CPEN 442, Fall 2015 KEY

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
TOTAL		42+5B

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 your wrote, they mark your answer as if the unreadable text is missing.

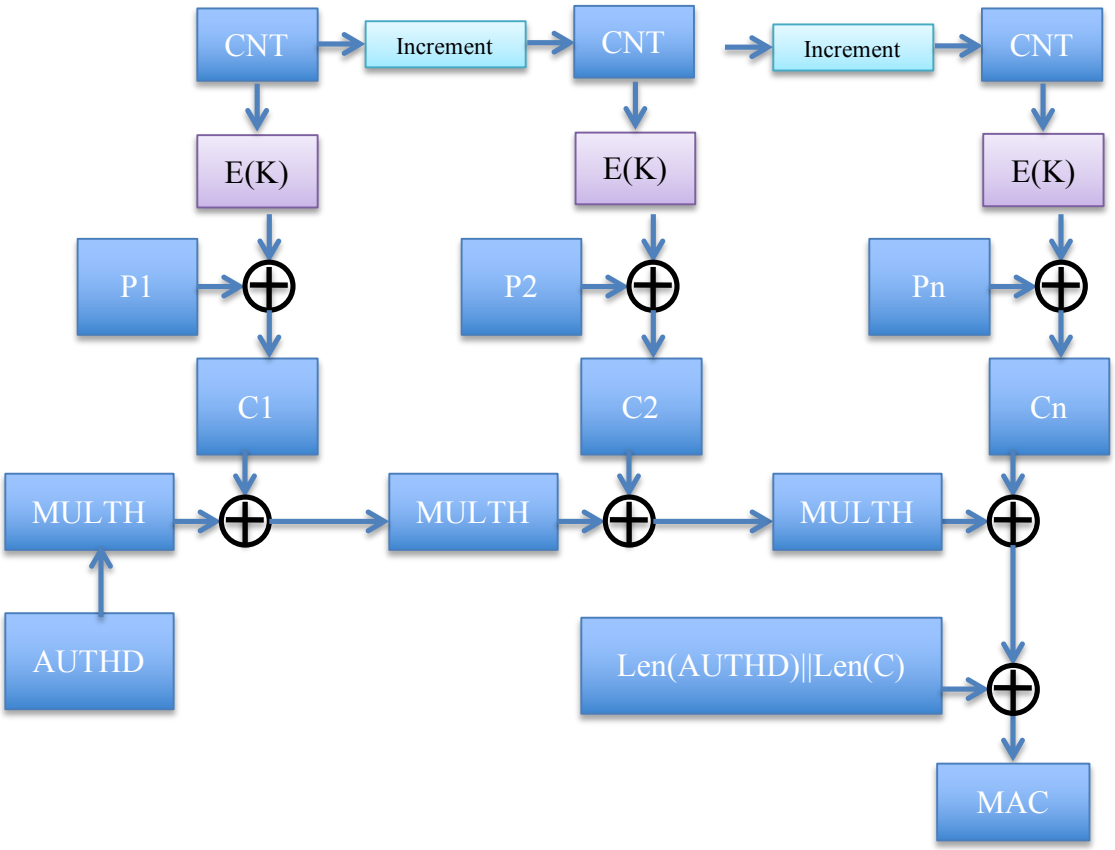
- Aim to be precise and to the point. The experience of teaching this course since 2004 suggests that excessively long answers tend to correlate with lower marks.

- 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:
P1,P2,...,Pn *– Plaintext blocks,* ***C1,C2,...,Cn*** *– 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)

Provides Confidentiality and Integrity.

b) (3 points)

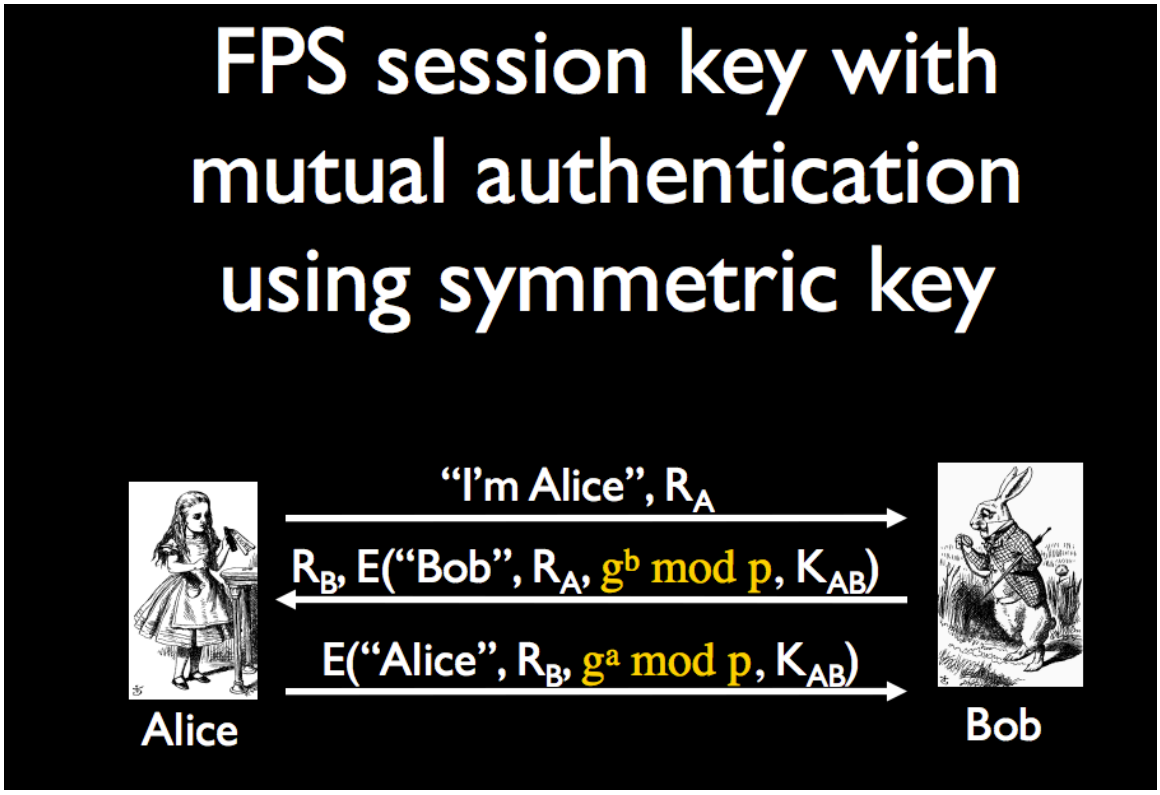
Encryption/Decryption parts are parallelizable. Although integrity protection is not.

c) (3 points)

While encryption is parallelizable, integrity protection is not.
Behaves like stream cipher, but requires the whole message to be encrypted before MAC can be calculated.

BONUS d) (5 points) Name the mode: _____GCM_____
CTR would give you 1 point
CCM would give you 3 points.

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?**

Digital signature gives non-repudiation while usual MAC with symmetric key does not.

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

Something you have – e.g., a key fob.
Something you are – e.g., Touch ID sensor for fingerprints.
Something you know – e.g., a password.

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						x		
Fail-Safe Defaults					x	x	x	
Economy of Mechanism				x			x	
Complete Mediation			x	x				
Open Design	x	x	x	x	x	x	x	x
Separation of Privilege		x	x	x	x		x	x
Least Common Mechanism			x	x			x	
Psychological Acceptability				x				
Defense in depth	x	x	x	x	x		x	x
Question assumptions								

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

Secure boot provides several layers (depth) of software attestation before passing control to the next layer.
Secure Enclave – the design is open, it always verifies all requests to it and provides another layer of defense.
Touch ID sensor – designed to be useable, always checks access to stored temporary key, provides another layer of security.