BIRZEIT UNIVERSITY

Electrical and Computer Engineering Department

First Semester 2021/2022

ENCS4320, Applied Cryptography

Midterm Exam

Date: Tuesday, 30/11/2021 Time: 15:50 - 17:10 (80 minutes) Room: ALSADIK202, ALSADIK203

Sec1: Dr. Ahmad Alsadeh
Sec2: Mr. Hanna Alzughbi

Student Name: _____________________**Student ID**: _____________

Question #	Full Mark	Student's Mark
Q1	12	
Q2	18	
TOTAL	30	

Q1) (12 pts) Consider the most suitable answer choice

1. 1. Consider the Vigenere cipher over the lowercase English alphabet, where the key length can be anything from 8 to 12 characters. What is the size of the key space for this scheme?

A. 26!
B. 26^{12}
C. 4×26^{12}
D. $26^8 + 26^9 + 26^{10} + 26^{11} + 26^{12}$

2. Let $M = C = K = \{0,1,2, \dots ,255\}$ and consider the following cipher defined over (K, M, C): $E(k, m) = m + k(\text{mod}256); D(k, c) = c - k(\text{mod}256)$. Does this cipher have perfect secrecy?

A. Yes, it does have perfect secrecy
B. No, there is a simple attack on this cipher
C. No, only the One Time Pad has perfect secrecy

3. Let (E, D) be a (one-time) semantically secure cipher where the message and ciphertext space is $\{0, 1\}^n$. Is the encryption scheme $E'(k, m) = E(k, m)||\ \text{LSB}(m)$ is (one-time) semantically secure?

A. **Yes, it is secure**
B. It depends on the attacker power
C. No, it is not secure
D. It depends on the message m

4. 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

5. Let $F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a secure PRF (i.e. a PRF where the key space, input space, and output space are all $\{0,1\}^n$ and say $n = 128$. Is $F'\big((k_1, k_2), x\big) = F((k_1, x) \parallel F(k_2, x)$ is a secure PRF?

A. Secure if $k_1 \neq k_2$
B. Not secure if $k_1 \neq k_2$
C. Secure if $k_1 = k_2$

6. Let m be a message consisting of l AES blocks (say $l = 100$). Alice encrypts m using CBC mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number $l/2$ is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted?

A. l
B. $l/2$
C. $1 + l/2$
D. 2

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. To encrypt a series of plaintext blocks $m_1, m_2, \dots, m_n$ using a block cipher E operating in electronic code book (ECB) mode, each ciphertext block $c_1, c_2, \dots, c_n$ is computed as $c_i = E(k, m_i)$. Which of the following **<u>is not</u>** a property of this block cipher mode?

A. Any repeated plaintext blocks will result in identical corresponding ciphertext blocks
B. Decryption can be fully parallelized
C. If a ciphertext block is modified or corrupted, then after decryption the corresponding plaintext block and all the following plaintext blocks will be affected.
D. None of the above; that is, (a), (b), and (c) are all properties of the ECB block cipher mode

9. To encrypt a series of plaintext blocks $m_1, m_2, \dots, m_n$ using a block cipher E operating in cipher block chaining (CBC) mode, each ciphertext block $c_1, c_2, \dots, c_n$ is computed as $c_i = E(k, m_i \oplus c_{i-1})$, where c_0 is a public initialization vector (IV) which should be different for each encryption session.
Which of the following **is** a property of this block cipher mode?

A. Any repeated plaintext blocks will result in identical corresponding ciphertext blocks
B. Decryption can be fully parallelized
C. If a ciphertext block is modified or corrupted, then after decryption the corresponding plaintext block and all the following plaintext blocks will be affected
D. None of the above; that is, neither (a), (b), nor (c) are properties of the CBC block cipher mode

10. Suppose a MAC system (S, V) is used to protect files in a file system by appending a MAC tag to each file. The MAC signing algorithm S is applied to the file contents and nothing else. What tampering attacks are not prevented by this system?

A. Swapping two files in the file system.
B. Replacing the tag and contents of one file with the tag and contents of a file from another computer protected by the same MAC system, but a different key.
C. Erasing the last byte of the file contents.
D. Changing the first byte of the file contents.

11. A hash function is constructed based on the Data Encryption Standard (DES, which is a permutation of 64-bit strings) using the Merkle-Damgard transform. Roughly, how many messages must be hashed so that we get a collision with probability greater than $\frac{1}{2}$?

A. 32
B. 64
C. 2^{32}
D. 2^{64}

12. MACs provide the following security properties:

A. Message confidentiality
B. Message integrity
C. Message non repudiation
D. Message origin authority

Q2)

1. (**2 pts**) Let $G: \rightarrow \{0,1\}^n$ be a secure PRG. Define $G'(k_1, k_2) = G(k_1) \wedge G(k_2)$ where $\wedge$ is the bitwise AND function. Consider the following statistical test A on $\{0,1\}^n$:
   $A(x)$ outputs $LSB(x)$, the least significant bit of x.
   What is $Adv_{PRG}[A, G']$? You may assume that $LSB(G(k))$ is 0 for exactly half the seeds k in $\boldsymbol{K}$.

   For a random string *x* we have *Pr*[A(*x*)=1]=1/2

   but for a pseudorandom string G'(k_1,k_2) we have $\Pr_{k1,k2}$[*A*(*G'*(k_1,k_2))=1]=1/2*1/2 = 1/4

2. (**2 pts**) A Feistel transformation is a function of the form

$$E\big(k, (L_0, R_0)\big) = \big(R_0, L_0 \oplus f(k, R_0)\big) = (L_1, R_1),$$

   where K is the key, L_0, R_0, L_1, R_1 are each n bit words, and $f(K, R_0)$ is an arbitrary function from n bits to n bits.
   Prove that every Feistel transformation is invertible. That is, show how to find $L_0, and\ R_0$ if $L_1, R_1, and\ K$ are known.

   Given $(\boldsymbol{L_1}, \boldsymbol{R_1})$, we immediately have $\boldsymbol{R_0} = \boldsymbol{L_1}$

   Then $\boldsymbol{R_1} = \boldsymbol{L_0} \oplus \boldsymbol{f}(\boldsymbol{k}, \boldsymbol{R_0}) = \boldsymbol{L_0} \oplus \boldsymbol{f}(\boldsymbol{k}, \boldsymbol{L_1}), \boldsymbol{so}$

$$\boldsymbol{L_0} = \boldsymbol{R_1} \oplus \boldsymbol{f}(\boldsymbol{k}, \boldsymbol{L_1}).$$

   That is

$$(\boldsymbol{L_0}, \boldsymbol{R_0}) = (\boldsymbol{R_1} \oplus \boldsymbol{f}(\boldsymbol{k}, \boldsymbol{L_1}), \boldsymbol{L_1})$$

3. (**2 pts**) Let E_K denote the encryption function of a block cipher with key $k \in \{0,1\}^n$. Suppose we try to strengthen this cipher by using two keys, $k_1, k_2 \in \{0,1\}^n$ and encrypting message m by the two keys $E(k_2, E(k_1, m))$. Describe a known plaintext attack on this cryptosystem that is faster than exhaustive search. How much faster is it, and how much memory does it use?

Meet in the middle attack

Given plaintext/ ciphertext pair (m, c), build list

A = {(E(K_1, m), K_1)} and B = {D(K_2, c), K_2}.

look for (x, K_1)

Time = 2^n.log(2^n) + 2^n.log(2^n) << 2^{2n} , space ≈ 2^n

4. (**3 pts**) Suppose that using commodity hardware it is possible to build a computer for about $200 that can brute force about 1 billion AES keys per second. Suppose an organization wants to run an exhaustive search for a single 128-bit AES key and is willing to spend 4 trillion dollars to buy these machines. How long would it take the organization to brute force this single 128-bit AES key with these machines? Ignore additional costs such as power and maintenance.

 # machines = $4*10^{12}/200 = 2*10^{10}$

 # keys processed per sec = $10^9 * (2*10^{10}) = 2*10^{19}$

 # seconds = $2^{128} / (2*10^{19})$ = 17,014,118,346,046,923,173.168730371588 = $1.7*10^{19}$

17,014,118,346,046,923,173.168730371588/ (60x60x24x365)= 539,514,153,540.3 years

The answer is about 540 billion years.

5. (**2 pts**) Let (S, V) be a secure MAC defined over (K, M, T) where $M = \{0,1\}^n$ and $T = \{0,1\}^{128}$. That is, the key space is K, message space is $\{0,1\}^n$, and tag space is $\{0,1\}^{128}$. Explain whether of the following is a secure MAC or not.

$S'(k, m) = S(k, m \oplus m)$ and
$V'(k, m, t) = V(k, m \oplus m, t)$

This construction is insecure because an adversary can request the tag for $\boldsymbol{m = 0^n}$

and thereby obtain a tag for any message.

This follows from the fact that $\boldsymbol{m \oplus m = 0}$

$\boldsymbol{S'(k, m_0) = S'(k, m_1)}$**, while $\boldsymbol{m_0 \neq m_1}$ Always give the same tag**

6. (**2 pts**) Let $H : M \rightarrow T$ be a collision resistant hash function. Is

$$H'(m) = H(m) \oplus H(m)$$

is collision resistant? Explain your answer.

$\boldsymbol{H'(m) = 0}$**, for** $\forall \boldsymbol{m} \in \boldsymbol{\mathcal{M}}$

This construction is not collision resistant because $\boldsymbol{H(m_0) = H(m_1)}$

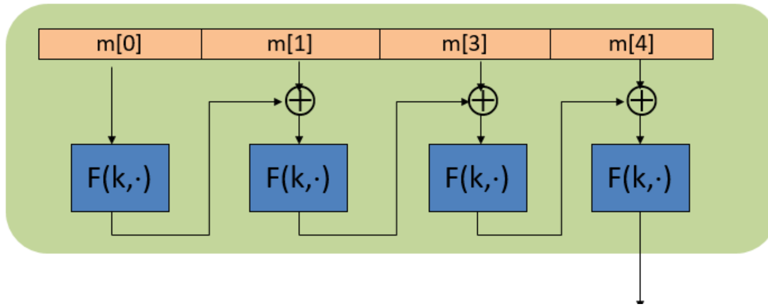
7. (**2 pts**) Suppose $\boldsymbol{F}: \boldsymbol{K} \times \boldsymbol{X} \longrightarrow \boldsymbol{Y}$ is a secure PRF with **Y = {0,1}**^{10}.Is the derived MAC I_F a secure MAC system? Explain

No tags are too short: anyone can guess the tag for any message

$$\boldsymbol{Adv[A, I_f] = {}^1/_{1024}}$$

8. (**3 pts**) The rawCBC is insecure MAC; explain the steps for attacking rawCBC construction.

raw CBC



Using chosen message attack

Adversary works as follows:

1- Choose an arbitrary one-block message $m \in X$

2- Request tag for m. Get $t = F(k, m)$

3- Output t **as MAC forgery for the 2-block message** $m' = (m,\ t \oplus m)$

Indeed: rawCBC$(k, (m,\ t \oplus m)\ ) = F(k, F(k, m) \oplus (t \oplus m)\ ) = F(k, t \oplus (t \oplus m)\ ) = t$

t **is a valid MAC for the 2-block message** $m' = (m, t \oplus m)$

So the adversary was able to produce this valid tag t **for this 2-block message that he never queried. And therefore, he was able to break the MAC**