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

1. What is the probability that at least two students enrolled to the IV054 course (there are 82 students enrolled) are having birthday on the same day. Assume years are non-leap.

2. Ciphertext $c = 1764$ created by the Rabin cryptosystem with $n = 41989$ decrypts as both $m_1 = 41947$ and $m_2 = 1435$. Without factorization of n decrypt $c_2 = 6661$.

3. Consider the ElGamal cryptosystem with a public key (p, q, y) and a private key x.
   (a) Let $c = (a, b)$ be a cryptotext. Suppose that Eve can obtain a decryption of any cryptotext $c' \neq c$. Show that this enables her to decrypt c.
   (b) Let $c_1 = (a_1, b_1)$, $c_2 = (a_2, b_2)$ be obtained by encrypting messages $m_1 \neq m_2$, respectively, using the same public key. Encrypt some other message m'.

4. Which of the following functions $f : \mathbb{N} \to \mathbb{N}$ are negligible? Prove your answer.
   (a) $2^{-\sqrt{n}}$
   (b) $2^{-\sqrt{\log(n)}}$
   (c) $n^{-\log\log(n)}$

5. Let p be a prime number and g an integer. The Diffie-Hellman Problem is the problem of computing the value of $g^{ab} \pmod p$ from the known values of $g^a \pmod p$ and $g^b \pmod p$.
   Suppose that Eve has access to an oracle that decrypts arbitrary ElGamal ciphertexts encrypted using arbitrary ElGamal public keys. Prove that Eve can use the oracle to solve the Diffie-Hellman problem.

6. Calculate x in the following equation using the Shank's algorithm. Show all the steps of your calculation.
$$5^x = 27 \pmod{107}$$

7. Let p be an odd prime number and g be a primitive root modulo p. Suppose m is an odd number, prove that g^m is a quadratic nonresidue modulo p.