Lab on Short Message RSA Attacks and Padding

In **short message attack of RSA**, if it is known that Alice is sending a four-digit number to Bob, Eve can easily try plaintext numbers from 0000 to 9999 to find the plaintext. Therefore, short message must be padded with random bits. **If you are Eve, show that you are able to find the plaintext containing four digit numbers given ciphertext.**

Optimal asymmetric encryption padding (OAEP) is recommended when short messages are encrypted with RSA algorithms. The following is the encryption and decryption processes of OAEP.

- **Encryption**
  - Pad the message to make m-bit message M, if M is less than m-bit
  - Choose a random number r
  - User one-way function G that inputs r-bit integer and outputs m-bit integer. This is the mask.
  - \( P_1 = M \oplus G(r) \)
  - \( P_2 = H(P_1) \oplus r \), function H inputs m-bit and outputs k-bit
  - \( C = E(P_1 || P_2) \). User RSA encryption here

- **Decryption**
  - \( P = D(P_1 || P_2) \)
  - Bob first recreates the value of r:
    - \( H(P_1) \oplus P_2 = H(P_1) \oplus H(P_1) \oplus r = r \)
  - Bob recreates msg:
    - \( G(r) \oplus P_1 = G(r) \oplus G(r) \oplus M = M \)

Pad your message with OAEP padding and then encrypt by RSA.

**What to submit:**
A report describes how you find the unpadded short plaintext (50 points), describes what you have observed after you apply OAEP padding (20 points), and discusses feasibility of short message attack after padding (30 points).