←

✓ **Congratulations! You passed!**

TO PASS 80% or higher

Keep Learning

GRADE
100%

Week 6 - Problem Set

LATEST SUBMISSION GRADE

100%

1. Recall that with symmetric ciphers it is possible to encrypt a 32-bit message and obtain a 32-bit ciphertext (e.g. with the one time pad or with a nonce-based system). Can the same be done with a public-key system?

1 / 1 point

○ Yes, when encrypting a short plaintext the output of the public-key encryption algorithm can be truncated to the length of the plaintext.

● No, public-key systems with short ciphertexts can never be secure.

○ Yes, the RSA-OAEP system can produce 32-bit ciphertexts.

○ It is possible and depends on the specifics of the system.

✓ **Correct**

An attacker can use the public key to build a