1. State the last (or, one but last) definition given in class for secure encryption.

**Answer.**

An encryption scheme is perfectly secret if,

(a) for every probability distribution over $M$, for every message $m \in M$ and every ciphertext $c \in C$ we have: $Pr[M = m|C = c] = Pr[M = m]$.

(b) for every probability distribution over $M$, for every message $m \in M$ and every ciphertext $c \in C$ we have: $Pr[C = c|M = m] = Pr[C = c]$.

(c) for every probability distribution over $M$, for every $m_0, m_1 \in M$ and every $c \in C$ we have: $Pr[C = c|M = m_0] = Pr[C = c|M = m_1]$.

Here we only consider distributions that assign non-zero probabilities to all $m \in M, \ c \in C$.

Alternatively, the encryption scheme $\Pi = (Gen, Enc, Dec)$ is perfectly secret if for every PPT adversary $A$ it holds that: $Pr[PrivK^{eav}(A, \Pi) = 1] = 0.5$.

2. The One-time Pad is used for encryption.

Let $m, m' \in M$ be distinct messages, $k \in K$ be a key (all binary strings of length $\ell$). It is proposed to use the same key $k$ to encrypt both $m$ and $m'$. (At the end of WWII, the Soviet Union ran out of keypads and started re-using earlier ones).

**If this were allowed then:**

Show that the One-time Pad is not a secure encryption scheme according to the definition you gave above.

(Assume that the adversary uses a ciphertext only attack)

**Answer.**

Let $c = k \oplus m, \ c' = k \oplus m'$.

Then $c \oplus c' = k \oplus m \oplus k \oplus m' = (k \oplus k) \oplus (m \oplus m') = m \oplus m'$.

So the adversary can derive a function $(m \oplus m')$ of the plaintexts $m, m'$ by combining the ciphertexts $c, c'$.

Therefore the encryption scheme is not secure.