CS 198 Codebreaking at Cal
Spring 2023 Homework

HW 4

Question 1

Compare and contrast the following MAC protocols:

1. MAC-and-encrypt: $(Enc(k,m), MAC(k,m))$
2. Encrypt-then-MAC: $(Enc(k,m), MAC(k,Enc(k,m)))$

Which is better to use in real-world situations?

Question 2

In this question we will explore the idea of a *cryptographic committment scheme* and how to build them using secure hash functions.

Say Alice wants to play a game with Bob about coin flipping. If Bob can guess the outcome of the coin, he wins \$5. Otherwise, he pays Alice \$5.

Alice wants to convince Bob her coin flip is fair, but doesn't want to tell him what the result was before he guesses. In order to solve this, they use a committment scheme – she finds a random bit $b \in \{0,1\}$ and publishes $H(b\|r)$, where r is some random string of sufficient length.

After Bob publishes his guess b', she reveals b and r, and Bob can verify for himself whether his guess was correct, and be sure that Alice did not change the real value upon seeing his guess.

1. **Explain why Bob is convinced of the fact that Alice did not cheat, assuming H is a cryptographically-secure hash function.**
2. **Is this scheme still secure if H is no longer preimage-resistant? If not, who has the 'advantage' in this scenario, and how would they exploit the change?**
3. **Is this scheme still secure if H is no longer collision-resistant? If not, who has the 'advantage' in this scenario, and how would they exploit the change?**

Question 3

Recall the MAC security game:

1. An adversary sends m and receives $MAC(k,m)$ for a polynomial amount of times (with different messages as desired).

2. If the adversary can output some **valid** $(m', MAC(k, m'))$ such that m' was not sent in the previous round, they win the MAC security game.

Consider the following MAC scheme, using SHA-2 as the hash function:

$$MAC(k, m) = H(k||m)$$

1. **Argue why this scheme is insecure using the MAC security game, and provide the steps an adversary would take to win the game.**

   HINT: What attack is SHA-2 vulnerable to in particular?

2. **Does your attack from part 1 work for the scheme** $MAC(k, m) = H(m||k)$**? Explain why or why not.**

Contributors:

- Ryan Cottone

- Will Giorza