Problem 2

Re-Using a One-Time Pad

Solution

Part A

If we assume they have the same encrypting pad, then the first ciphertext is $c_1 = m_1 \oplus p$, and the second is $c_2 = m_1 \oplus p$. From this, we can do $c_1 \oplus c_2 = (m_1 \oplus p) \oplus (m_2 \oplus p) = m_1 \oplus m_2$. Since we know that each message is a 12-character English word, we can iterate through all such words for m_1, and see if $m_1 \oplus (m_1 \oplus m_2) = m_2$ is a valid English word. We can similarly do this for m_2. Using this method we determined the first message is "intelligence" and the second is "cryptography". The pad used to encrypt them is

```
cf cb 19 91 e0 cc 95 e1 b3 71 4c 8c
```

Part B

Starting with the scheme and noticing the invertibility of the $\oplus$ operation, we have

$$\begin{aligned} c_i &= g(m_i \oplus c_{i-1}) \oplus p_i \\ c_i \oplus p_i &= g(m_i \oplus c_{i-1}) \\ g^{-1}(c_i \oplus p_i) &= m_i \oplus c_{i-1} \\ g^{-1}(c_i \oplus p_i) \oplus c_{i-1} &= m_i \end{aligned}$$

Because g is both public and one-to-one, we know g^{-1}. We are given c_i, c_{i-1}, and p_i, thus we can derive m_i.

Part C

Let the message bth message be $M^b = (m_1^b, m_2^b, \ldots, m_n^b)$, a sequence of bytes. We want to show $\mathcal{P}(b|C) = 1/2$. From lecture, using Bayes' Law we determined showing $\mathcal{P}(C|b) = \mathcal{P}(C) = 1/2^n$ is sufficient to show security. We proceed with a proof of induction on c_i.

For the base case, we want to show that $\mathcal{P}(c_1|b) = \mathcal{P}(c_1) = 1/2$. Following from the fact that g is a one-to-one mapping, we have $\mathcal{P}(c_1 = g(m_1^b) \oplus p_1|b) = \mathcal{P}(c_1 = g(m_1^b) \oplus p_1|g(m_1^b)) = 1/2$. Next we have $\mathcal{P}(c_1) = \mathcal{P}(c_1|b=0)\mathcal{P}(b=0) + \mathcal{P}(c_1|b=1)\mathcal{P}(b=1) = (1/2)(1/2) + (1/2)(1/2)$.

For the inductive case, we want to show $\mathcal{P}(c_i|b) = \mathcal{P}(c_i) = 1/2$. Following from the fact that g is a one-to-one mapping, we have $\mathcal{P}(c_1 = g(m_i^b \oplus c_{i-1}) \oplus p_i|b) = \mathcal{P}(c_1 = g(m_i^b \oplus c_{i-1})|g(m_i^b \oplus c_{i-1})) = 1/2$. Next we have $\mathcal{P}(c_i) = \mathcal{P}(c_i|b=0)\mathcal{P}(b=0) + \mathcal{P}(c_i|b=1)\mathcal{P}(b=1) = (1/2)(1/2) + (1/2)(1/2)$. This proves that we gain no information about the message from the ciphertext.

Part D

The messages are

```
Cryptography is the study of "mathematical" systems
 involving two kinds of security problems: privacy
and authentication. A privacy system prevents the e
xtraction information by unauthorized parties from
messages transmitted over a public channel, thus as
suring the sender of a message that it is being rea
d only by the intended recipient. An authentication
 system prevents the unauthorized injection of mess
ages into a public channel, assuring the receiver o
f a message of the legitimacy of its sender.
```

and the pad is

```
9e c6 d4 29 00 62 ab 51 7a 72 e5 c1 d4 10 cd d6 17
54 e4 20 84 50 e4 f9 00 13 fd a6 9f ef 19 d4 60 2a
42 07 cd d5 a1 01 6d 07 01 32 61 3c 65 9a 8f 5d 33
```

Since we were given ten ciphertexts and know that each character is a readable hex character, we have a bounded number of possible bytes to which each ciphertext byte can decode. So, for each of the 51 bytes, we can iterate through the 256 possible pad bytes and see which byte, when used to decrypt the ciphertext byte, yields readable characters for all ten ciphertexts. The code for this can be found at https://github.com/DanielPradoSanchez/857_PSET_1/blob/master/2d.py.