2018 - Exercises V.

1. *Extended Euclidean algorithm* is arguably the most important algorithm in number theory.
   (a) Use the Euclidean algorithm to find the $\gcd(4757, 4087)$.
   (b) Use the extended Euclidean algorithm to find an inverse of 97 in $(\mathbb{Z}_{977}, \cdot)$.

2. Alice uses the RSA cryptosystem with modulus $n = 9017$ and public key $e = 1727$. Bob sent her encrypted message $c = 6766$ and you have managed to obtain the corresponding plaintext $w = 2374$ by other means. Bob sent her another encrypted message $c' = 8464$.
   Decrypt the cryptotext c' without factoring the modulus n.

3. (a) Encrypt your UČO (personal identification number) using the RSA cryptosystem with public key $e = 3$ and $n = 1207$. Then, with the knowledge $17 \times 71 = 1207$, 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) using the Knapsack cryptosystem with public key $X' = (155, 208, 57, 216, 126, 150, 153)$. Then, with the knowledge of $X = (1, 3, 7, 13, 29, 59, 127)$, $u = 155$ and $m = 257$, show the decryption steps.

4. Consider the RSA cryptosystem with the public key $n = 1363, e = 3$. You have obtained the following plaintext-cryptotext pairs:
   $$(1062, 3), \quad (979, 5), \quad (16, 7).$$
   Decrypt the cryptotexts $c_1 = 135$ nd $c_2 = 245$ without factoring n.

5. Alice and Bob use the Diffie-Hellman key exchange. They have chosen $p = 1217$ and $q = 3$. Eve is eavesdropping their communication. She intercepts message $X = 1193$ sent by Alice to Bob and message $Y = 910$ sent by Bob to Alice. She has also precomputed the following table of discrete logarithms:

x	$\log_3 x \mod 1217$
2	216
3	1
5	819
7	113
11	1059
13	87

   Compute Alice's and Bob's shared key using Eve's information.

6. Let (e, n_1) and (e, n_2) be Alice's and Bob's RSA public keys and let their encryption exponent be $e = 3$. Charlotte sends both of them the same short secret message m. Suppose n_1 and n_2 are coprimes and $m^e \ll n_1 n_2$.
   (a) Show how Eve, who intercepted both cryptotexts, reconstructs m. (Do not use brute force.)
   (b) Calculate m given public moduli $n_1 = 1363, n_2 = 2419$ and cryptotexts $c_1 = 18$ and $c_2 = 325$.

7. You have a machine that generates RSA keys for smart cards. The machine generated the following moduli:
   $$101060693, \quad 91991791, \quad 129560071, \quad 115602119, \quad 86893073.$$
   Try to factorize them without using brute force.

8. Consider the Knapsack cryptosystem described in the lecture slides with $n \geq 5$. Show that for any $1 \leq i \leq 5$ the following inequality holds
   $$|k_i x'_1 - k_1 x'_i| \leq 2^{n+6}$$
   for some integers k_i.
   (*Hint:* you can use as the fact, without providing a proof, that for a superincreasing sequence it holds: $0 \leq x_i \leq 2^{-n+i} m$ for any $1 \leq i \leq n$.)