IV054 Coding, Cryptography and Cryptographic Protocols
2011 - Exercises VI.

1. Let $c = 56$ and $n = 143$. Using the Chinese Remainder Theorem, determine in detail all square roots of c mod n.
2. Consider the Rabin cryptosystem with $n = 189209$. You know that ciphertext $c = 9084$ decrypts as $w_1 = 1234$, $w_2 = 39593$, $w_3 = 187975$ and $w_4 = 149616$. Decrypt $c' = 85780$. Do not use brute force.
3. Let $p > 7$ be a prime such that none of the numbers 3, 5, 7 is a quadratic residue modulo p. Which of the integers 15, 21, 35, 105 are quadratic residues mod p? Explain your reasoning.
4. Consider the ElGamal cryptosystem with $p = 199999$, $q = 23793$ and $x = 894$. Let $r = 723$ and $w = 15131$. Perform encryption and decryption of the message w.
5. Calculate x using Shank's algorithm. Show all steps of the calculation.
$$5^x \equiv 112 \pmod{131}.$$
6. Let p be an odd prime. Determine the number of quadratic residues modulo p. Explain your reasoning.
7. Let $p = 503$, $q = 2$ and $x = 42$. Decrypt the ElGamal ciphertexts $c_1 = (4, 100)$ and $c_2 = (299, 457)$.
8. Consider the uniform distribution of birthdays in a 365-day year.
   (a) What is the probability that two people in the group of 45 people have a birthday on the same day?
   (b) How many people must be in group so that the probability is greater than 75%?