# Cryptography: HW1

Due electronically on Friday 15 Jan

1. Alice is using one-time pad and notices that when her key is the all-zeroes string $k = 0^\lambda$, then $\mathsf{Enc}(k, m) = m$ and her message is sent in the clear! To avoid this problem, she decides to modify KeyGen to choose a key uniformly from $\{0,1\}^\lambda \setminus \{0^\lambda\}$. In this way, her plaintext is never sent in the clear.

   Does the modified scheme still have one-time secrecy? Justify your answer.

2. Show that the following encryption scheme does **not** have one-time secrecy, by constructing a program that distinguishes the two relevant libraries from the one-time secrecy definition.

| | | |
|---|---|---|
| $\mathcal{K} = \mathbb{Z}_{10}$ | KeyGen: | Enc$(k, m)$: |
| $\mathcal{M} = \mathbb{Z}_{10}$ | $k \leftarrow \mathbb{Z}_{10}$ | return $k \times m \,\%\, 10$ |
| $\mathcal{C} = \mathbb{Z}_{10}$ | return $k$ | |

3. Consider the following encryption scheme:

| | | | |
|---|---|---|---|
| $\mathcal{K} = \mathbb{Z}_n$ | KeyGen: | Enc$(k, m)$: | Dec$(k, c)$: |
| $\mathcal{M} = \mathbb{Z}_n$ | $k \leftarrow \mathbb{Z}_n$ | return $(k + m) \,\%\, n$ | ?? |
| $\mathcal{C} = \mathbb{Z}_n$ | return $k$ | | |

   (a) Fill in the details of the Dec algorithm so that the scheme satisfies correctness.

   (b) Prove that the scheme satisfies one-time secrecy.

4. Suppose there are 9 people on an important committee: Alice, Bob, Carol, David, Eve, Frank, Gina, Harold, & Irene. Alice, Bob & Carol form a subcommittee; David, Eve & Frank form another subcommittee; and Gina, Harold & Irene form another subcommittee.

   Suggest how a dealer can share a secret so that it can only be opened when a majority of each subcommittee is present. Describe why a 6-out-of-9 threshold secret-sharing scheme does **not** suffice.

   You do not have to give a formal proof, but please give an informal argument about why every unauthorized set of users has no information about the secret.