IV054 Coding, Cryptography and Cryptographic Protocols
2013 - Exercises V.

1. Suppose that Alice wants to send a message 011101 to Bob using the Knapsack cryptosystem with $X = (2, 4, 7, 17, 31, 70)$, $m = 145$ 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.
2. Find all primes p such that $p + 2$ and $p + 4$ are also prime numbers.
3. Find the private key d of Bob's RSA cryptosystem with modulus $n = 437$ and public key $e = 35$ with the only information that the number $a = 2$ has order $r = 198$ in $\mathbb{Z}_n^*$.
4. Answer the following questions. Explain your reasoning.
   (a) Let $\phi(n)$ denote the Euler totient function. Decide whether the following statement holds. For all multiplicative monoids $\mathbb{Z}_n$, $d = e^{-1} \pmod{\phi(n)}$, where $\gcd(e, \phi(n)) = 1$, is the lowest possible decryption exponent for the decryption to work for any plaintext in $\mathbb{Z}_n$.
   (b) Is it secure to have p fixed and only randomize q when using the RSA cryptosystem?
   (c) Eve has found out three mutually different numbers x such that $x^2 = 1 \pmod{\text{n}}$. Can she use this knowledge to break the RSA?
5. Consider the Diffie-Hellman protocol. Alice and Bob decided to use $\mathbb{Z}_n^*$ instead of $\mathbb{Z}_p^*$ where $n = ab$ and a, b are secret large primes. Does this modification affect security of the protocol?
6. Consider the RSA cryptosystem. Suppose that malicious Eve can intercept, transform and resend a ciphertext and that she can later gain access to the discarded meaningless plaintext which is the result of unsuccessful decryption of the tampered ciphertext performed by the authorized recipient. Propose an attack that allows Eve to recover the original plaintext.
7. Suppose you have an efficient algorithm to solve Computional Diffie-Hellman problem, *ie.* given g, g^a and g^b, compute g^{ab}. Show that in such case you are able to efficiently solve the following problem: given g and g^a, compute $g^{a^{-1}}$.