IV054 Coding, Cryptography and Cryptographic Protocols
2016 - Exercises V.

1. In the Blom's key pre-distribution protocol show that the key generated by A and B is the same, *i.e.* show that $K_{AB} = K_{BA}$.

2. Consider the RSA cryptosystem with $p = 43$, $q = 67$ and $d = 937$. Determine the public key and encrypt the plaintext 297435863215.

3. Suppose that you have eavesdropped the following message intended for your boss, Mr. Smith:
   "58495 was transferred to your personal bank account."
   You know that the number is the amount of money encrypted and that the RSA cryptosystem with $n = 198269$ was used. Later, you listened him complaining that he had obtained only 100$. Next week he received another message: "136892 was transferred to your personal bank account."
   What is the amount of money transferred to his bank account in this case?

4. Use the Rabin-Miller's Monte Carlo algorithm to decide whether 4537 is a prime. Use the numbers 623, 37 and 4001 as your random integers for the algorithm. State the accuracy of your result.

5. Consider the following set of RSA moduli, generated by an imperfect random prime number generator which is biased towards some numbers (some numbers appear with larger probability than others). Determine which of these moduli are secure. Do not use brute force factorization.

$$\{21427577, 33792547, 33811619, 33876551, 36249431,$$
$$39325051, 41204519, 43930871, 45170869, 47864099\}$$

6. Find all $n \in \mathbb{N}$ such that $\varphi(n) = 6$. Explain your reasoning.

7. Consider an RSA cryptosystem with public encryption key $e = 3$ and modulus of length 4096 bits where plaintexts are encrypted in blocks of length 1365 bits. Explain why this system is not secure.

8. Bob has sent the same message m to three of his friends using RSA cryptosystems. You know that Bob used public exponent $e = 3$ for each cryptosystem. You have intercepted the following ciphertexts: $c_1 = 284, c_2 = 278, c_3 = 338$. You also know the corresponding public moduli: $n_1 = 445, n_2 = 451, n_3 = 391$. Recover the message without factoring any of moduli.