1 One-time-pad

Write a program that achieves the following: It takes as input two ciphertexts $c_1$ and $c_2$ of the same length. Both are expected to be the encryption of a single word $m_1, m_2$ using the one-time-pad. To produce the ciphertexts, the same key has been used. The program then finds $m_1$ and $m_2$.

Consider the following ciphertexts: $c_1 = 4A5C45492449552A$, $c_2 = 5A47534D35525F20$ (eight bytes each, presented in hex). Figure out the plaintexts using your program.

Solution

In Python. The function split_xor is the main algorithm.

Running the program otp-xor.py given on the website, we get that $m_0 = \text{question}$ and $m_1 = \text{answered}$ (or vice versa).

2 Perfect secrecy

Show that there is no encryption scheme that has perfect secrecy and allows us to reuse the key. More precisely, show that there is no encryption scheme $E$ that satisfies the following definition (and that can be decrypted):

**Definition 1 (Perfect secrecy with key reuse)** Let $K$ be the set of keys, let $M$ be the set of messages, and let $E$ be the encryption algorithm (possibly randomized) of an encryption scheme. We say the encryption scheme has perfect secrecy with key reuse iff for all $n$, and all $m_0^{(1)}, \ldots, m_0^{(n)}, m_1^{(1)}, \ldots, m_1^{(n)} \in M$ and for all $c_1, \ldots, c_n$, we have that

$$\Pr[(c_1, \ldots, c_n) = (c'_1, \ldots, c'_n) : k \xleftarrow{} K, c'_1 \leftarrow E(k, m_0^{(1)}), \ldots, c'_n \leftarrow E(k, m_0^{(n)})] = \Pr[(c_1, \ldots, c_n) = (c'_1, \ldots, c'_n) : k \xleftarrow{} K, c'_1 \leftarrow E(k, m_1^{(1)}), \ldots, c'_n \leftarrow E(k, m_1^{(n)})]$$

Solution

Assume there is an encryption scheme $E$ satisfying [Definition 1]. Let $n \geq 1$ be an integer such that $|M|^n > |K|$. (We assume $|M| \geq 2$ here.) We construct an encryption scheme $E'$ for messages in $M' := M^n: E'(k, (m_1, \ldots, m_n)) := (E(k, m_1), \ldots, E(k, m_n))$.

That is, to encrypt a message that consists of $n$ blocks in $M$, we simply encrypt each block individually with $E$ (using the same key for all blocks).

Now $E'$ has a message space $M'$ that is bigger than its key space $K$. ($|M'| = |M^n| = |M|^n > |K|$.) And $E'$ still has perfect secrecy. That can be seen as follows: For any ciphertext $c = (c_1, \ldots, c_n)$ of $E'$ and any two messages $m_0 = (m_0^{(1)}, \ldots, m_0^{(n)})$ and
\[ m_1 = (m_1^{(1)}, \ldots, m_1^{(n)}) \] in the message space \( M' \) of \( E' \), we have

\[
\Pr[c = c' : k \overset{\$}{\leftarrow} K, c' \leftarrow E'(k, m_0)] \\
= \Pr[(c_1, \ldots, c_n) = (c'_1, \ldots, c'_n) : k \overset{\$}{\leftarrow} K, c'_1 \leftarrow E(k, m_1^{(1)}), \ldots, c'_n \leftarrow E(k, m_1^{(n)})] \\
\overset{(*)}{=} \Pr[(c_1, \ldots, c_n) = (c'_1, \ldots, c'_n) : k \overset{\$}{\leftarrow} K, c'_1 \leftarrow E(k, m_0^{(1)}), \ldots, c'_n \leftarrow E(k, m_0^{(n)})] \\
= \Pr[c = c' : k \overset{\$}{\leftarrow} K, c' \leftarrow E'(k, m_1)].
\]

Here \((*)\) comes from the Definition [1].

Thus \( E' \) has perfect secrecy by the definition of perfect secrecy.

Summarizing, we have constructed an encryption scheme \( E' \) with perfect secrecy and with message space \( M' \) bigger than its key space. That is impossible according to the result proved in lecture.. Thus the assumption that an encryption scheme \( E \) satisfying [Definition 1] exists must be false.