

Group Assignment 2 (6%): Digital Signature Generation and Verification

Deadline: 9/25/2025, send it to yxw1259@miami.edu

Question 1

The goal of this assignment is to help you understand how **digital signatures** work in practice. You will generate a digital signature using your **private key** and then allow verification using your **public key**, ensuring authenticity and integrity.

Requirements

1. **Key Generation**
 - a. Generate an RSA key pair (private key and public key).
 - b. Save the keys securely.
2. **Message Preparation**
 - a. Create a text message containing your **full name or group name**.
3. **Signature Generation**
 - a. Use your **private key** to generate a digital signature for the message.
4. **Verification**
 - a. Provide both your **public key** and the **signature**.
 - b. I will use your public key to verify that the signature matches your message.

Submission

- A text file containing:
 - Your **public key**.
 - Your **original message (full name or your group name)**.
 - The **signature** (in base64 format).

The codes are here: <https://colab.research.google.com/drive/1j-w47-wWk1FJnHWLiOuTuT3mkFL94AEO?usp=sharing>

Question 2: Answer the following questions

1. What is a digital signature, and how is it different from a handwritten signature?
2. List and explain the four assurances provided by a digital signature.

3. Describe the steps involved in creating a digital signature.
4. Why is the private key used only for encrypting the hash value and not the entire message?
5. How does a recipient verify a digital signature?