Information Security Basics
Public-key Cryptography Part

Jean-Sébastien Coron

Université du Luxembourg

1. Explain how to construct a public-key encryption scheme from a trapdoor one-way permutation.
2. What are the advantages and drawbacks of public-key encryption compared to symmetric-key encryption ?
3. Explain how hybrid encryption (combination of public-key encryption and symmetric-key encryption) works. What are the advantages compared to a pure public-key encryption scheme ?
4. Explain why encryption must be probabilistic. An encryption scheme is said to be probabilistic when for a given plaintext there corresponds (exponentially) many ciphertexts, one of which is generated at random during encryption.
5. 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 ?