

# CPEN 442, Fall 2015

## Quiz #3

Your Family name: \_\_\_\_\_

Your Given name: \_\_\_\_\_

Your student ID: \_\_\_\_\_

Your CPEN 442 alias: \_\_\_\_\_  
\_\_\_\_\_

#	Points	Out of
1		9 + 5B
2		9
3		4
4		6
4		14
<b>TOTAL</b>		<b>42+5B</b>

Notes:

- **This assignment is marked out of 45 points. There are 5 bonus points, which can be used to makeup for misses in any other question.**
- Make sure your handwriting is legible. If the teaching staff does not understand what you wrote, they mark your answer as if the unreadable text is missing.
- Aim to be precise and to the point. The experience of teaching this course since 2004 suggests that excessively long answers tend to correlate with lower marks.
- As in real world, stated questions and/or accompanied descriptions in this quiz are often open-ended and one has to make assumptions in order to answer them. If you do make assumptions, state them clearly and explicitly.
- Don't panic if you feel like you are severely short on time. Everybody is. ☺

1. (9 point + 5 bonus points) Analyze the following mode of operation and state (a) security properties it achieves, (b) pros, and (c) cons of this mode (3 points for each a, b and c subparts).

**Terms:**

$P_1, P_2, \dots, P_n$  – Plaintext blocks,  $C_1, C_2, \dots, C_n$  – ciphertext

$K$  – encryption key and  $E(K)$  – Encrypt with  $K$

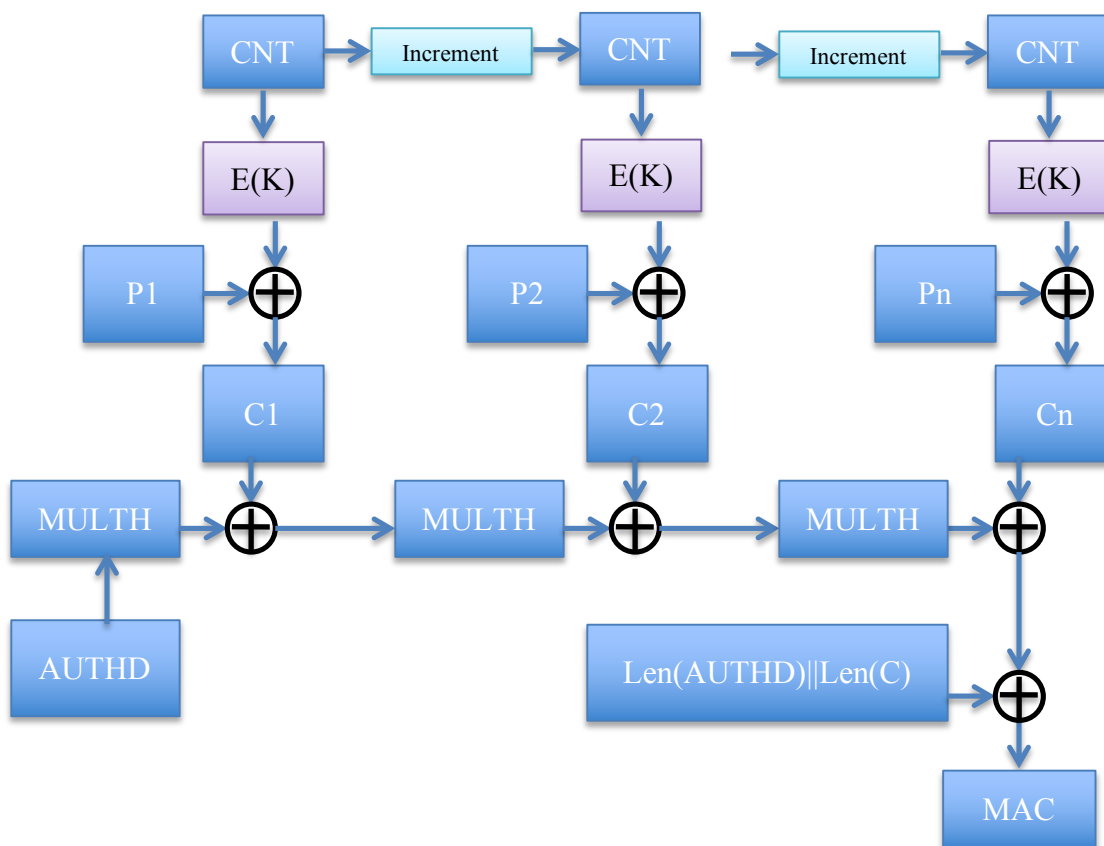
$CNT$  – a counter

$MAC$  – Message Authentication Code

$AUTHD$  – Data that needs to be authenticated

$MULTH$  – Multiplication of input with current internal value. Treat this as a hash function.

$Len(AUTHD)$  – length of  $AUTHD$ , and  $Len(C)$  – length of ciphertext



**a) (3 points)**

**b) (3 points)**

**c) (3 points)**

**BONUS d) (5 points) Name the mode: \_\_\_\_\_**

2. **(9 points) Design a communication protocol between Alice and Bob who share Shared Key (SK), so that the following properties are achieved: (a) Perfect Forward Secrecy, (b) Replay attack resistance, and (c) mitigate Man-In-The-Middle attack. (Each of the points is worth 3 points).**

**3. (4 points) What data signing with a private key achieves that cannot be achieved with MAC?**

**4. (6 points) List the three authentication factors and provide a real-life example for each.**

**5. The handout contains a reproduction of the iOS security features.**

- a. **(7 points) For each principle for designing secure systems, put a checkmark in the following table for those aspects of iOS that enable or follow this principle.**

**Attention:** The total number of points for this question will be determine using the following formula:  $R - W$ , where  $R$  is the number of right checkmarks and  $W$  is the number of wrong checkmarks.

	Secure Boot Chain	System Software Authorization	Secure Enclave	Touch ID	File Data Protection	Keychain Data Protection	App code signing	Runtime process security
Least Privilege								
Fail-Safe Defaults								
Economy of Mechanism								
Complete Mediation								
Open Design								
Separation of Privilege								
Least Common Mechanism								
Psychological Acceptability								
Defense in depth								
Question assumptions								

**(7 points) Write justification for the checkmarks in the above table. Give first priority to those checkmarks that are less obvious.**

