Selected Topics in Cryptography
HOMEWORK #1, JURAJ BELOHOREC
Deadline: October 24, midnight

Basic rules for submitting your homework:

- *the file has to be named: "firstname-lastname-HW1.pdf"*
- *put your name on the top of each page*
- *number the pages*
- *clearly mark which problem is being solved and list the solutions in the order of the problems from the assignment*
- *write the solutions carefully providing sufficient details; when in doubt, write more*
- *HW is to be turned in via* moodle *in the* pdf *format*
- *late homeworks only accepted in justified situations*

The total number of points in this HW is greater than 50 points. You cannot receive more than 50 points, so you may choose to just solve problems worth 50 pts. However, if you choose to do that, and some of your solutions turn out wrong or imperfect, you will loose points and will not receive the full 50 pts. On the other hand, if you choose to solve problems worth more than 50 points, even with some mistakes in some of the problems you may get enough done to earn the maximum of 50 points.

1. (10 pts) **Cardan's Rectangular Grid Encryption**

   Recall that for Cardan's Rectangular Grid Encryption one needs to use a $2n \times 2n$ grid with certain windows cut out. The encryption protocol for a plain text of $4n^2$ characters is to place the grid in the first position, write the message from the left upper open window (one character per window), then turn the grid by 90 degrees, while keeping it in place, continue filling the windows with the message, and repeat that two more times. After four uses of the grid, the entire message is written in a $2n \times 2n$ grid.

   As a simple example, consider the grid:

X			
			X
		X	
	X		

   where the windows marked 'X' are cut out.

   Suppose the message to be sent is the message

   THEREWILLBEPARTY

   The encryption will then look like this:

   1. First we write into the first 4 cut-out windows:

T			
			H
		E	
	R		

   2. Then we turn the grid by 90 degrees to the right, and fill in the next part of the message:

			E
W			
	I		
		L	

   3. Turn again by 90 degrees to the right:

		L	
	B		
E			
			P

   3. And finally, turning again by 90 degrees to the right:

	A		
		R	
			T
Y			

The final encrypted text will look like this:

T	A	L	E
W	B	R	H
E	I	E	T
Y	R	L	P

a) Describe a general method for constructing $2n \times 2n$ rectangular grids to be used for this type of protocol.

b) How many different $2n \times 2n$ rectangular grids are there that have the property that the uppermost left window is cut out?

c) Argue that Cardan's grid encryption is a permutation encryption. Given a $2n \times 2n$ rectangular grid, find the corresponding permutation to be used to obtain the same encrypted text. What are the notable properties of all permutations asscociated with Cardan's grid encryption?

d) Design a quick attack on Cardan's grid encryption protocol where you assume that the encrypted plaintext is a 'normal' text. The description of your attack may be quite informal, but it should be more efficient than trying all the permutations.

2. (10 pts) Consider the 'vocabulary' encryption defined via a bijection from ψ from the 26 symbols of the English alphabet to the 26 symbols of the English alphabet.

a) Suppose you know the cycle structure of ψ. Can that speed up an attack? If it can, how?

b) Suppose you know the order of ψ. Can that speed up an attack? If it can, how?

c) Are there 'safer' permutations and 'less safe' permutations?

3. (10 pts) Consider the following protocol:

Let $\varphi : \mathcal{E} \to \mathcal{P}_3(\mathcal{A})$ be an injection from the set of characters of the English alphabet into the set of ordered triples of some alphabet $\mathcal{A}$ having the additional property $\varphi(a_i) \cap \varphi(a_j) = \emptyset$, for all $i \neq j$. Let $p : \mathcal{E} \to \mathbb{R}^3$, $p(a_i) = (p_1, p_2, p_3)$, $0 \leq p_i \leq 1$ a $p_1 + p_2 + p_3 = 1$ and let E be the encryption function, which associates $a_i \in \mathcal{E}$ with the j-th element $\varphi(a_i)_j$ of $\varphi(a_i)$ with probability $p(a_i)_j$ (thus the element a_i is sometimes encrypted with $\varphi(a_i)_1$, sometimes with $\varphi(a_i)_2$, and sometimes with $\varphi(a_i)_3$; with the prescribed probabilities).

a) Suggest a frequency attack for the case $p_1 = p_2 = p_3 = \frac{1}{3}$, for all $a_i \in \mathcal{E}$.

b) Design a frequency attack for general probabilities description $p(a_i)$ for all $a_i \in \mathcal{E}$; assuming you know the probability distributions $p(a_i)$ for all $a_i \in \mathcal{E}$.

c) Design a frequency attack for general probabilities description $p(a_i)$ for all $a_i \in \mathcal{E}$; for the case when you do not know the probability distributions $p(a_i)$.

4. (20 pts) Solve the following exercises from Chapter 10, Introduction to Cryptography:

Problems 10.1:

$$2, 4, 5, 6, 7, 11, 12, 13$$

5. (10 pts) Decrypt the following text that has been generated using substitution cipher if you know that the corresponding plaintext was in English:

lnikpybvgbojihpkkiejijjiylpbvvxkeawlnialnielneiibepjlalivpbylxcijakgbojbvplxlnikpybvgbojiakbl
npymoyhiecpyjiwiemijlebyjgiyhjaolakbyhpykvoiygijlnialniekoyhbwiylbvgbojijakplkpybvgbojij
oyhiecpylnialnielne

6. (10 pts) Decrypt the following text that has been generated using Hill's cipher with a 2×2 matrix if you know that the corresponding plaintext was in English:

ybonstevgfkactdiwttfcxoedymbgfkaosbodgoaqmwtluecybhacxwpvqchsddsodstmyqevznsj
gdsnawcgfqyybfhoedymbgfxooxjeafkwwtbtuawpgfxupqwpgfodertsfmnsluqiqmmvfovzjgjm
sudjknykwplsduoedymbgfxosadbfmkwscoedymbgfmjrc

7. (10 pts) Read Stinson's text in the cryptanalysis of the Vigenère cipher (Section 2.2.3), and determine the length of the key used in the following text:

lsyxxvvtcjawraurluhkypbobsxfqqhhwmyruhdlzrxmjwfhvvyqiehlewbuhbuuqlydjtqkhrqrbvrk
kyfrqreszrplesmurabjjvwgqszrxmjwfhvhdtqkhqhjdlrmitofrmjnkhqsigxvhcesqkhrufojxlusqv
qdyleerqysdfrtdyolhrijihfsjmbvdluulolb