Exercise 1 – Introduction to Cryptography 89-656

Due Date: October 28, 2018

Honour code: You are expected to do your homework by yourself (individually). It goes without saying that you can and should consult with other students when you have difficulties. However, it is in your best interest to first try to solve the problems without any help. In any case, you must write your solutions by yourself.

Exercise 1: Decrypt the following ciphertext, encrypted with a substitution cipher:

```
JGRMQOYGHMVBJWRWQFPWHGFFDQGFPFZRKBEEBJIZQQOCIBZKLFAFGQVFZFWWE
OGWOPFGFHWOLPHLRLOLFDMFGQWBLWBWQOLKFWBYLBLYLFSFLJGRMQBOLWJVFP
FWQVHQWFFPQOQVFPQOCFPOGFWFJIGFQVHLHLROQVFGWJVFPFOLFHGQVQVFILE
OGQILHQFQGIQVVOSFAFGBWQVHQWIJVWJVFPFWHGFIWIHZZRQGBABHZQOCGFHX
```

Exercise 2: Analyze the security of the shift, substitution and Vigenere ciphers under known-plaintext and chosen-plaintext attacks. How much known or chosen plaintext is needed for the adversary to completely recover the key. Discuss the difference between the known and chosen plaintext cases (if there is any).

Exercise 3: Provide a formal proof that if the Shift Cipher is modified so that a different key is chosen for each letter sent, then the result is a perfectly-secret encryption scheme.

Exercise 4: Modify the one-time pad so that keys are used twice. That is, let the key-space $\mathcal{K}$ be such that first a key $\tilde{k}$ is uniformly chosen from $\{0,1\}^{\ell/2}$ and then the key is defined by $k = \tilde{k}\|\tilde{k}$, where "$\|$" denotes concatenation. (In addition, define $\mathcal{M} = \mathcal{C} = \{0,1\}^{\ell}$.) Prove that this scheme is not perfectly secure.

Exercise 5: Prove or refute: If an encryption scheme is perfectly secure, then for every probability distribution over $\mathcal{M}$ every $m_0, m_1 \in \mathcal{M}$ and for every $c \in \mathcal{C}$,

$$\Pr[\mathcal{M} = m_0 \mid \mathcal{C} = c] = \Pr[\mathcal{M} = m_1 \mid \mathcal{C} = c].$$

Assume that the distributions over $\mathcal{M}$ and $\mathcal{C}$ assign non-zero probabilities to all elements.

Exercise 6: It is clear that if the key k in the one-time pad scheme is the string of ℓ zeroes (i.e., $k = 0^{\ell}$), then the ciphertext equals the plaintext. That is, encryption does nothing. Due to this, it has been suggested that the one-time pad scheme be modified so that the key space $\mathcal{K}$ includes all strings of length ℓ except for 0^{ℓ}.

Analyze the security of the modified scheme (with a formal proof) and *explain* your answer on an intuitive level.