Name: _____ **Student No.:** _____ **Date:** __/__/____

Modern Cryptography

RSA ALGORITHM

It was introduced in 1977 as the **first public-key encryption system** and is named after its creators, **Rivest, Shamir, and Adleman.**

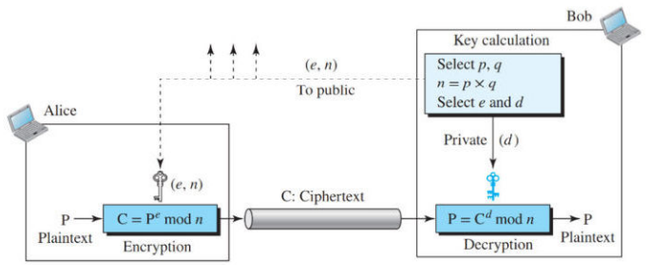
Its **security** is based on the **difficulty of factoring the product of two large prime numbers.**

In this worksheet, you will **explore RSA encryption with public and private keys.**

How does RSA encryption work?

Suppose Alice wants to send Bob a secure message using RSA. Bob **generates two mathematically linked keys:**

- **Public key: Shared with everyone** to **encrypt** messages.
- **Private key: Kept secret** to **decrypt** messages.



These keys are generated by selecting **two large primes**, multiplying them to form a **modulus**, computing **Euler's totient function** (which helps determine a suitable encryption key), and finding the corresponding decryption key.

Here's how to encrypt and decrypt messages with RSA using **OpenSSL**:

The **OpenSSL** software library is a robust, commercial-grade, full-featured toolkit for **general-purpose cryptography** and **secure communication.**

1. **Set Up OpenSSL**
   a. Open **Command Prompt** and **type:**
   ```
   openssl
   ```
   b. If OpenSSL is **not found, install it.** Scan the **QR code** for a **Windows installation tutorial.**
2. **Pair Up with a Lab Partner:** Use **separate computers** to **exchange** encrypted messages.
3. **Create a New Folder**
   a. Navigate to your **Documents** folder:
   ```
   cd Documents
   ```
   b. Create a **new folder** named with your **last name:**
   ```
   mkdir [Your Last Name]_Lab_Exer_2
   ```
   c. Enter the new folder:
   ```
   cd [Your Last Name]_Lab_Exer_2
   ```
4. **Create your Message File**
   a. Open **Notepad** to create a **new text file** named with your **last name:**
   ```
   notepad message-[Your Last Name].txt
   ```
   b. In the text file, **enter your information and save it:**
   - **Name:** [Your Full Name]
   - **Year and Section:** [Your Year and Section]
   - **Date:** [Today's Date]

   Example:
   ```
   Name: Juan A. Dela Cruz
   ```

```
Year and Section: BSI/T 3A
Date: 02/26/2025
```

5. **Append Date and Time**
   a. Add the **current date and time** to the **message file**:
   ```
   echo %DATE% %TIME% >> message-[Your Last
       Name].txt
   ```
6. **Generate Your RSA Key Pair**
   a. Create a **Private Key**:
   ```
   openssl genrsa -out private-[Your Last
       Name].pem 2048
   ```
   This generates a **2048-bit** private key in **PEM** format.
   b. Create a **Public Key**:
   ```
   openssl rsa -in private-[Your Last Name].pem
       -pubout -out public-[Your Last Name].pem
   ```
7. **Exchange Public Keys**
   a. **Give your public key file** (`public-[Your Last Name].pem`) to your lab partner.
   b. **Receive** your **partner's public key file.**
8. **Encrypt Your Message**
   a. Use your **partner's public key** to **encrypt** your message:
   ```
   openssl pkeyutl --encrypt --inkey
       public-[Your Partner's Last Name].pem
       --pubin --in message-[Your Last Name].txt
       --out message-[Your Last Name].enc
   ```
9. **Verify the Encrypted Message**
   a. Open **Notepad** to view **your encrypted message**:
   ```
   notepad message-[Your Last Name].enc
   ```
10. **Delete the Unencrypted Message**
    a. For security, **remove** the **original text file**:
    ```
    del message-[Your Last Name].txt
    ```
11. **Exchange Encrypted Messages**
    a. **Give your encrypted message** (`message-[Your Last Name].enc`) to your partner.
    b. **Receive** your **partner's encrypted message file.**
12. **Decrypt Your Partner's Message**
    a. Use **your private key** to **decrypt** the message from your partner:
    ```
    openssl pkeyutl --decrypt --inkey
        private-[Your Last Name].pem --in
        message-[Your Partner's Last Name].enc
        --out message-[Your Partner's Last
        Name].txt
    ```
13. **Append Date and Time**
    a. Add the **current date and time** to the **decrypted message file**:
    ```
    echo %DATE% %TIME% >> message-[Your Partner's
        Last Name].txt
    ```
14. **Verify the Decrypted Message**
    a. Open **Notepad** to view your **partner's message**:
    ```
    notepad message-[Your Partner's Last Name].txt
    ```
    b. Check the file to make sure the message is **displayed correctly.**

✓ Files to Upload

Compress your folder into a **.zip** file and name it `[Your Last Name]_Lab_Exercise_2.zip`.

Resources:

Serious Cryptography, Aumasson
Cryptography and Network Security, Stallings
Data Communications and Networking, Forouzan
https://www.keylength.com/en/4/
https://docs.aws.amazon.com/acm/latest/userguide/import-certificate-format.html
https://0xshakhawat.medium.com/demystifying-rsa-encryption-and-decryption-with-openssl-ea1e86e30271