1 Encryption

Consider the following PRP, $E(k, x)$:

$$E : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$$

where

$$\mathcal{K} = \{\text{ant}, \text{bird}, \text{cat}, \text{dog}, \text{eel}, \text{fish}\}$$
$$\mathcal{X} = \{0, 1\}^3$$

E	000	001	010	011	100	101	110	111	x
ant	000	100	110	001	111	010	011	101	
bird	111	001	000	110	100	010	101	011	
cat	011	100	001	010	101	000	110	111	
dog	000	100	110	010	101	011	001	111	
eel	110	100	101	011	001	111	010	000	
fish	000	001	100	110	011	101	010	111	
k									

1.1

Fill in the inverse table for $D(k, x)$:

D	000	001	010	011	100	101	110	111	x
ant									
bird									
cat									
dog									
eel									
fish									
k									

1.2

Based on your work, verify that this is a PRP. In particular:

- $f(x) = E(k, x)$ is a permutation for any specific key $k \in \mathcal{K}$.
  - If you assign each value in $\{0,1\}^3$ a distinct color and use this to color in the table, what would happen?
- $f(x) = E(k, x)$ always has a unique inverse $f^{-1}(x) = D(k, x)$.
  - This should hold because of the permutation property.
- $E(k, x)$ and $D(k, x)$ are efficiently computable for any $k \in \mathcal{K}, x \in \mathcal{X}$.

Note that this is not a *secure* PRP because $|\mathcal{K}|$ and $|\mathcal{X}|$ are very small. (The entire table fits on a single page!)

1.3

Decrypt the following messages:

- Decrypt ($IV = \texttt{101}, c = \texttt{000 011 010}$) using CBC with the key cat.
  - (You should get `000 000 000`).
- Decrypt ($IV = \texttt{110}, c = \texttt{010 111 111}$) using CTR with the key cat. [SOLUTION: `100 000 100`]

2

Verify the following signatures:

- Verify $s = \texttt{110}$ for the message `000` using CBC-MAC with the key $(k_1, k_2) = (\text{dog}, \text{eel})$.
- Verify $s = \texttt{010}$ for the message `001 010 011` using CBC-MAC with the key $(k_1, k_2) = (\text{dog}, \text{eel})$.

For the following section, we will be using the authenticated encryption systems built from our and existing cipher $Encrypt, Decrypt$, and CBC-MAC. The encryption method is:

$Encrypt - Then - Sign\Big((k_E, (k_1, k_2)), x\Big)$:

- $(IV, c) = Encrypt(k_E, x)$
- $s = Sign((k_1, k_2), IV \| c)$
- output (IV, c, s)

3

Why is it safe to concatenate the IV with c for the signature?

(Recall that excluding the IV completely allows for an easy forgery. Why can this not happen here?)

4

Decrypt and verify the following authenticated encryption:

- $(IV_{CBC} = \texttt{111}, c = \texttt{111 111 000 001 111 100}, s = \texttt{001})$ using CBC with CBC-MAC:
  - $k_{CBC} =$ eel
  - $k_{CBC\_MAC} = (k_1, k_2) =$ (cat, dog)
    [SOLUTION: 011]

4.1

Bonus: Unpad and decode the message using ASCII character codes. (Assume our standard padding scheme was used: add a one bit, then add zeros.)

[SOLUTION:

010 010 000 100 100 110

ASCII version: "HI"]

4.2

Decrypt and verify the following authenticated encryption:

- $(s = \texttt{011}, IV_{CTR} = \texttt{110}, c = \texttt{111 001 101 100 010 100})$ using CTR with CBC-MAC:
  - $k_{CTR} =$ bird
  - $k_{CBC\_MAC} = (k_1, k_2) =$ (ant, fish)
    [SOLUTION: 011]

[SOLUTION:

010 010 000 100 100 110

ASCII: "IT"]

4.3

Pick partner you haven't worked with before.

Agree on a CTR key and a CBC-MAC (double) key with your partner. Ask them to send you *two* authenticated encryptions of different 9-bit messages:

- One with a valid signature.
- One where they have either tampered with the encrypted ciphertext, the IV, or the MAC.

Check that exactly of the messages verifies, and decrypt the valid one.

(If you want, use a longer ASCII-encoded message instead of 9 bits. Make sure you both know what padding you're using.)

4.4

Pick one of the ways CBC-MAC can be broken:

- "Randomized" IV
- No finalization (no extra encryption at the end).
- Same key for the CBC portion and the the finalization.

Ask Lucas/Aaron/Conrad queries in the MAC Security game and produce a forgery.

5 One-Time MAC

Recall our one-time MAC from class:

- $p \in \mathbb{P}$
- $(a, b) \xleftarrow{R} \mathbb{Z}_p^* \times \mathbb{Z}_p$
- $Sign\Big((a, b), x\Big) = a \cdot x + b \mod p$

5.1

Say we have a particular key (a, b).

Prove that each different message would result in a different message if we sign it (using this particular key).

5.2

If p is large enough and (a, b) is a completely random valid key, can you use this as a secure PRP?

[SOLUTION:
No, two queries and you've broken it.
]

5.3

Let $(a, b) = (3, 4) \in \mathbb{Z}_7^* \times \mathbb{Z}_7$ (i.e. $p = 7$).

- Compute the signatures of $x = 0, 1, ..., 6$

5.4

Here are two valid message-signature pairs computed using the same key with $p = 13$

- $(x = 4, s = 5)$
- $(x = 2, s = 4)$

Produce a valid forgery for the message $x = 10$.

(Can you find an easy way to do it in this case, without solving for a and b?)

5.5

Do the previous problem with a partner, using $p = 17$

- Ask them to select a random key $(a, b) \xleftarrow{R} \mathbb{Z}_{17}^* \times \mathbb{Z}_{17}$.
- Send them two messages x and x' and receive a signature on each.
- Produce a forgery on a new message x''.

5.6

Open-Ended: Can you fix this system so that it allows more than two uses?