IV054 Coding, Cryptography and Cryptographic Protocols
2014 - Exercises VI.

1. Using Fermat's little theorem, determine an integer x such that $8^x \equiv 2 \pmod{23}$.

2. How many cars do you have to observe in order for the probability to be greater than 50% of observing at least two cars with the same first three symbols on their license plate? A car license plate consists of 7 symbols: there is a capital letter (A, ..., Z) in the second position, other positions are occupied with digits. Each symbol is equally probable.

3. Let p be an odd prime number and g be a primitive root modulo p. This means that the powers $1, g, g^2, \cdots, g^{p-2}$ are all distinct modulo p. Suppose m is an odd number. Prove that g^m is a quadratic nonresidue modulo p.

4. Suppose we know how to factorize large numbers and we find out that the private keys of the Rabin cryptosystem are $p = 163$ and $q = 307$. Decrypt the cryptotext "15244 33337". The message is a meaningful English word.

5. Let f, g be negligible functions. Prove the following:

   (a) f^k is negligible for any $k > 0, k \in \mathbb{R}$.

   (b) $f + g$ is negligible.

   (You can use the alternative definition of negligible function: it is enough for the function to be smaller than n^{-c} (for every positive integer c) rather than $\frac{1}{p(n)}$.)

6. Show that you can factorize efficiently if you have an oracle for finding square roots. Demonstrate by factorizing $n = 88416763$ in case the oracle tells you that the square roots of 51733469 (mod 88416763) are 50224876, 38191887, 22222, 88394541.

7. Using the Shank's algorithm find x such that

   $$88^x = 80 \pmod{107}$$

   and show all steps of the algorithm.

8. Consider the Rabin cryptosystem with $n = p^k q^s$ where $k,\ s > 1$.

   (a) How many possible plaintexts do we obtain after decryption?

   (b) Find a decryption of cryptotext $c = 14590$ using private keys $11^2 7^3 = 41503$.

   Hint: (Hensel's Lemma)
   If r_i is square root of $a \pmod{p^i}$ then

   $$r_{i+1} = r_i + tp^i$$

   is a square root of $a \pmod{p^{i+1}}$ where t is solution of

   $$t2r_i \equiv -C \pmod{p}$$

   and $C = \frac{r_i^2 - a}{p^i}$ (here always $p^i | r_i^2 - a$).