IV054 Coding, Cryptography and Cryptographic Protocols
2020 - Exercises V.

1. *(4 points)*
   (a) Encrypt your UČO (personal identification number) with the RSA cryptosystem with public key $e = 11$ and $n = 1147$. Then, with the knowledge $31 \times 37 = 1147$, show the decryption steps.
   (b) Encrypt encrypt the binary expansion of the last two digits of your UČO (this is a binary vector of length 7) with Knapsack cryptosystem with public key $X' = (393, 396, 140, 152, 435, 486, 323)$. Then, with the knowledge $u = 131$ and $m = 521$, show the decryption steps.

2. *(3 points)* You have purchased a device that generates RSA keys. The device generated the following moduli:
   $$65201327, 134635439, 122176133, 122237737 \text{ and } 99633161.$$
   Can you consider them safe (omit the fact that they are small)? If not, try to factorize them without using brute force. Explain.

3. *(3 points)* You are given $n = 633917$, for which you know that it is a product of two primes and $phi(n) = 632256$. Find factors of n without using brute force. Explain your calculations.

4. *(5 points)* Show that if $f : \{0,1\}^n \to \{0,1\}^n$ is a strongly one-way function then $g_c : \{0,1\}^{2n} \to \{0,1\}^{2n}$, $g_c(x_1 \parallel x_2) = c \parallel f(x_1)$, where $x_1, x_2 \in \{0,1\}^n$ and $\parallel$ is concatenation, is also a strongly one-way function for any constant parameter $c \in \{0,1\}^n$.

5. *(5 points)* Consider the McEliece cryptosystem with
   $$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \quad P = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$
   (a) Compute the public key G'.
   (b) Using the error vector $e = 0000100$ encode the message $w = 1010$.
   (c) Decode cryptotext $c = 1100110$.

6. *(5 points)* Consider a Galois field $\mathrm{GF}(2^n)$, $n > 1$. Alice wants to securely send a message $m \in \mathrm{GF}(2^n)$ to Bob. They perform the following:
   i. Alice chooses e_A with $\gcd(e_A, 2^n - 1) = 1$, computes $A = m^{e_A}$ in $\mathrm{GF}(2^n)$ and sends A to Bob.
   ii. Bob chooses e_B with $\gcd(e_B, 2^n - 1) = 1$, computes $B = A^{e_B}$ in $\mathrm{GF}(2^n)$ and sends B to Alice.

   Show how Alice and Bob continue their communication and how can Bob recover m. Prove your answer.