# Old MM Quiz 5

**Due** Dec 2 at 10pm **Points** 10 **Questions** 5
**Available** until Dec 2 at 10pm **Time Limit** None
**Allowed Attempts** Unlimited

# Instructions

This is a mid-module quiz from a previous semester.

It is not necessarily representative of what this semester's quiz will look like, but is good practice.

It is worth a small amount toward your grade.

You may take it as many times as you wish.

You may work on it alone or collaborate with others.

You may use course materials and your own notes and homework during the quiz.

Do not give away answers to people you are not collaborating with.

This quiz was locked Dec 2 at 10pm.

## Attempt History

| | Attempt | Time | Score |
|---|---|---|---|
| **KEPT** | Attempt 8 | 4 minutes | 10 out of 10 |
| **LATEST** | Attempt 8 | 4 minutes | 10 out of 10 |
| | Attempt 7 | less than 1 minute | 8 out of 10 |
| | Attempt 6 | less than 1 minute | 6 out of 10 |
| | Attempt 5 | 6 minutes | 4 out of 10 |
| | Attempt 4 | 2 minutes | 4 out of 10 |
| | Attempt 3 | 2 minutes | 4 out of 10 |
| | Attempt 2 | 88 minutes | 3 out of 10 |
| | Attempt 1 | 363 minutes | 2 out of 10 |

ⓘ Correct answers are hidden.

Score for this attempt: **10** out of 10
Submitted Dec 1 at 1:28pm
This attempt took 4 minutes.

## Question 1

**2 / 2 pts**

Each of the following is a true/false statement about a tweakable block cipher (TBC). Place a checkmark next to each true statement.

- [ ] Because of its extra features, a TBC is always much slower than a regular block cipher.
- [ ] A good TBC allows change of the key with little computational cost.
- [x] A good TBC allows change of the tweak with little computational cost.
- [ ] A tweakable block cipher is a prominent part of the design of GCM.
- [ ] Each time a new tweak is given to a TBC, the TBC behaves like a new random function.
- [x] Each time a new tweak is given to a TBC, the next output of the TBC is uniformly distributed.

## Question 2

**2 / 2 pts**

Each of the following is a true/false statement about authenticated encryption. Place a checkmark next to each true statement.

- [ ] The only benefit to authenticated encryption is the ability to use the same key for both authentication and encryption.
- [ ] OCB is the most used authenticated encryption algorithm.
- [x] OCB is faster than GCM.
- [ ] GCM is essentially a univeral-hash-based authentication paired with CBC-mode encryption.
- [ ] Patents slowed the adoption of GCM.
- [ ] GCM completes encryption before it begins authentication.

## Question 3

**2 / 2 pts**

How many bits of entropy are there in the result of throwing a pair of four-sided dice (each side numbered 1, 2, 3, 4) and summing the two resulting values?

Answer to the nearest thousandth.

2.65

## Question 4

**2 / 2 pts**

I showed you in lecture how OCB uses a tweakable block cipher (TBC). It uses the universal hash function $h(T) = (iv)2^T$ where each message has its own random iv and calculation is over a Galois field. The TBC is then constructed as $E'(T,X) = h(T)$ xor $E(X$ xor $h(T))$. This hash function

is optimized for finding h(T+1) given h(T).

For demonstration purposes let's do an example over GF($2^8$). If h(0) is 42 (in hex), what are h(1) and h(2)?

h(1) 84

h(2) 13

Answer each with a two-digit hex answer and no spaces.

**Answer 1:**

84

**Answer 2:**

13

## Question 5

**2 / 2 pts**

Let's now say that we are using as our blockcipher the S-box from AES (ie, imagine that we have given a block cipher a key and it has given us the AES S-box as our permutation to use).

If h(0) = 42, then using the construction and hash function from the previous problem, what are the following values?

E'(1, 00000000) DB

E'(2, 10101010) 45

Answer each with a two-digit hex answer and no spaces.

**Answer 1:**

DB

**Answer 2:**

45

Quiz Score: **10** out of 10