Midterm Exam

1. (a) Describe the simple substitution cipher. **(2 points)**

   (b) Alice and Bob are students of the BSM. They would like to use a simple substitution cipher on the English alphabet with the restriction that $\{\texttt{a}, \texttt{e}, \texttt{i}\}$ is mapped to itself, and also $\{\texttt{o}, \texttt{u}\}$ is mapped to itself. (This is important for them, because occasionally they want to use Hungarian accents and dots, and this is the simplest if they encrypt accented and dotted characters to others which may have the same accents and dots.) How many possible keys are there, if they do not impose further conditions? **(4 points)**

2. (a) Define groups. **(2 points)**

   (b) What are the subgroups of the multiplicative group $\mathbf{Z}_8^\times$? **(4 points)**

3. (a) Describe the Diffie-Hellman key exchange (over the group $\mathbf{F}_p^\times$). **(2 points)**

   (b) Alice, Bob and Charles choose publicly a large prime p. They would like to agree on a residue class modulo p, but they know that their communication is monitored by an eavesdropper. How could they do that in spirit of Diffie-Hellman? **(4 points)**

4. (a) Describe the chosen plaintext attack. **(2 points)**

   (b) Consider the following symmetric cryptosystem: fix a large prime number p, and let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbf{F}_p$, $e_k(m) \equiv km \bmod p$. Prove that this cryptosystem is vulnerable to the chosen plaintext attack. **(4 points)**