BIRZEIT UNIVERSITY

Faculty of Engineering and Technology
Electrical and Computer Engineering Department

ENCS4320, Applied Cryptography

Midterm Exam

Wednesday, 17/08/2022

Name:________ Answer ____________**ID**:_________________________

Q1) (10 points) True or False

1. The advantage of a stream cipher is that you can reuse keys.
   a) True
   b) False

2. The one-time-pad encryption scheme is CPA-secure.
   a) True
   b) False
   The one-time-pad is deterministic, so it can never be CPA-secure.

3. Any private-key encryption scheme that is CPA-secure must also be computationally indistinguishable:
   a) True
   b) False

4. If G' is a PRG, then $G(s) = G'(s) \oplus G'(\bar{s})$ is necessarily a PRG.
   a) True
   b) False
   G is not necessarily a PRG. Suppose that G' is a PRG which outputs the first bit of the seed and applies another PRG G'' to remainder: $G' = (b \parallel s'') = b \parallel G''(s'')$ where $b \in \{0,1\}, s'' \in \{\{0,1\}^{n-1}$.This G' is a PRG, but mow notice the first bit of $G(s)$ is always 1, because $b \oplus \bar{b} = 1$for any b.

5. If pseudorandom functions (PRF) exist, then pseudorandom generators (PRG) exist.
   a) True
   b) False
   True, $G(k) := F_k(1)||F_k(2)|| \cdots F_k(s)$ is a PRG (of stretch $n \cdot s$).

6. Let $Enc(K, M)$ be an IND-CPA secure encryption function. If Alice computes Enc("Hello","World") and Bob computes Enc("Hello","World"), they will always evaluate to the same ciphertext.
   a) True
   b) False
   Because this encryption function is IND-CPA secure, the scheme cannot be deterministic; consequently, encrypting the same thing twice (even with the same key and value) must yield two unique ciphertexts.

7. The IV in counter (CTR) mode must be kept secret.

a) True

b) False

8. CBC-mode encryption with PKCS#5 padding provides message integrity, as long as the receiver makes sure to verify the padding upon decryption.

c) True

d) False

9. Any private-key encryption scheme that is CCA-secure must also be CPA-secure.

a) True

b) False

10. Properly used, a MAC provides both confidentiality and integrity.

a) True

b) False

Q2) (10 points)

1- Which of the following are true about the Vigenere cipher?

a) The Vigenere cipher is computationally infeasible to break if the key has length 100, even if 1000s of characters of plaintext are encrypted.

b) The Vigenere cipher can always be broken, regardless of the length of the key and regardless of the length of plaintext being encrypted.

c) A Vigenere cipher with key of length 100 can be broken (in a reasonable amount of time) using exhaustive search of the key space.

d) The Vigenere cipher is perfectly secret if the length of the key is equal to the length of the messages in the message space.

2- Let $G: \{0,1\}^s \rightarrow \{0,1\}^n$ be a secure PRG. Is $G'(k) = G(k) \oplus 1^n$ is secure PRG?

a) Yes it is secure

b) No it is not secure

c) It depends on the distinguisher algorithm A

d) Not enough information to determine

3- In the definition of perfect secrecy, what threat model is assumed?

a) The attacker can eavesdrop on as many ciphertexts as it likes

b) The attacker can eavesdrop on a single ciphertext

c) The attacker is able to interfere with the communication channel between the two honest parties.

d) The attacker can carry out a chosen-plaintext attack

4- Which of the following is **NOT** true about computational secrecy?

a) Computational secrecy currently relies on unproven assumptions

b) Computational secrecy means that it is trivial for an attacker to always learn the entire message

c) Computational secrecy only ensures secrecy against attackers running in some bounded amount of time

d) Computational secrecy allows an attacker to learn information about the message with small probability

5- Consider a pseudo one-time pad encryption scheme Π constructed using some function G. Which of the following did our proof of security for the pseudo one-time pad show?

a) Π is always perfectly secret, for any G

b) Π is always computationally secret, for any G

c) If G is a pseudorandom generator, then Π is perfectly secret

d) If G is a pseudorandom generator, then Π is computationally secret

6- Double-DES was broken with the following attack:

a) Linear cryptanalysis attack

b) Man-in-the-middle attack

c) Meet-in-the-middle attack

d) Start-from-the-middle attack

7- Suppose Alice uses CBC Mode for encrypting a message m. However, she forgets the value she used for IV, but has c and k . Can she recover m?

a) Almost everything except m_1 (Where m_1 is the first block)

b) Can only recover m_{n-1}

c) Can only recover m_n

d) Almost everything expect m_1 and m_2

8- Say we use CBC-mode encryption based on a block cipher with 256-bit key length and 128-bit block length to encrypt a 512-bit message. How long is the resulting ciphertext?

a) 640 bits

b) 512 bits

c) 768 bits

d) Not enough information to determine.

9- One type of attack **not** covered by the definition of secure MAC scheme.

a) Forgery attack

b) Collision Attack

c) Replay attack

d) Key recovery attack

10- Which of the following is the most appropriate primitive for achieving message integrity between two users sharing a key?

a) Message authentication code

b) Block cipher

c) Collision-resistant hash function

d) Private-key encryption scheme

Q3) (5 points)

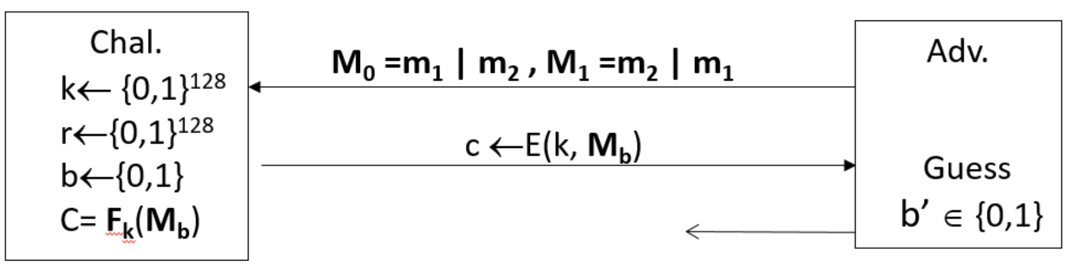
Let F be a block cipher with 128-bit block length. Consider the following encryption scheme for 256-bit messages: to encrypt message $M = m_1 \parallel m_2$ using key k (where $|m_1| = |m_2| = 128$, choose random 128-bit r and compute the ciphertext $r \parallel F_k(r) \oplus m_1 \parallel m_2$. Show how you could mount a valid chosen-plaintext attack (CPA) against this encryption scheme?

Let m_1 and m_2 be arbitrary but distinct.
Using the encryption oracle, obtain an encryption $r \| c_1 \| c_2$ of $m_1 \| m_2$.
Output messages $M_0 = m_1 \| m_2$ and $M_1 = m_2 \| m_1$.

Not that the last block is not encrypted. Therefore,

- **if $c_2 = m_2$ ➔ the challenge cipher for M_0**
- **if $c_2 = m_1$ ➔ the challenge cipher for M_1**

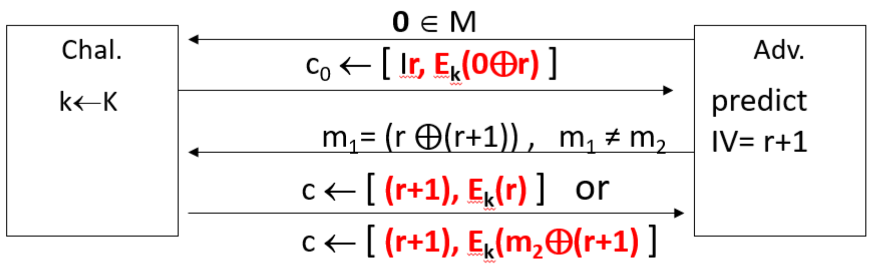
The attacker win the game with probability 1.



Q4) (5 points)

If Alice encrypts a message with AES-CBC, but instead of using completely random IVs, she uses r, $r+1$, $r+2$, and so on, where r is a random value that she chose once. Explain whither if this scheme is IND-CPA secure or not.

If the attacker can predict future IVs in AES-CBC, then AES-CBC is not IND-CPA secure.



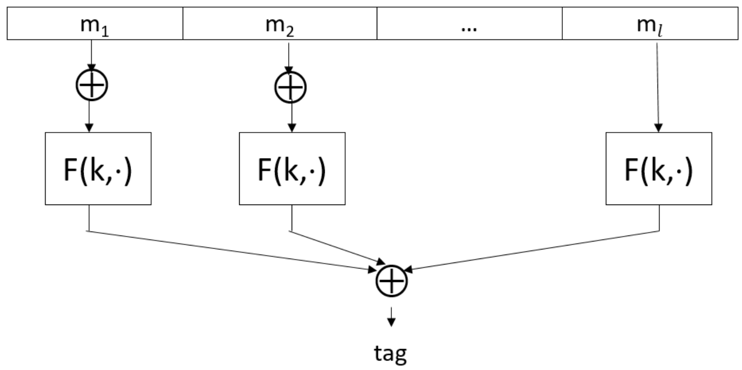
If $c = c_0$ them the challenge cipher for m_1 otherwise for m_2

Q5) (5 points)

Let F be a PRF. Show that the following constructions of MAC are insecure. Let $\mathcal{K} = \{0,1\}^n$ and $m = m_1 \parallel \cdots \parallel m_\ell$ with $m_i \in \{0,1\}^n$ for $i \in [1, \ell]$.

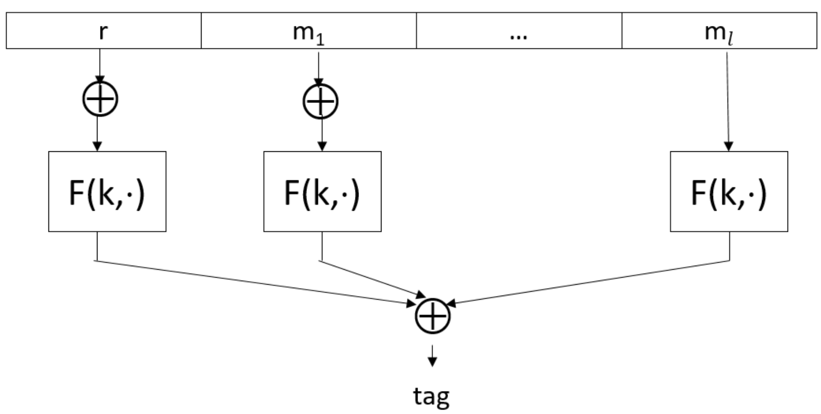
a) Send $t = F_k(m_1) \ldots \oplus F_k(m_\ell)$.

If t is the tag for $m_1 \| m_2 \| \cdots \| m_l$, t would be a valid forgery for $m_2 \| m_1 \| m_3 \| \cdots \| m_l$ since changing the order of message blocks does not change the value of the tag given by $F_k(m_1) \oplus \cdots \oplus F_k(m_l)$.



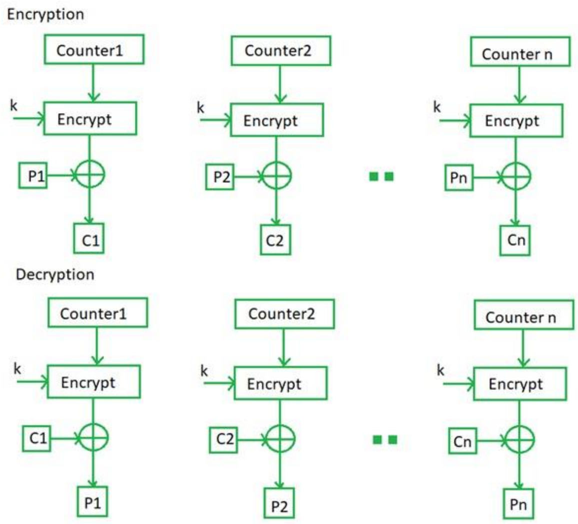
b) Pick $r \xleftarrow{U} \{0,1\}^n$, compute $t = F_k(r) \oplus F_k(m_1) \oplus \ldots \oplus F_k(m_\ell)$ and send (r, t).

A: Same attack (as in the previous part) works here. (r; t) remains a valid tag for any permutation of m_1, m_2, … , m_l



Q6) (5 points)

Assume an honest user wants to send an 8-bit integer to their bank indicating how much money should be transferred to the bank account of an attacker. The user uses CTR-mode encryption based on a block cipher F with 8-bit block length. The attacker knows that the amount of money the user wants to transfer is exactly $16, and has compromised a router between the user and the back. The attacker receives the ciphertext 10111100 01100001 (in binary) from the user. What ciphertext should the attacker forward to the bank to initiate a transfer of exactly $32?



C (c_1c_0): 10111100 01100001

M(16): 00000000 00010000

Y: 10111100 01110001

M'(32) 00000000 00100000

C' 10111100 01010001

The answer may different depends on how you represent the data