Introduction to Cryptography
Exercise Week 2 Solutions

Dr. Patrick Struck
patrick.struck@uni.kn

Leon Weingarten
leon.weingarten@uni.kn

Jonah Herr
jonah.herr@uni.kn

Exercise 1.
Consider the following scenario:

Alice wants to encrypt a message of length n using the One-Time Pad, but knows that it will be sent in the clear if the key k happens to be 0^n. To prevent that, she chooses a new random key until $k \neq 0^n$, and only then encrypts her message.

Prove that the resulting scheme is no longer perfectly secret, using

(a) Definition 2.3.

(b) Lemma 2.5. (Reminder: A scheme is perfectly secret if and only if, for every $m, m' \in \mathcal{M}$ and every $c \in \mathcal{C}$, Equation (2.1)

$$\mathsf{Pr}[\mathsf{Enc}_K(m) = c] = \mathsf{Pr}[\mathsf{Enc}_K(m') = c]$$

holds.)

Solution 1.
(a) Assume $\mathcal{M}$ is uniformly distributed. Given any ciphertext $c \in \mathcal{C}$ with $\mathsf{Pr}[C = c] > 0$, an adversary aware of the scheme (Kerckhoffs' principle!) can immediately deduce that $M \neq c$, thus for $m = c$

$$\mathsf{Pr}[M = m | C = c] = 0 \neq \frac{1}{2^n} = \mathsf{Pr}[M = m]$$

and therefore the scheme is not perfectly secret.

(b) For any fixed $c \in C$, we can choose $m = c$ and $m' \neq c$. Then

$$\mathsf{Pr}[\mathsf{Enc}_K(m) = c] = 0 \neq \frac{1}{2^n - 1} = \mathsf{Pr}[\mathsf{Enc}_K(m') = c]$$

and again, it follows that the scheme is not perfectly secret.

Exercise 2.
In each of the following schemes, $\mathsf{Enc}_k(m) = [m + k \mod 3]$. State in each case whether the scheme is perfectly secret, and justify your answers.

(a) The message space is $\mathcal{M} = \{0, 1\}$, and Gen chooses a uniform key from the key space $\mathcal{K} = \{0, 1\}$.

(b) The message space is $\mathcal{M} = \{0, 1, 2\}$, and Gen chooses a uniform key from the key space $\mathcal{K} = \{0, 1, 2\}$.

(c) The message space is $\mathcal{M} = \{0, 1\}$, and Gen chooses a uniform key from the key space $\mathcal{K} = \{0, 1, 2\}$.

Solution 2.
For all cases the ciphertext space is $\mathcal{C} = \{0, 1, 2\}$.

(a) The scheme is not perfectly secret.

Proof. For any probability distribution over $\mathcal{M}$ with $\mathsf{Pr}[M = 0] > 0$ and $\mathsf{Pr}[M = 1] > 0$ (the latter is to ensure $\mathsf{Pr}[C = 2] > 0$) we get

$$\mathsf{Pr}[M = 0 | C = 2] = 0 \neq \mathsf{Pr}[M = 0]$$

$\square$

(b) The scheme is perfectly secret.

Proof. Here we can use Shannon's theorem, since $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. The key is chosen uniformly and clearly, for any $m \in \mathcal{M}$ and $c \in \mathcal{C}$ there is exactly one key for which $\mathsf{Enc}_k(m) = c$, which is $k := c - m \mod 3$. $\square$

(c) The scheme is perfectly secret.

Proof. For arbitrary $c \in \mathcal{C}, m \in \mathcal{M}$ we have

$$\begin{aligned} \mathsf{Pr}[\mathsf{Enc}_K(m) = c] &= \mathsf{Pr}[m + K = c \mod 3] \\ &= \mathsf{Pr}[K = c - m \mod 3] \\ &= \frac{1}{3} \end{aligned}$$

where the first equation follows by definition of Enc and the second because Gen chooses keys uniformly. The probability is independent of the message, thus the scheme is perfectly secret, since Equation (2.1) is fulfilled. $\square$

Exercise 3.
What is the ciphertext that results when the plaintext `0x012345` (written in hex) is encrypted using the one-time pad with key `0xFFEEDD`?

Solution 3.
Recall that in hexadecimal notation, each digit represents exactly four bits. For example, `0x0`= 0000, `0x1`= 0001, ...,`0xF`= 1111. Therefore, we can just decode the hexadecimal representation of the plaintext and the key into binaries.

$$\texttt{0x012345} = 0000\,0001\,0010\,0011\,0100\,0101$$
$$\texttt{0xFFEEDD} = 1111\,1111\,1110\,1110\,1101\,1101.$$

XORing this yields

$$1111\,1110\,1100\,1111\,1001\,1000,$$

which translates in hex to `0xFECF98`.

Exercise* 4.
Recall the affine cipher from question 4 of the first exercise sheet. Assume that every key $(a, b) \in \mathcal{K}$ is chosen with equal probability $1/|\mathcal{K}|$.

(a) Show that for messages of length $n \geq 2$, this cipher is not perfectly secret.

(b) Prove that for messages of length $n = 1$, this cipher *is* perfectly secret.

Solution 4.

(a) Take the uniform distribution on $\mathcal{M}$ and choose $m = 0...0$ of length $n \geq 2$. Further, let $c = 10...0$ be the ciphertext of length n starting with a one and followed by $n-1$ zeros, and let $(a, b) \in \mathcal{K}$ the key which encrypts m to c, that is $\texttt{Enc}_{(a,b)}(m) = c$ (assuming such a key exists). Encrypting the first two letters of m yields the following system of equations:

$$1 \equiv a \cdot 0 + b \bmod 26,$$
$$0 \equiv a \cdot 0 + b \bmod 26,$$

which leads to $b \equiv 1$ and $b \equiv 0 \bmod 26$, which is clearly a contradiction. In particular, this means that there is no such key (a, b) that encrypts m to c and therefore,

$$\Pr[M = m \mid C = c] = 0 \neq \frac{1}{26^n} = \Pr[M = m]$$

for this particular choice of m and c.

Another possible argument is that for $n \geq 2$, we have $|\mathcal{M}| = 26^2 > 316 = |\mathcal{K}|$ (this was proven on the last exercise sheet), which contradicts Theorem 2.11.

(b) Take an arbitrary distribution on $\mathcal{M}$. It suffices to show that for every $m \in \mathbb{Z}_{26}$ and every $c \in \mathbb{Z}_{26}$, there is always the same number of possible keys (a, b) such that $c \equiv a \cdot m + b \bmod 26$. And indeed, for every pair (m, c) we can choose an arbitrary $a \in \mathbb{Z}_{26}$ with $\gcd(a, 26) = 1$, and define $b := c - a \cdot m \bmod 26$. It is easy to see that

$$\texttt{Enc}_{(a,c-a\cdot m)}(m) = a \cdot m + (c - a \cdot m) = c.$$

As there are $12 (= \varphi(26))$ possible choices for a, and every a corresponds to exactly one b (defined as above), we see that for every pair (m, c), there are 12 different keys (a, b) which encrypt m to c. Phrased differently, this means that for any given c, the probability that c is the ciphertext of a message m is equal for all messages m, namely $12/312 = 1/26$. Therefore, for every message $m \in \mathcal{M}$ and every ciphertext $c \in \mathcal{C}$,

$$\Pr[M = m \mid C = c] = \frac{1}{26} = \Pr[M = m],$$

(respectively $= 0$ for $\texttt{Pr}[M = m] = 0$) which proves perfect secrecy.

Exercise* 5.

In this problem we consider definitions of perfect secrecy for the encryption of *two* messages, using the same key. Here we consider distributions on pairs of messages from the message space $\mathcal{M}$; we let M_1, M_2 be random variables denoting the first and second message, respectively. (These random variables are not assumed to be independent.) We generate a (single) key k, sample a pair of messages (m_1, m_2) according to the given distribution, and then compute ciphertexts $c_1 \leftarrow \texttt{Enc}_k(m_1)$ and $c_2 \leftarrow \texttt{Enc}_k(m_2)$; this induces a distribution on pairs of ciphertexts and we let C_1, C_2 be the corresponding random variables.

(a) Say encryption scheme (`Gen, Enc, Dec`) is *perfectly secret for two messages* if for all distributions on $\mathcal{M} \times \mathcal{M}$, all $m_1, m_2 \in \mathcal{M}$, and all ciphertexts $c_1, c_2 \in \mathcal{C}$ with $\Pr[C_1 = c_1 \wedge C_2 = c_2] > 0$:

$$\Pr[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = \Pr[M_1 = m_1 \wedge M_2 = m_2]$$

Prove that *no* encryption scheme can satisfy this definition.

(b) Say encryption scheme (`Gen, Enc, Dec`) is *perfectly secret for two distinct messages* if for all distributions on $\mathcal{M} \times \mathcal{M}$ where the first and second messages are guaranteed to be different (i.e., distributions on pairs of *distinct* messages), for all $m_1, m_2 \in \mathcal{M}$ and for all ciphertexts $c_1, c_2 \in \mathcal{C}$ with $\Pr[C_1 = c_1 \wedge C_2 = c_2] > 0$:

$$\Pr[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = \Pr[M_1 = m_1 \wedge M_2 = m_2]$$

Give an encryption scheme that fulfills this property. Can you also prove it?

Hint: Think of permutations. For the proof, you may use Bayes theorem and the law of total probability.

Solution 5.

(a) Consider the uniform distribution over $\mathcal{M} \times \mathcal{M}$. We want to show that the equation above is not fulfilled for distinct $m_1, m_2 \in \mathcal{M}$ but equal $c_1, c_2 \in \mathcal{C}$, which proves the claim. Therefore, lets choose $m_1 \neq m_2$ and $c_1 = c_2$ with $\Pr[C_1 = c_1 \wedge C_2 = c_2] > 0$. As `Dec` is required to be deterministic (equal ciphertexts must be decrypted to equal messages when using the same key), we deduce that the original messages m_1, m_2 must be equal. Consequently, if we choose $m_1 \neq m_2$, we get

$$\Pr[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = 0 \neq \Pr[M_1 = m_1 \wedge M_2 = m_2].$$

(b) We define the key space $\mathcal{K}$ to be the set of all permutations on the message space $\mathcal{M}$. Then $|\mathcal{K}| = |\mathcal{M}|!$. We define the following cipher:

- `Gen` chooses a random permutation $\pi : \mathcal{M} \to \mathcal{M}$ from $\mathcal{K}$.
- $\texttt{Enc}_\pi(m)$ encrypts a message m by applying the permutation π to obtain the ciphertext $c = \pi(m)$. Note that this gives another element from the message space as ciphertext.
- $\texttt{Dec}_\pi(c)$ decrypts the ciphertext c by applying the inverse π^{-1} of the permutation π to the ciphertext $m = \pi^{-1}(c)$. (Note that with $\pi \in \mathcal{K}$ if and only if $\pi^{-1} \in \mathcal{K}$.)

It is clear that this scheme is correct. Next, we want to show that it is *perfectly secret for two distinct messages*. Consider an arbitrary distribution on the set of pairs of distinct messages from $\mathcal{M}$, and fix $m_1, m_2 \in \mathcal{M}$ and $c_1, c_2 \in \mathcal{C}$. Then there are $(|\mathcal{M}| - 2)!$ different permutations π with $\pi(m_1) = c_1, \pi(m_2) = c_2$ (Note that we can assume $|\mathcal{M}| > 1$, because otherwise there are no distinct m_1, m_2). Using Bayes Theorem, it follows that

$$
\begin{aligned}
&\Pr[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] \\
=&\frac{\Pr[C_1 = c_1 \wedge C_2 = c_2 \mid M_1 = m_1 \wedge M_2 = m_2] \cdot \Pr[M_1 = m_1 \wedge M_2 = m_2]}{\Pr[C_1 = c_1 \wedge C_2 = c_2]} \\
=&\frac{\Pr[\mathcal{K}(M_1) = c_1 \wedge \mathcal{K}(M_2) = c_2 \mid M_1 = m_1 \wedge M_2 = m_2] \cdot \Pr[M_1 = m_1 \wedge M_2 = m_2]}{\Pr[C_1 = c_1 \wedge C_2 = c_2]} \\
=&\frac{\Pr[\mathcal{K}(m_1) = c_1 \wedge \mathcal{K}(m_2) = c_2] \cdot \Pr[M_1 = m_1 \wedge M_2 = m_2]}{\Pr[C_1 = c_1 \wedge C_2 = c_2]} \\
=&\frac{(|\mathcal{M}| - 2)!}{|\mathcal{M}|!} \frac{\Pr[M_1 = m_1 \wedge M_2 = m_2]}{\Pr[C_1 = c_1 \wedge C_2 = c_2]} \\
=&\frac{\frac{(|\mathcal{M}|-2)!}{|\mathcal{M}|} \Pr[M_1 = m_1 \wedge M_2 = m_2]}{\sum\limits_{m_1, m_2 \in \mathcal{M}} \Pr[C_1 = c_1 \wedge C_2 = c_2 \mid M_1 = m_1 \wedge M_2 = m_2] \cdot \Pr[M_1 = m_1 \wedge M_2 = m_2]} \\
=&\frac{\frac{(|\mathcal{M}|-2)!}{|\mathcal{M}|} \Pr[M_1 = m_1 \wedge M_2 = m_2]}{\sum\limits_{m_1, m_2 \in \mathcal{M}} \frac{(|\mathcal{M}|-2)!}{|\mathcal{M}|} \cdot \Pr[M_1 = m_1 \wedge M_2 = m_2]} \\
=&\frac{\Pr[M_1 = m_1 \wedge M_2 = m_2]}{\sum\limits_{m_1, m_2 \in \mathcal{M}} \Pr[M_1 = m_1 \wedge M_2 = m_2]} \\
=&\frac{\Pr[M_1 = m_1 \wedge M_2 = m_2]}{1} = \Pr[M_1 = m_1 \wedge M_2 = m_2].
\end{aligned}
$$

This proves the claim.