Information Security Basics
Public-key Cryptography Part

Jean-Sébastien Coron

Université du Luxembourg

1 OAEP Encryption

From the description of OAEP in the course, provide the pseudo-code of OAEP encryption and decryption.

2 PSS Signature

From the description of PSS in the course, provide the pseudo-code of PSS signature and verification.

3 Is RSA Encryption Anonymous ?

Bob must send 10 messages $m_1, \ldots, m_{10}$, either to Alice whose RSA public-key is (N_1, e_1), or to Anais whose RSA public-key is (N_2, e_2).

Therefore if Bob sends his 10 messages to Alice, he is going to send the ciphertexts:

$$c_i = (m_i)^{e_1} \mod N_1$$

for $1 \leq i \leq 10$.

Whereas if Bob sends his messages to Anais, he sends the following ciphertexts:

$$c_i = (m_i)^{e_2} \mod N_2$$

An eavesdropper gets the 10 ciphertexts c_i, and also knows the public-key of Alice and Anais, but she doesn't know the messages m_i. How might she be able to determine whether Bob sent his messages to Alice or Anais ?