1

1.1 PRP

For this homework, use the following PRP:

$$E(k, m) : \{0,1\}^3 \times \{0,1\}^3 \times \{0,1\}^3$$

	000	001	010	011	100	101	110	111	m
000	011	001	111	010	000	101	110	100	
001	101	110	010	000	111	100	001	011	
010	001	110	100	111	011	010	000	101	
011	101	011	100	111	110	000	010	001	
100	001	101	110	010	100	011	000	111	
101	000	001	010	011	100	110	101	111	
110	100	000	011	101	111	001	010	110	
111	110	101	001	011	111	000	010	100	
k									

1.2 Davies-Meyer

Recall the Davies-Meyer compression function:

$$h(x, y) = E(x, y) \oplus y$$

1.3 Padding

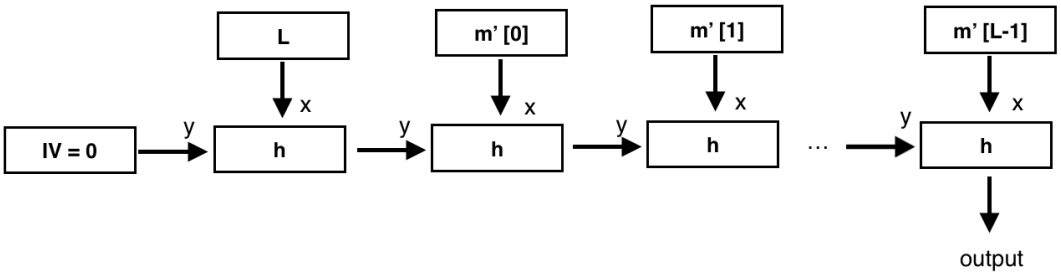
And recall our usual padding scheme $pad(m)$:

- Add a 1 to the end of m.
- Add zeros until the result aligns with the block size.

2 SPCS–Hash

Recall $SPCS\text{-}Hash(m)$ from class:

- Let $m' = pad(m)$
- Let L be the number of blocks in m'



2.1

Calculate the following using the PRP from section 1.1 and Davies-Meyer as h:

- $SPCS\text{-}Hash(\texttt{0})$ **Proof.** [SOLUTION: 111] □
- $SPCS\text{-}Hash(\texttt{1})$ **Proof.** [SOLUTION: 100] □
- $SPCS\text{-}Hash(\texttt{00})$ **Proof.** [SOLUTION: 001] □
- $SPCS\text{-}Hash(\texttt{000})$ **Proof.** [SOLUTION: 001] □
- $SPCS\text{-}Hash(\texttt{000 111})$ **Proof.** [SOLUTION: 110] □
- $SPCS\text{-}Hash(\texttt{101 101})$ **Proof.** [SOLUTION: 001] □

2.2

Since the PRP is very small, can you produce any collisions?

3 Compression Functions

3.1 Collision Resistance

In class we saw that Davies-Meyer is often used to convert an ideal block cipher into a collision resistant compression function from 2 blocks to 1. Let $E(k, m)$ be a block cipher where the message space is the same as the key space (e.g. 128-bit AES). Show that the following methods do not work, by breaking the following:

- Collision Resistance: it's hard to find two different pairs of inputs (x, y) and (x', y') such that $h(x, y) = h(x', y')$.

First show how to do this in general (e.g. how you would do it for AES), then construct actual collisions using our block cipher.

- $h_1(x, y) = E(x, y) \oplus x$
- $h_2(x, y) = E(y, x) \oplus y$
- $h_3(x, y) = E(x, x \oplus y)$
- $h_4(x, y) = E(x, x) \oplus x \oplus y$

(For the *pair* to be different, you need either $x \neq x'$, or $y \neq y'$. If both are different, that also works.)

Proof. [SOLUTION: This is from CS255 homeworks.

- $z, x = anything,\ y = D(x, x \oplus z)$
- $z, y = anything,\ x = D(y, y \oplus z)$
- $z, x = anything,\ y = D(x, z) \oplus x$
- $z, x = anything,\ y = E(x, x) \oplus x$

For any of these: Choose two different values of "anything" to get a collision.

] □

3.2 Preimage Resistance

Suppose someone gives you a specific target hash value z (say, $z = 111...1$). For which of the previous compression functions can you find inputs (x, y) such that $f(x, y) = z$?

Proof. [SOLUTION: TOdO: Switch with previous question.] □

4 Breaking CBC-MAC as a Hash

In class, we discussed how you can't convert CBC-MAC into a hash function because it wouldn't have pre image resistance and collision resistance.

Suppose we selected two values k_1, k_2 (permanently) and used the following hash:

$$H : \{0,1\}^* \to \{0,1\}^n$$

$$H(x) = CBC\text{-}MAC\Big((k_1, k_2), pad(x)\Big)$$

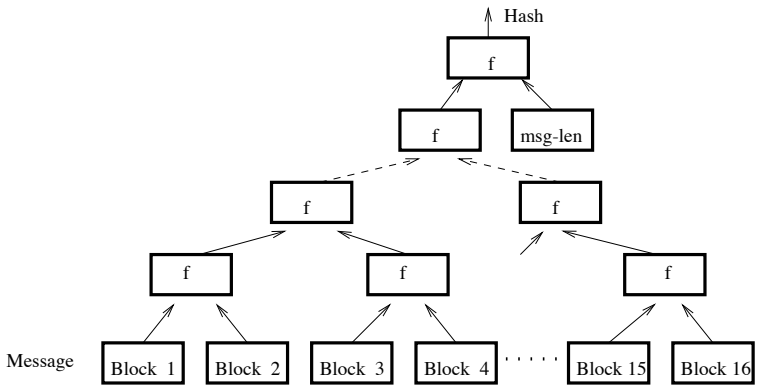
Show that it easy to break preimage resistance and collision resistance by finding expressions to calculate the following (for any choice of keys):

- Given z, show that you can find a message x such that $H(x) = z$
- Show that you can find messages x, y such that $H(x) = H(y)$

Apply your answers $H(x)$ using our block cipher, with $k_1 = \texttt{001}$ and $k_2 = \texttt{010}$

5 Merkle Hash Trees

Back in the day, Merkle suggested a parallel method for constructing hash functions out of compression functions. Let f be a compression function that takes two n-bit blocks and outputs one n-bit block. To hash a message m we use the following tree construction:



For simplicity, assume that the number of blocks in m is always a power of 2.

5.1

Evaluate $H(\texttt{000 001 010 011})$ using our PRP.

Proof. [SOLUTION: 000] □

5.2

- Prove that if one can find a collision for the resulting hash function then one can find collisions for the compression function.
- Show that if the msg-len block is eliminated (e.g. the contents of that block is always set to 0) then the construction is not collision resistant.

Proof. [SOLUTION: This is from CS255 homeworks.] □

5.3

Can you find a way to extend this to handle messages of arbitrary length? You will need to:

- Handle padding.
- Prove that it is impossible to find any hash collisions if without finding collisions in the compression function.

(This is actually tricky to get right, and it's it's easy to believe your proof is your correct even if it has a significant mistake. I suggest you leave this question for the end.)

6 Algorithm Substitution Attack

Suppose we are having a secret communication using a key m, and want to allow someone with a certain master key mk to listen in. Consider the following (authenticated) encryption algorithm $E_{PRP}(k, m)$ that uses a PRP E:

- Calculate $IV = E_{PRP}(mk, k)$
- Send the usual (authenticated) encryption $AE(k, m)$, using the IV from the previous step.

Answer:

- Show that anyone with the master key can decrypt the message.
- Show that the receiver (who also has k) can't tell the message apart from a valid encryption that uses a random IV.
- Show that no one without either k or mk can decrypt the message.
- What happens if you send the encryption of two different messages? Can you find a fix to the problem that comes up?