IV054 Coding, Cryptography and Cryptographic Protocols
2012 - Exercises V.

1. Let $(n, 3)$ be a public key of the RSA cryptosystem. Describe how the plaintext m can be found, provided the cryptotexts c, c' corresponding to the plaintexts m, $m+1$, respectively, are known.

2. You are given $n = 177773$ and $\phi(n) = 176928$. Factorize n if you know that it has two factors. Do not use brute force.

3. Consider Alice and Bob use Diffie-Hellman protocol to establish a common secret key. Let $p = 599$ and $q = 11$. Alice and Bob have chosen secret exponents $x = 11$ and $y = 27$, respectively. Perform in detail steps of the protocol and determine X, Y and the secret key K.

4. Suppose Bob is using RSA with modulus $n = 15093209$ and two public exponents $e_1 = 7$ and $e_2 = 17$ corresponding to the same n. Alice wanted to be sure that Bob will get her message, so she encrypted the same plaintext m with both of Bob's public keys and sent $c_1 = m^{e_1} \pmod n = 2922630$ and $c_2 = m^{e_2} \pmod n = 1902230$. Without factorization of n determine m.

5. Let x, y be positive integers. Decide whether the following statements are true. For each of them, provide either a counterexample or a proof.

   (a) If x divides y^2, then x divides y.

   (b) If x^3 divides y^2, then x divides y.

6. Suppose that Alice wants to send a message 11010 to Bob using the Knapsack cryptosystem with $X = (1, 3, 5, 11, 25)$, $m = 181$ and $u = 42$.

   (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.

7. Bob wants more secure RSA, so he tries to repeat encryption of the ciphertext.

   (a) Let $n = 35$ be the RSA modulus and let m be a plaintext. Show that $e(e(m)) = m^{e^2} \pmod{35} = m$ for any legitimate public exponent e which leads to a completely insecure RSA cryptosystem.

   (b) Generalize results of (a) and explain how to mount a similar attack in order to decrypt a ciphertext c given the corresponding public key (n, e).

8. Let p, q be primes such that $p \neq q$, $n = pq$, $\phi(n) = (p-1)(q-1)$ and $g = \gcd(p-1, q-1)$. Prove that
$$a^{\phi(n)/g} \equiv 1 \pmod n$$
for all a satisfying $\gcd(a, n) = 1$.