Problem Set 2—Solutions

1. This is false—do you see why?

2. (a) The scheme is not perfectly secret. To see this, we can use the equivalent definition of perfect secrecy given by Equation (2.1). If the message is 0, then the ciphertext is 0 if and only if \( k \in \{0, 5\} \). So \( \Pr[\text{Enc}_K(0) = 0] = 1/3 \). On the other hand, if the message is 1, then the ciphertext is 0 if and only if \( k = 4 \). So

\[
\Pr[\text{Enc}_K(1) = 0] = 1/6 \neq \Pr[\text{Enc}_K(0) = 0],
\]

and so the scheme is not perfectly secret.

(b) One can prove that this is perfectly secret by analogy with the one-time pad. (Essentially the final bit of the message is being ignored here, since it is always 0.)

3. No, the modified scheme cannot be perfectly secret since the message space is larger than the key space. If this modified scheme is used then when the attacker observes a ciphertext \( c \), the attacker learns that the message is not equal to \( c \), which is information it did not (necessarily) have before.

4. (a) Say \( \text{aab} \) is encrypted to give ciphertext \( c \). What is the probability that the first and second characters of \( c \) are equal? When \( t = 1 \) (which occurs 1/3 of the time) this always happens. When \( t \in \{2, 3\} \) this happens only if the first and second characters of the key are equal, which occurs with probability 1/26. So

\[
\Pr[\mathcal{A} \text{ outputs 0 } | \text{ } m_0 \text{ is encrypted}] = \frac{1}{3} + \frac{2}{3} \cdot \frac{1}{26} \approx 0.359.
\]

If instead \( \text{abb} \) is encrypted, then the first and second characters of \( c \) can never be equal when \( t = 1 \), but are equal with probability 1/26 when \( t \in \{2, 3\} \). Thus,

\[
\Pr[\mathcal{A} \text{ outputs 0 } | \text{ } m_1 \text{ is encrypted}] = \frac{2}{3} \cdot \frac{1}{26} \approx 0.026.
\]

We therefore have

\[
\Pr[\text{Priv}_{K_{s, k}}^\text{adv} = 1] = \frac{1}{2} \cdot \Pr[\mathcal{A} \text{ outputs 0 } | \text{ } m_0 \text{ is encrypted}] + \frac{1}{2} \cdot \Pr[\mathcal{A} \text{ outputs 1 } | \text{ } m_1 \text{ is encrypted}]
\]

\[
\approx \frac{1}{2} \cdot 0.359 + \frac{1}{2} \cdot 0.974 \approx 0.667.
\]
(b) Consider the adversary $A'$ who outputs $m_0 = \text{aaa}$ and $m_1 = \text{abc}$ and outputs ‘0’ iff the first and second characters in the ciphertext $c$ are the same, or if the first and last characters in the ciphertext are the same. Call this event $E$.

Say \text{aaa} is encrypted. If $t \in \{1, 2\}$ then $E$ always happens. When $t = 3$ all characters in the ciphertext are uniform and independent; rather than calculate the probability of $E$ in this case let’s just call it $p$.

Say \text{abc} is encrypted. If $t = 1$ then $E$ never happens. When $t = 2$ the first and last characters of $c$ are never equal, but the first and second characters are equal with probability $1/26$. When $t = 3$ then all characters in the ciphertext are random and so $E$ occurs with probability $p$.

Putting everything together gives:

$$
\Pr[\text{PrivK}_{X', H} = 1] = \frac{1}{2} \cdot \Pr[A' \text{ outputs } 0 \mid m_0 \text{ is encrypted}] + \frac{1}{2} \cdot \Pr[A' \text{ outputs } 1 \mid m_1 \text{ is encrypted}] \\
= \frac{1}{2} \cdot \left( \frac{2}{3} + \frac{1}{3} \cdot p \right) + \frac{1}{2} \cdot \left( 1 - \left( \frac{1}{3} \cdot \frac{1}{26} + \frac{1}{3} \cdot p \right) \right) \approx 0.827.
$$

5. This is left as an exercise for the reader.

6. The main point here is that if $c_1 = c_2$ then the attacker knows with certainty that $m_1 = m_2$. And for any (stateless) scheme, the probability that $c_1 = c_2$ when $m_1 = m_2$ is non-zero. Details are left to the reader.

7. Let $m_0, m_1$ be as in the hint. By construction, an encryption of $m_0$ has length at most $q(n)$. But it is not hard to show that (with high probability) an encryption of $m_1$ will have length larger than $q(n)$, which leads to an easy attack.

8. The main point here is to define some reversible encoding that maps every message of length at most $\ell(n)$ to a message of length exactly $\ell(n) + 1$. (This can be done because $\sum_{i=1}^{\ell(n)} i < 2^{\ell(n)+1}$.) Details of such an encoding are left as an exercise for the reader. (It is quite easy to come up with an encoding of length $\ell(n) + \log \ell(n)$, which is also fine for solving the problem. It is a little harder to find an encoding of length $\ell(n) + 1$ bits.)

9. Consider the following distinguisher $D$: on input a string $y \in \{0, 1\}^{2n}$, parse it as $y = x_1 \parallel x_2$ with $x_1, x_2 \in \{0, 1\}^n$. Output 1 if and only if $x_1 = x_2$. Note that

$$
\Pr_{y \leftarrow \{0, 1\}^{2n}}[D(y) = 1] = 2^{-n}
$$

but $\Pr_{x \leftarrow \{0, 1\}^n}[D(G(x)) = 1] = 1$.

Here is the solution to part 1 of the graded (programming) assignment:

1. The XOR of these two ciphertexts, which is also the XOR of the underlying plaintexts, is 0101 0000. Since the second bit is a 1, we know that one of the two plaintext characters is a space, i.e., 0010 0000. And so the other plaintext must be 0111 0000, or $p$. But we don’t know which ciphertext corresponds to which.
2. Proceeding as before, we can deduce that either (1) the first and third plaintexts are a space, and the second is a q, or (2) the first and third plaintexts are a q, and the second is a space.

3. By XORing the first and second ciphertext, we learn that either the first or second plaintext is a space. By XORing the first and third ciphertext, we learn that either the first or third plaintext is a space. But at most one plaintext can be a space, since the three ciphertexts are all different! We thus conclude that the first plaintext is a space, and from that we can deduce that the second plaintext is a t and the third plaintext an e.