IV054 Coding, Cryptography and Cryptographic Protocols
2015 - Exercises VI.

1. Consider the RSA cryptosystem with public modulus $n = 779$ and encryption exponent $e = 287$. You have obtained the following two pairs of (plaintext, cryptotext):

$$(445, 12),\ (312, 31).$$

Using this knowledge decrypt the cryptotext $c = 372$ without factoring the public modulus.

2. Consider the Blom's key pre-distribution protocol with $n = 5$ and $p = 17$. Let the public identifiers of users be $r_1 = 1$, $r_2 = 2$, $r_3 = 3$, $r_4 = 4$, $r_5 = 5$. Suppose you are the user 1 and your private keys are $a_1 = 3$, $b_1 = 7$.

   (a) Find the shared key with user 5.

   (b) Can you use your secret keys a_1 and b_1 to find secret keys of other users?

   (c) Suppose you also learned that $a_2 = 14$. Find all secret key pairs $(a_i, b_i), i \in \{2, 3, 4, 5\}$.

3. Consider we want to set up the RSA cryptosystem in a network of n users. How many prime numbers should be generated? Consider we want to reduce this number with generating less of them and making combinations of these primes to set up each user's key. How does that affect security?

4. Suppose the Goldbach's conjecture is true. Show that every odd integer $n > 11$ can be written as a sum of 5 prime numbers.
(*Goldbach's conjecture:* Every even integer greater than 2 can be expressed as the sum of two primes.)

5. Let $n = pq$ where p, q are primes with $p > q$.

   (a) Show that $p - q = \sqrt{(p+q)^2 - 4n}$.

   (b) Express p and q in terms of n and $\varphi(n)$.

6. Use the Rabin-Miller's Monte Carlo algorithm for prime recognition to decide whether the number $n = 5101$ is prime and state the accuracy of your result. Use the numbers $x_1 = 1720$, $x_2 = 551$ and $x_3 = 97$ as the random integers used by the algorithm.

7. Find (by hand) all natural numbers x such that $4^x \equiv 16 \pmod{105}$.