phi(N) \) is \( \text{______________} \), the value of private key \( d \) is \( \text{__________} \).
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 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**.
You will receive a cipher text that is only half as long: