IV054 Coding, Cryptography and Cryptographic Protocols
2018 - Exercises VI.

1. Use the Chinese remainder theorem to solve the following congruences:

$$\begin{aligned} x &\equiv 3 \mod 7 \\ x &\equiv 5 \mod 11 \\ x &\equiv 7 \mod 13 \end{aligned}$$

   Show computation steps in detail.

2. Alice and Bob use the ElGamal cryptosystem. Alice generated the public key $(p, q, y) = (1021, 2, 512)$ and Bob sent her cryptotext $c_1 = (853, 342)$. Alice later publicly revealed that the message was $m_1 = 123$. After that Bob sent her another cryptotext $c_2 = (853, 222)$. Decrypt c_2. What did Bob wrong?

3. Consider a cryptographic hash function with 25 bits long output. What is the minimal number of random guesses you need to perform to find a collision with probability at least 0.7?

4. (a) Encrypt your UČO using the Rabin cryptosystem with $n = 698069$.
   (b) Calculate all four possible decryptions of the ciphertext you calculated, with the knowledge that $n = 887 \times 787$.

5. (a) Prove that if $f(n)$ is a negligible function and $g(n)$ is not a negligible function, then $g(n) - f(n)$ is not negligible.
   (b) Decide whether the function $e^{1/n} - 1$ is negligible. Prove your answer.

6. Let $p = 83$, $q = 50$ and $y = 16$. Use Shanks' baby-step giant-step algorithm to find the discrete logarithm $\log_q y \mod p$.

7. (a) What is the probability that at least *two* students attending IV054 course have the same birthday?
   (b) What is the probability that at least *three* students attending IV054 course share the same birthday?

   (42 students attend IV054 in 2018.)