Keep Learning

Week 4 - Problem Set

Graded Quiz • 20 min

Due Jun 8, 12:29 PM IST

✓ **Congratulations! You passed!**

TO PASS 80% or higher

GRADE

100%

Week 4 - Problem Set

LATEST SUBMISSION GRADE

100%

1. An attacker intercepts the following ciphertext (hex encoded):

1 / 1 point

20814804c1767293b99f1d9cab3bc3e7 ac1e37bfb15599e5f40eef805488281d

He knows that the plaintext is the ASCII encoding of the message "Pay Bob 100$" (excluding the quotes). He also knows that the cipher used is CBC encryption with a random IV using AES as the underlying block cipher.

Show that the attacker can change the ciphertext so that it will decrypt to "Pay Bob 500$". What is the resulting ciphertext (hex encoded)?

This shows that CBC provides no integrity.

20814804c1767293bd9f1d9cab3bc3e7 ac1e37bfb15599e5f40eef805488281d

✓ **Correct**

You got it!

2. Let (E, D) be an encryption system with key space K, message

1 / 1 point

space $\{0,1\}^n$ and ciphertext space $\{0,1\}^s$. Suppose (E, D)

provides authenticated encryption. Which of the following systems