IV054 Coding, Cryptography and Cryptographic Protocols
2019 - Exercises V.

1. *(4 points)*

   (a) Encrypt your UČO (personal identification number) with the RSA cryptosystem with public key $e = 7$ and $n = 1147$. Then, with the knowledge $31 \times 37 = 1147$, show the decryption steps.

   (b) Encrypt the binary expansion of the last two digits of your UČO (this is a binary vector of length 7) with the Knapsack cryptosystem with public key $X' = (155, 208, 57, 216, 126, 150, 153)$. Then, with the knowledge $X = (1, 3, 7, 13, 29, 59, 127)$, $u = 155$, $m = 257$, show the decryption steps.

2. *(4 points)*

   (a) You are given $n = 11021$ and $\phi(n) = 10812$. Factorize n if you know that it has two prime factors. Do not use brute force.

   (b) You are given RSA modulus $n = 53916647$. Determine p and q knowing the fact that the difference between factors is small.

3. *(4 points)* Consider the Knapsack cryptosystem with public key

$$X' = (1099, 893, 790, 378, 1855, 207, 1616, 2030, 626, 1459).$$

   Decrypt the ciphertext $(3867, 2085, 2688, 5301, 7390)$ knowing the modulus $m = 2301$ and the fact that the corresponding private key was not carefully chosen.

4. *(3 points)* Consider the RSA cryptosystem with public modulus $n = 1147$ and encryption exponent $e = 7$. You have obtained the following (plaintext, cryptotext) pairs: $(21, 321)$, $(29, 1081)$, $(33, 562)$. Use this knowledge to decrypt cryptotexts $c_1 = 323$ and $c_2 = 475$ without factoring n.

5. *(4 points)* Consider the following public-key cryptosystem that allows Bob to send an encrypted message m to Alice:

   (i) Alice chooses a Galois field $\mathbb{F}_q$.

   (ii) Alice chooses l polynomials in n variables $P_1, \dots P_l$, such that $P_i(v_1, \dots v_n) = 0$ for some $v = (v_1, \dots v_n) \in \mathbb{F}_q^n$, for all $1 \leq i \leq l$.

   (iii) Alice makes $\mathbb{F}_q$ and $(P_1, \dots, P_l)$ public.

   (iv) To send a message m, Bob chooses l polynomials with n variables $Q_1, \dots Q_l$ and encrypts m using the function

$$f : m \mapsto f(m) = m + \sum_{j=1}^{l} Q_j P_j.$$

   (v) Bob sends $f(m)$, the polynomial that is the encrypted message m, to Alice.

   The function f is a trapdoor function. Find the decryption process and the trapdoor information Alice needs to perform decryption.

6. *(4 points)* Use the Rabin Miller's Monte Carlo algorithm (see Exercise Book) to decide whether 6997 is prime or composite. Give the error probability of the outcome. During the evaluation, consider the following random choices of x: 2101, 3035, 6101, and 30.

7. *(4 points)* Alice, Bob, and Charlie use the RSA cryptosystem to communicate. Alice has public key $e_A = 29$, $n = 20453$, Bob's public key is $e_B = 61, n = 20453$, and Charlie has $e_C = 97, n = 20453$. Bob sent the same message m to both Alice and Charlie. Eve intercepted cryptotexts $c_{B\to A} = 3968$ and $c_{B\to C} = 6390$ sent from Bob to Alice and to Charlie, respectively. Can Eve, who is not using any brute force methods, determine the secret message? Omit the fact that the numbers are small. If your answer is yes, determine m. Justify your reasoning.

More on next page >>>

8. *(3 points)* Recall that density of a Knapsack vector $X = (x_1, \ldots, x_n)$ is defined as

$$d(X) = \frac{n}{\log(\max\{x_i \mid 1 \leq i \leq n\})}$$

.

(a) Calculate the density of X from Exercise 1(b).

(b) Show that the upper bound for density of a super-increasing vector of length n is $\frac{n}{n-1}$.