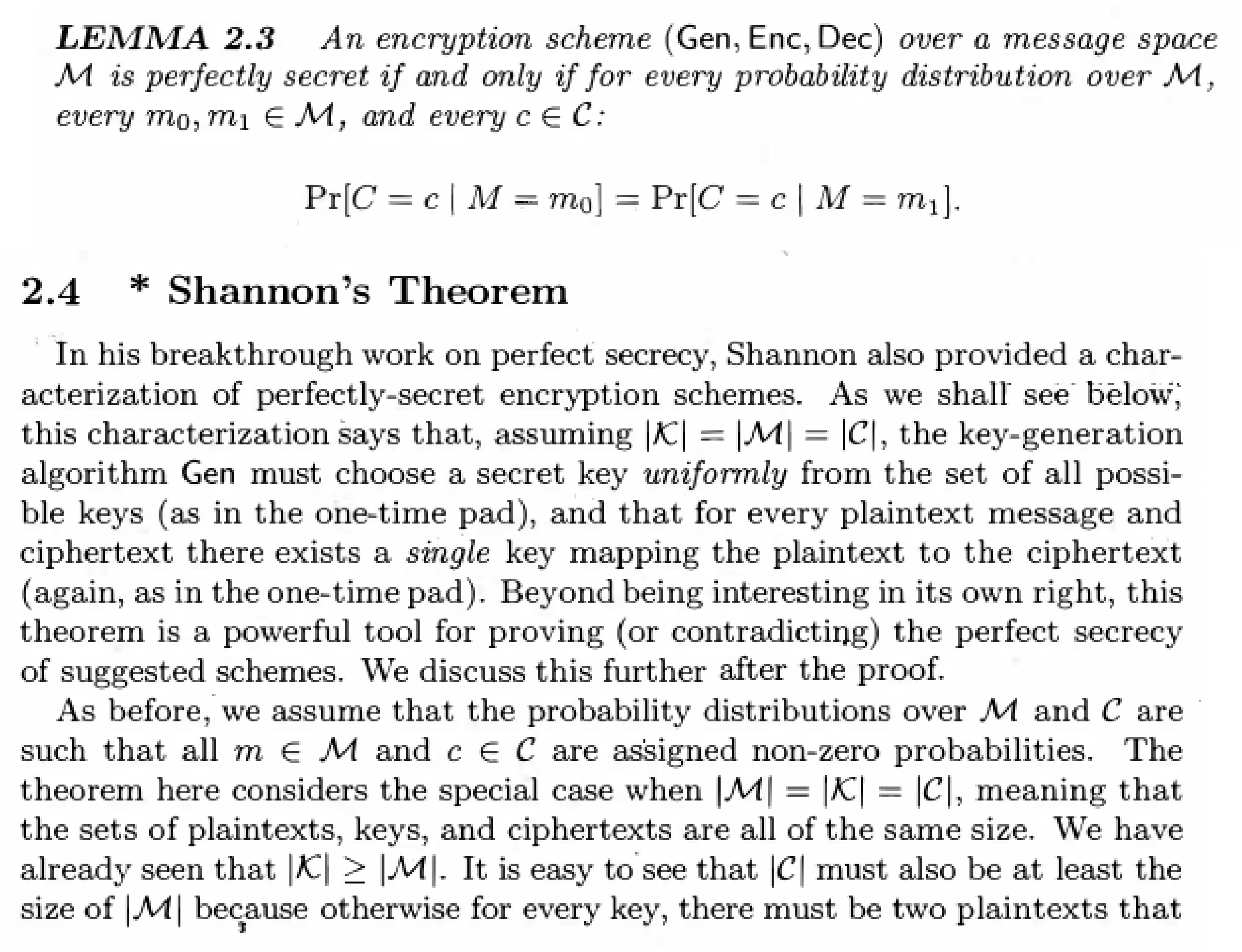
PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

**Criptografía y Seguridad Computacional - IIC3253**
**$1^{\text{er}}$ semestre - 2022**
**Lothar Droppelmann**

# Ayudantía 1 Solución

## Solución Pregunta 2

La demostración (siguiente página) está rescatada del libro Introduction to Modern Cryptography – Jonathan Katz.



***LEMMA 2.3*** *An encryption scheme* (Gen, Enc, Dec) *over a message space* $\mathcal{M}$ *is perfectly secret if and only if for every probability distribution over* $\mathcal{M}$*, every* $m_0, m_1 \in \mathcal{M}$*, and every* $c \in \mathcal{C}$*:*

$$\Pr[C = c \mid M = m_0] = \Pr[C = c \mid M = m_1].$$

## 2.4 * Shannon's Theorem

In his breakthrough work on perfect secrecy, Shannon also provided a characterization of perfectly-secret encryption schemes. As we shall see below, this characterization says that, assuming $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$, the key-generation algorithm Gen must choose a secret key *uniformly* from the set of all possible keys (as in the one-time pad), and that for every plaintext message and ciphertext there exists a *single* key mapping the plaintext to the ciphertext (again, as in the one-time pad). Beyond being interesting in its own right, this theorem is a powerful tool for proving (or contradicting) the perfect secrecy of suggested schemes. We discuss this further after the proof.

As before, we assume that the probability distributions over $\mathcal{M}$ and $\mathcal{C}$ are such that all $m \in \mathcal{M}$ and $c \in \mathcal{C}$ are assigned non-zero probabilities. The theorem here considers the special case when $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$, meaning that the sets of plaintexts, keys, and ciphertexts are all of the same size. We have already seen that $|\mathcal{K}| \geq |\mathcal{M}|$. It is easy to see that $|\mathcal{C}|$ must also be at least the size of $|\mathcal{M}|$ because otherwise for every key, there must be two plaintexts that are mapped to a single ciphertext (making it impossible to unambiguously decrypt). Therefore, in some sense, the case of $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$ is the "most efficient". We are now ready to state the theorem:

***THEOREM 2.8 (Shannon's theorem)*** *Let* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *be an encryption scheme over a message space* $\mathcal{M}$ *for which* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. *The scheme is perfectly secret if and only if:*

1. *Every key* $k \in \mathcal{K}$ *is chosen with equal probability* $1/|\mathcal{K}|$ *by algorithm* $\mathsf{Gen}$.
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$, *there exists a unique key* $k \in \mathcal{K}$ *such that* $\mathsf{Enc}_k(m)$ *outputs* $c$.

**PROOF** The intuition behind the proof of this theorem is as follows. First, if a scheme fulfills item (2) then a given ciphertext $c$ could be the result of encrypting any possible plaintext $m$ (this holds because for every $m$ there exists a key $k$ mapping it to $c$). Combining this with the fact that exactly one key maps each $m$ to $c$, and by item (1) each key is chosen with the same probability, perfect secrecy can be shown as in the case of the one-time pad. For the other direction, the intuition is that if $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$ then there must be exactly one key mapping each $m$ to each $c$. (Otherwise, either some $m$ is not mapped to a given $c$ contradicting perfect secrecy, or some $m$ is mapped by more than one key to $c$, resulting in another $m'$ not being mapped to $c$, again contradicting perfect secrecy.) Given this, it must hold that each key is chosen with equal probability or some plaintexts would be more likely than others, contradicting perfect secrecy. The formal proof follows.

Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be as in the theorem. For simplicity, we assume $\mathsf{Enc}$ is deterministic. We first prove that if $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is perfectly secret, then items (1) and (2) hold. As in the proof of Theorem 2.7, it is not hard to see that for every $m \in \mathcal{M}$ and $c \in \mathcal{C}$, there exists *at least one* key $k \in \mathcal{K}$ such that $\mathsf{Enc}_k(m) = c$. (Otherwise, $\Pr[M = m \mid C = c] = 0 \neq \Pr[M = m]$.) For a fixed $m$, consider now the set $\{\mathsf{Enc}_k(m)\}_{k \in \mathcal{K}}$. By what we have just said, $|\{\mathsf{Enc}_k(m)\}_{k \in \mathcal{K}}| \geq |\mathcal{C}|$ (because for every $c \in \mathcal{C}$ there exists a $k \in \mathcal{K}$ such that $\mathsf{Enc}_k(m) = c$). In addition, we trivially have $|\{\mathsf{Enc}_k(m)\}_{k \in \mathcal{K}}| \leq |\mathcal{C}|$. We conclude that

$$|\{\mathsf{Enc}_k(m)\}_{k \in \mathcal{K}}| = |\mathcal{C}|.$$

Since $|\mathcal{K}| = |\mathcal{C}|$, it follows that $|\{\mathsf{Enc}_k(m)\}_{k \in \mathcal{K}}| = |\mathcal{K}|$. This implies that there are no distinct keys $k_1, k_2 \in \mathcal{K}$ with $\mathsf{Enc}_{k_1}(m) = \mathsf{Enc}_{k_2}(m)$. Since $m$ was arbitrary, we see that for every $m$ and $c$, there exists *at most* one key $k \in \mathcal{K}$ such that $\mathsf{Enc}_k(m) = c$. Combining the above (i.e., the existence of at least one key and at most one key), we obtain item (2).

We proceed to show that for every $k \in \mathcal{K}$, $\Pr[K = k] = 1/|\mathcal{K}|$. Let $n = |\mathcal{K}|$ and $\mathcal{M} = \{m_1, \ldots, m_n\}$ (recall, $|\mathcal{M}| = |\mathcal{K}| = n$), and fix a ciphertext $c$. Then, we can label the keys $k_1, \ldots, k_n$ so that for every $i$ ($1 \leq i \leq n$) it holds that $\mathsf{Enc}_{k_i}(m_i) = c$. This labeling can be carried out because, as just shown, for every $c$ and $m_i$ there exists a *unique* key $k_i$ such that $\mathsf{Enc}_{k_i}(m_i) = c$, and furthermore these keys are distinct for distinct $m_i, m_j$ (since otherwise unambiguous decryption would be impossible). By perfect secrecy we have that for every $i$:

$$\begin{aligned}\Pr[M = m_i] &= \Pr[M = m_i \mid C = c] \\ &= \frac{\Pr[C = c \mid M = m_i] \cdot \Pr[M = m_i]}{\Pr[C = c]} \\ &= \frac{\Pr[K = k_i] \cdot \Pr[M = m_i]}{\Pr[C = c]},\end{aligned}$$

where the second equality is by Bayes' theorem and the third equality holds by the labeling above (i.e., $k_i$ is the unique key that maps $m_i$ to $c$). From the above, it follows that for every $i$,

$$\Pr[K = k_i] = \Pr[C = c].$$

Therefore, for every $i$ and $j$, $\Pr[K = k_i] = \Pr[C = c] = \Pr[K = k_j]$ and so all keys are chosen with the same probability. We conclude that keys are chosen according to the uniform distribution. That is, for every $k$, $\Pr[K = k_i] = 1/|\mathcal{K}|$ as required.

We now prove the other direction of the theorem. Assume that every key is obtained with probability $1/|\mathcal{K}|$ and that for every $m \in \mathcal{M}$ and $c \in \mathcal{C}$ there is a unique key $k \in \mathcal{K}$ such that $\mathsf{Enc}_k(m) = c$. This immediately implies that for every $m$ and $c$,

$$\Pr[C = c \mid M = m] = \frac{1}{|\mathcal{K}|}$$

irrespective of the probability distribution over $\mathcal{M}$. Thus, for every probability distribution over $\mathcal{M}$, every $m, m' \in \mathcal{M}$, and every $c \in \mathcal{C}$ we have

$$\Pr[C = c \mid M = m] = \frac{1}{|\mathcal{K}|} = \Pr[C = c \mid M = m'],$$

and so by Lemma 2.3 the encryption scheme is perfectly secret. ■