✓ **Congratulations! You passed!**

TO PASS 80% or higher

[Keep Learning]

GRADE
100%

Final Exam

LATEST SUBMISSION GRADE

100%

1. Let (E, D) be an authenticated encryption system built by combining

   a CPA-secure symmetric cipher and a MAC. The system is combined

   with an error-correction code to correct random transmission errors.

   In what order should encryption and error correction be applied?

   ○ The order does not matter -- neither one can correct errors.

   ○ Apply the error correction code and then encrypt the result.

   ◉ Encrypt and then apply the error correction code.

   ○ The order does not matter -- either one is fine.

   1 / 1 point

   > ✓ **Correct**
   >
   > That is correct. The error correction code will do its best
   >
   > to correct random errors after which the MAC in the ciphertext will be checked
   >
   > to ensure no other errors remains.

2. Let X be a uniform random variable over the set $\{0, 1\}^n$.

   1 / 1 point