

2010 - Exercises V.

1. Suppose that Eve observes a cryptotext $c = m^e \bmod n$ encrypted using the RSA cryptosystem. Suppose further that she is permitted to request a decryption of a single cryptotext $c' \neq c$. Show how she can find the plaintext m .
2. There are given $n = 11021$ and $\phi(n) = 10812$. Factorize n if you know that it has two prime factors. Do not use bruteforce. Explain your reasoning.
3. Consider the RSA cryptosystem. Let Alice's public key be $(n_A, e_A) = (3127, 3)$, Bob's $(n_B, e_B) = (6319, 3)$ and Charles's $(n_C, e_C) = (5029, 3)$. Suppose that David sends to Alice, Bob and Charles the same message m which is encrypted as $c_A = 302$, $c_B = 3081$ and $c_C = 137$, respectively. Can Eve, who is not using bruteforce, learn some knowledge about m ? If yes, determine that knowledge.
4. Suppose that Alice wants to send a message 01101 to Bob using the Knapsack cryptosystem with $X = (1, 3, 7, 13, 26)$, $m = 523$ and $u = 467$.
 - (a) Find Bob's public key X' .
 - (b) What is the cryptotext c computed by Alice?
 - (c) Perform in detail Bob's decryption of c .
5. Suppose Alice and Bob use the McEliece cryptosystem with

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \quad P = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

- (a) Compute G' .
 - (b) Decode cryptotext $c = 0110110$.
6. Alice participates in a knowledge quiz and Bob is her friend on telephone. When the question is too hard, Alice can ask Bob for the answer. In order to have a secure conversation they have established a communication protocol with RSA cryptosystem with prime numbers $p = 331$ and $q = 283$. They have selected their own public keys $e_A = 18241$ and $e_B = 1871$. Each plaintext character is represented by a number between 10 (A) and 35 (Z), 36 represents a blank. Using this representation, a message is divided into blocks of length 5 and each of them is encrypted/decrypted separately. Before sending, every message is first authenticated by the sender (encrypted with sender's private key) and encrypted with receiver's public key. Now, imagine that you are Bob and you received the following message:

19262508878951581769668582295738494832318265871682136128922828831

Find out the original message and use this protocol to send Alice the correct answer.