1. Consider the following encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$. The message space is $\mathcal{M} = \{0, \ldots, 9\}$. $\text{Gen}$ chooses a key uniformly at random from $\{0, \ldots, 9\}$. $\text{Enc}_k(m)$ returns $m + k \mod 10$. $\text{Dec}_k(c)$ returns $c - k \mod 10$.

Check for yourself (no need to submit) that this scheme $\Pi$ is perfectly secret. Then, for each of the variations below, determine whether the resulting scheme is perfectly secret or not, and formally prove your answer.

(a) (12 points) Original scheme $\Pi$ except that $\mathcal{M} = \{2, 3, 7\}$ (a smaller message space)

(b) (12 points) Original scheme $\Pi$ except that $\text{Gen}$ chooses a key uniformly at random from $\{0, \ldots, 10\}$ (a larger keyspace)

(c) (12 points) Original scheme $\Pi$ except $\text{Enc}$, $\text{Dec}$ now work over the integers, rather than mod 10. That is, $\text{Enc}_k(m) = m + k$, $\text{Dec}_k(c) = c - k$.

2. (22 points) Assume you’re given $\Pi^1 = (\text{Gen}^1, \text{Enc}^1, \text{Dec}^1)$ and $\Pi^2 = (\text{Gen}^2, \text{Enc}^2, \text{Dec}^2)$ that are perfectly secret encryption schemes for message spaces $\mathcal{M}^1$ and $\mathcal{M}^2$ respectively. Construct an encryption scheme $\widehat{\Pi} = (\widehat{\text{Gen}}, \widehat{\text{Enc}}, \widehat{\text{Dec}})$ which is perfectly secret for message space $\mathcal{M}^1 \cup \mathcal{M}^2$. Prove correctness and perfect secrecy of $\widehat{\Pi}$.

3. (22 pts) Recall from class: a scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ for message space $\mathcal{M}$ is perfectly secret for two messages if $\forall m_1, m_2, m'_1, m'_2 \in \mathcal{M}$, and $\forall c_1, c_2 \in \mathcal{C}$,

$$\Pr_{k \leftarrow \text{Gen}}[\text{Enc}_k(m_1) = c_1 \land \text{Enc}_k(m_2) = c_2] = \Pr_{k \leftarrow \text{Gen}}[\text{Enc}_k(m'_1) = c_1 \land \text{Enc}_k(m'_2) = c_2] \quad (1)$$

We showed that no encryption scheme can satisfy perfect secrecy for two messages. The intuition behind the proof was that if you encrypt two messages with the same key, at least a little bit of information about the messages must be leaked. In particular, if it’s a pair of identical messages, there’s non-zero probability that they result in identical ciphertexts, while different messages have zero probability of this happening.

Your assignment: Suppose we modify the definition to consider only pairs of distinct messages. That is, we say that the scheme is perfectly secret for two distinct messages if equation (1) holds $\forall m_1, m_2, m'_1, m'_2 \in \mathcal{M}$ satisfying $m_1 \neq m_2, m'_1 \neq m'_2$, and $\forall c_1, c_2 \in \mathcal{C}$.

Show an encryption scheme that satisfies this definition. (Hint: your scheme does not have to be efficient).

4. (a) (12 pts) Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be any encryption scheme for message space $\mathcal{M}$. Prove that there is an encryption scheme $\Pi' = (\text{Gen}', \text{Enc}', \text{Dec}')$ for $\mathcal{M}$, such that $\text{Enc}'$ is deterministic (as a function of the key and the message), and

$$\Pr_{k' \leftarrow \text{Gen}'}[\text{Enc}'_k(m) = c] = \Pr_{k \leftarrow \text{Gen}}[\text{Enc}_k(m) = c]$$

for all $m$ and $c$. 

COMS W4261, Introduction to Cryptography, Homework 1, p. 1
(b) In part (a) you proved that for any encryption scheme there’s another one that maps messages to ciphertexts in exactly the same way, but where the encryption algorithm is deterministic.

This may seem to suggest that we can always assume without loss of generality that the encryption scheme is deterministic. However, this “lesson” is wrong; we already hinted, and will see again later in class, that encryption must be randomized if you want to achieve any reasonable level of security.

Can you think of how to settle these seemingly contradictory conclusions?