BIRZEIT UNIVERSITY

Electrical and Computer Engineering Department

Second Semester 2018/2019

ENCS 532: Data and Network Security

Midterm Exam

Time: 12:50 - 14:05 (75 minutes)   Date: Wednesday, 10/04/2019   Room: Bamieh002

Dr. Ahmad Alsadeh

Student Name: _________ KEY _____________**Student ID**: _____________

Question #	Full Mark	Student’s Mark
Q1	12	
Q2	9	
Q3	9	
TOTAL	30	

Q1) Consider the most suitable answer choice

1. What is the size of key space in the substitution cipher assuming 26 letters?

A. |K| = 26
B. $|\mathcal{K}| = 26!$
C. |K| = 2^{26}
D. |K| = 26^2

2. You are given a message (*m*) and its One-Time-Pad (OTP) encryption (*c*). Can you compute the OTP key from m and c ?

A. No, I cannot compute the key
B. Yes, the key is $k = m \oplus m$
C. Yes, the key is $k = m \oplus c$
D. I can only compute half the bits of the key

3. Can a stream cipher have perfect secrecy?

A. Yes, if the pseudorandom generator (PRG) is really "secure"
B. No, there are no ciphers with perfect secrecy
C. Yes, every cipher has perfect secrecy
D. No, since the key is shorter than the message

4. Data compression is often used in data storage and transmission. Suppose you want to use data compression in conjunction with encryption. Does it make more sense to:

A. The order does not matter -- neither one will compress the data
B. Encrypt then compress
C. Compress then encrypt
D. The order does not matter -- either one is fine

5. Let $G: k \longrightarrow \{0,1\}^n$ be a secure PRG. Define $G'(k_1, k_2) = G(k_1) \wedge G(k_2)$ where $\bigwedge$ is the bit-wise 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 K.
Note: Please enter the advantage as a decimal between 0 and 1 with a leading 0. If the advantage is 3/4, you should enter it as 0.75

A. 0.25
B. 0.50
C. 0.75
D. 1

6. Let $M = C = K = \{0,1,2,\ldots,255\}$ and consider the following cipher defined over (K, M, C): $E(k,m) = m + k(mod256); D(k,c) = c - k(mod256)$. Does this cipher have perfect secrecy?

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

7. Let (E, D) be a (one-time) semantically secure cipher where the message and ciphertext space is$\{0,1\}^n$. Which of the following encryption schemes are (one-time) semantically secure?

A. $E'(k,m)$ =reverse($E(k,m)$)
B. $E'(k,m) = E(0^n, m)$
C. $E'(k,m) = E(k,m) \parallel LSB(m)$
D. $E'(k,m) = E(k,m) \parallel k$

8. 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 was willing to spend 4 trillion dollars to buy these machines (this is more than the annual US federal budget). 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.

A. More than a year but less than 100 years

B. More than a billion (10^9) years

C. More than a 100 years but less than a million years

D. More than a month but less than a year

E. More than an hour but less than a day

9. Let m be a message consisting of ℓ AES blocks (say $\ell = 100$). Alice encrypts m using CBC mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number $\ell/2$ 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. 1

C. $\ell/2$

D. $1 + \ell/2$

E. 2

10. 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. No

B. Almost everything except $\boldsymbol{m_1}$

C. Almost everything expect m_1m₁ and m_2

D. Can only recover m_{n-1}

11. To encrypt a series of plaintext blocks $p_1, p_2, \dots, p_n$ 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 $c_i = E(k, p_i)$. 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

12. To encrypt a series of plaintext blocks $p_1, p_2, \dots, p_n$ 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 $c_i = E(k, p_i \oplus c_{i-1})$, 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.

Q2) Basics and classical encryptions

1. (4 points) Encrypt the plaintext BESTSTUDENTS using the Shift Cipher with a key of 17.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext	**B**	**E**	**S**	**T**	**S**	**T**	**U**	**D**	**E**	**N**	**T**	**S**
	1	**4**	**18**	**19**	**18**	**19**	**20**	**3**	**4**	**13**	**19**	**18**
	18	**21**	**35**	**36**	**35**	**36**	**37**	**20**	**21**	**30**	**36**	**35**
mod26	**18**	**21**	**9**	**10**	**9**	**10**	**11**	**20**	**21**	**4**	**10**	**9**
Ciphertext	**S**	**V**	**J**	**K**	**J**	**K**	**L**	**U**	**V**	**E**	**K**	**J**

S V J K J K L U V E K J

2. (5 points) Decrypt the ciphertext `FVEBVGKHMCTIK`. It was encrypted using the Vigenere cipher with the keyword "`TRAIN`".

Cipher	**F**	**V**	**E**	**B**	**V**	**G**	**K**	**H**	**M**	**C**	**T**	**I**	**K**
	5	**21**	**4**	**1**	**21**	**6**	**10**	**7**	**12**	**2**	**19**	**8**	**10**
Key	**19**	**17**	**0**	**8**	**13**	**19**	**17**	**0**	**8**	**13**	**19**	**17**	**0**
diff	**-14**	**4**	**4**	**-7**	**8**	**-13**	**-7**	**7**	**4**	**-11**	**0**	**-9**	**10**
	12	**4**	**4**	**19**	**8**	**13**	**19**	**7**	**4**	**15**	**0**	**17**	**10**
Plaintext	**M**	**E**	**E**	**T**	**I**	**N**	**T**	**H**	**E**	**P**	**A**	**R**	**K**

Plaintext : Meet in the park

Q3) Block Cipher

1. (4 points) 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 $\boldsymbol{R_1} = \boldsymbol{L_0} \oplus \boldsymbol{f}(\boldsymbol{K}, \boldsymbol{R_0}) = \boldsymbol{L_0} \oplus \boldsymbol{f}(\boldsymbol{K}, \boldsymbol{L_1})$, so

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

That is

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

2. (5 points) 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 that 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

جامعة بيرزيت
BIRZEIT UNIVERSITY
Faculty of Engineering and Technology
Electrical and Computer Engineering Department

ENCS 532: Data and Network Security
Midterm
Dr. Ahmad Alsadeh
November 30, 2014

Name:___________ Solution Key______________________ **ID:**___________________________

Question 1: (20 points) Multiple choice

Please fill in your multiple choice answers using CAPITAL letters!

1	2	3	4	5	6	7	8	9	10
D	D	E	C	B	A	E	A	D	A

1. Over which finite field in Advanced Encryption Standard (AES), the S-box operations are performed?
   A. Z^{17}
   B. Z_{257}
   C. GF(2^4)
   D. GF(2^8)
   E. GF(2^{32})

2. There is NO finite field with _________________.
   A. 7 elements
   B. 8 elements
   C. 9 elements
   D. 10 elements
   E. 11 elements

3. For a prime number *p*, the property $a^p \equiv a$ (mod *p*) is known as ____________.
   A. Euler's Theorem
   B. Totient Theorem
   C. Miller-Rabin Theorem
   D. Primality Testing Theorem
   E. Fermat's Little Theorem

4. The technique used to speed up the modulo computations is called ______________.
   A. Totient computation
   B. Euler's Theorem
   C. Chinese Remainder Theorem
   D. Primitive root generation
   E. Discrete logarithm computation

5. Two integers are __________ if their only common positive integer factor is 1
   A. congruent modulo
   B. relatively prime
   C. polynomials
   D. residual
   E. odd

6. A group (G, *) is said to be _________ if it satisfies the condition $a * b = b * a$ for all a, b in G.
   - **A. Abelian**
   - B. Cyclic
   - C. Associative
   - D. Distributive
   - E. Swappable

7. Which algorithm is typically used to test a large number for primality?
   - A. Fermat
   - B. Euler
   - C. Newton
   - D. RSA
   - **E. Miller–Rabin**

8. How many elements are contained in the group of units Z^{*}_{26}, where Z^{*}_{26} contains the elements that have multiplicative inverse
   - **A. 12 // 26 = 13x2 → φ(26)= (13-1)(2-1)= 12**
   - B. 13
   - C. 15
   - D. 25
   - E. 26

9. A source that is effectively random is referred to as:
   - A. Open source
   - B. Seed
   - C. Keystream
   - **D. Entropy source**
   - E. Uniform randomness

10. What is the multiplicative inverse of x^{15} in $Z_2 [x]$ (mod $x^4 + x + 1$)?
   - **A. 1**
   - B. $x+1$
   - C. $x^2 + x + 1$
   - D. $x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$
   - E. x^{14}

   You start the Euclidean algorithm for polynomials:

   $x^{15} / (x^4 + x + 1) = x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$, with remainder 1.

   This means that $x^{15} \equiv 1$ (mod $x^4 + x + 1$), hence its inverse is 1.

Question 2: (30 points)

1. (**7 points**) What is the remainder when 37^{129} is divided by 80? (Hint: 80= 5×16)

φ(80) = φ((5)(16)) = φ(5) φ(16) = (5 – 1)(16 – 8) = 32.

Thus, $37^{32} \equiv 1$ mod 80.

$37^{129} \equiv (37^{32})^4(37)$ mod 80

$\equiv (1)^4(37)$ mod 80

≡ 37 mod 80

2. (**8 points**) Using multiplication in the field defined in AES (GF(2^8) with irreducible polynomial $x^8+ x^4+x^3+x+ 1$), what is the result (in hex) of multiplying the byte **03** by the byte **B7**?

$\mathbf{03}{\circ}\boldsymbol{B}\mathbf{7}=\mathbf{01}{\circ}\boldsymbol{B}\mathbf{7}+\ \mathbf{02}{\circ}\boldsymbol{B}\mathbf{7}=(\mathbf{1011\ 0111})+(\mathbf{1\ 0110\ 1110})$

Adding, we get

```
   1011  0111
1  0110  1110
-----------------
1  1101  1001
```

Reducing mod the AES polynomial we get

```
     1   1101  1001
+    1   0001  1011
   --------------------
     0   1100  0010
```

In Hex, this is C2.

3. (**15 points**) I have a certain number of pennies. If you divide the number of pennies I have by 49, the remainder is 33. If you divide the number of pennies I have by 55, the remainder is 16. If I have fewer than 2000, what is the exact number of pennies that I have?

Let X be the answer to the question. Then we have the two following equations:

$X \equiv 33 \bmod 49$

$X \equiv 16 \bmod 55$

This is an instance of the Chinese Remainder Theorem with $m_1 = 49$, $m_2 = 55$, $a_1 = 33$, $a_2 = 16$, $M = 2695$

a_i	**M= 49×55= 2695**	**M_i^{-1}**	**$a_i M_i M_i^{-1}$**
a_1=33	**M_1 = 55**	**M_1^{-1} = 41**	**74415**
a_2=16	**M_2=49**	**M_2^{-1} = 9**	**7056**
			81471

with $m_1 = 49$, $m_2 = 55$, $a_1 = 33$, $a_2 = 16$, $M = 2695$, $M_1 = 55$ and $M_2 = 49$. First, we need to find $M_1^{-1} \bmod M_2$ and $M_2^{-1} \bmod M_1$:

$55^{-1} \bmod 49 = 6^{-1} \bmod 49$. ($49 = 6 \times 8 + 1$, so $49 – 6 \times 8 = 1$, so $6^{-1} \equiv -8 \equiv 41 \bmod 49$.)

$49^{-1} \bmod 55 = 9$ ($55 = 1 \times 49 + 6$, so

$49 = 8 \times 6 + 1$.

$1 = 49 – 8 \times 6$

$1 = 49 – 8(55 – 49)$

$1 = 49 – 8 \times 55 + 8 \times 49$

$1 = 9 \times 49 – 8 \times 55$, so $49^{-1} \bmod 55 = 9$.

The solution is

$X = (a_1M_1M_1^{-1} + a_2M_2M_2^{-1}) \bmod M$.

$= (33 \times 55 \times 41 + 16 \times 49 \times 9) \bmod 2695$

$= 81471 \bmod 2695$

= <u>621 (Answer)</u>

Question 3: (40 points) Multiple choice

Please fill in your multiple choice answers using CAPITAL letters!

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**18**	**20**
D	**E**	**B**	**A**	**D**	**C**	**B**	**E**	**D**	**C**	**A**	**B**	**B**	**E**	**C**	**D**	**E**	**B**	**A**	**C**

1. A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack is called:
   A. Security algorithm
   B. Security protocol
   C. Security defense
   D. Security mechanism
   E. Security service

2. A loss of __________ is the unauthorized disclosure of information.
   A. trust
   B. integrity
   C. authenticity
   D. reliability
   E. confidentiality

3. If the information has been a subject of an unauthorized modification then we say that it lost its____.
   A. purity
   B. integrity
   C. reliability
   D. validity
   E. originality

4. When an attacker performs a capture of a data unit and its subsequent retransmission to produce an unauthorized effect, which attack he is performing?
   A. Replay
   B. Disruption
   C. Masquerade
   D. Service denial
   E. Unauthorized change of the content

5. In which attack scenario can we assume that the opponent has the least amount of information to work with?
   A. Chosen ciphertext
   B. Known plaintext
   C. Chosen plaintext
   D. Ciphertext-only
   E. Chosen plaintext-ciphertext

6. If a cipher has the property that given limited computing resources (for example time needed for calculations is greater than age of universe), the cipher cannot be broken, then the cipher is offering a(n) _____ .
   A. unconditional security
   B. conditional security
   C. computational security
   D. ultimate security
   E. universal security

7. The cipher design principle that makes relationship between ciphertext and key as complex as possible is called ______________.
    - A. diffusion
    - **B. confusion**
    - C. substitution
    - D. permutation
    - E. ideal cipher

8. Which two criteria are used to validate that a sequence of numbers is random?
    - A. One-way and Independence
    - B. Unpredictability and Chaoticity
    - C. Unpredictability and Smoothness
    - D. Uniform distribution and Indeterminism
    - **E. Uniform distribution and Independence**

9. An S-box satisfies the following criterion: For a 1-bit input change, at least *n* output bits change. We say that the S-box satisfies the
    - A. Bit change criterion
    - B. Bijection criterion
    - C. Diffusion criterion
    - **D. Avalanche criterion**
    - E. Confusion criterion

10. What is the block cipher structure in DES?
    - A. SAC
    - B. Shannon
    - **C. Feistel**
    - D. Rendell
    - E. One Way Permutation

11. What is correct?
    - **A. DES uses a 64-bit message block and a 56-bit key.**
    - B. DES uses a 64-bit message block and a 64-bit key.
    - C. DES uses a 56-bit message block and a 64-bit key.
    - D. DES uses a 56-bit message block and a 48-bit key.
    - E. DES uses a 64-bit message block and a 128-bit key.

12. If by $E_K(\,)$ we denote the encryption function of a block cipher with a key K, and if the mode of operation is $C_i = E_K(P_i \oplus C_{i-1})$ then the mode of operation is ______.
    - A. ECB
    - **B. CBC**
    - C. CFB
    - D. OFB
    - E. CTR

13. The RC4 stream cipher is:
    - A. bit oriented
    - **B. byte oriented**
    - C. 16 bit oriented
    - D. Big-endian oriented
    - E. Little-endian oriented

14. An encryption scheme that requires large quantities of random keys that are as long as the messages that have to be encrypted, and are distributed on a regular basis to both sender and receiver, is known as:
    A. Key-pad scheme
    B. iPad scheme
    C. crypto-pad scheme
    D. time-pad scheme
    E. one-time pad scheme

15. 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
    E. Differential cryptanalysis attack

16. The main reason why Triple-DES was not kept as the only standard for block ciphers and have been replaced by AES is that
    A. it has too short key
    B. it has too long key
    C. it is patented
    D. it is slow
    E. it is old

17. Double version of the 56-bit DES is much less secure than a single 112-bit DES because
    A. the plaintext *m* is encoded twice with different keys
    B. double DES can be attacked by brute-force attack, which takes not much more time than 2^{56}
    C. double DES is vulnerable to chosen plaintext attack, which takes not much more time than 2^{56}
    D. double DES is vulnerable to chosen ciphertext attack, which takes not much more time than 2^{56}
    E. double DES can be attacked by meet-in-the-middle, which takes not much more time than 2^{56}

18. By Miller-Rabin algorithm we can prove that a number is:
    A. prime
    B. composite
    C. power of 2
    D. relatively prime to another number
    E. a factor of another number

19. In practice, why is the Miller-Rabin algorithm used for primality testing, instead of the AKS algorithm?
    A. Miller-Rabin test is much quicker than AKS
    B. Miller-Rabin test is always correct
    C. Miller-Rabin test is iterative
    D. AKS test result is inaccurate
    E. AKS test does not work for large numbers

20. The ciphertext for a Vigenere cipher is "HZXKEP". The original plaintext is “FRIDAY”? What was the encryption keyword "?
    A. CAESAR
    B. CIRCLE
    C. CIPHER
    D. COVERT
    E. CREDIT

Ciphertext	**H**	**Z**	**X**	**K**	**E**	**P**
	7	25	23	10	4	15
Plaintext	**F**	**R**	**I**	**D**	**A**	**y**
	5	17	8	3	0	24
	2	8	15	7	4	17
Key	**C**	**I**	**P**	**H**	**E**	**R**

Question 4: (10 points)

1. (**4 points**) The smallest version of AES uses a 128 bit key. How many keys would have to be searched per second in order for a brute force attack to break AES in a year? Express your answer in scientific notation.

Total number of keys = 2^{128}.

Number of seconds in a year = 60 x 60 x 24 x 365 = 3153600.

The number of searched per second to finish the task in a year
= 2^{128} / 3153600 = 1.0790 x 10^{32}

2. (**4 points**) List two advantages of stream ciphers over block ciphers.

   1. **Stream ciphers are generally faster.**
   2. **Stream ciphers do not require padding to a block size**
   3. **Stream ciphers do not propagate errors, which is useful for multimedia**
   4. **The keystream can be precomputed and only an exclusive-OR is necessary once the stream becomes available, reducing transmission latency.**

3. (**5 points**) Which of the following can operate as stream ciphers and which can only operate as a bock cipher?

AES	DES	AES-OFB	AES-CBC	AES-CTR
Block	**Block**	**Stream**	**Block**	**Stream**

BIRZEIT UNIVERSITY
Faculty of Engineering and Technology
Electrical and Computer Engineering Department

ENCS 532: Data and Network Security
Midterm Exam
Dr. Ahmad Alsadeh
Date: November 24, 2015
Time: 14:00 - 15:30

Name:__________ **Solution Key**______________________ **ID**:__________________________

Question 1: Classical Encryption techniques

1. The ciphertext for a Vigenere cipher is "HZXKEP". If the encryption keyword is "CIPHER", what was the original plaintext?

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**G**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

H Z X K E P	**7 25 23 10 4 15**
C I P H E R	**2 8 15 7 4 17**
------------------------	**------------------------**
F R I D A Y	**5 17 8 3 0 -2**

2. Encrypt "LASTQUESTION" using the playfair cipher and the keyword "LEMONS".

Here is the grid:

L	**E**	**M**	**O**	**N**
S	**A**	**B**	**C**	**D**
F	**G**	**H**	**I/J**	**K**
P	**Q**	**R**	**T**	**U**
V	**W**	**X**	**Y**	**Z**

Plaintext:	LA	ST	QU	ES	TI	ON
Ciphertext:	**ES**	**CP**	**RP**	**LA**	**YT**	**NL**

Encryption is **ESCPRPLAYTNL.**

Question 2: DES and AED

1. (20 pts) Consider a simple cryptosystem with a 16 bit block and 16 bit key as follows:
Step 1: Compute $C_0 = A(P)$, where A is the permutation matrix shown below.
Step 2: Compute $C_1 = C_0 \oplus K$, where K is the input key.
Step 3: Compute $C_2 = S(C_1)$. S splits its input into four blocks of four bits. For each block of four bits, it substitutes for it values shown in B. For example, if the four bits of input were 0101, which corresponds to 5, we would look in spot #5 in B, in row 1, column 2, which is 12 and substitute 1100. As another example if the input were 1110, the output would be 0101.
Step 4: Let $C_2 = LR$, where L is the left byte and R is the right byte. Compute the ciphertext C = RL.

$$A = \begin{bmatrix} 3 & 7 & 12 & 9 \\ 11 & 14 & 6 & 1 \\ 15 & 16 & 10 & 13 \\ 2 & 4 & 5 & 8 \end{bmatrix}, \qquad B = \begin{bmatrix} 6 & 1 & 11 & 4 \\ 13 & 12 & 15 & 8 \\ 0 & 3 & 10 & 9 \\ 7 & 2 & 5 & 14 \end{bmatrix}$$

Compute the encryption of the plaintext A349 with the key 5DF7.

Plaintext: A349

1 0 1 0 0 0 1 1 0 1 0 0 1 0 0 1
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

$$C_0 = \begin{bmatrix} \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}$$

C_0: 1100 0001 0111 0001 (4 pts)
K: 0101 1101 1111 0111

C_1: 1001 1100 1000 0110 (1pts)
9 12 8 6

C2: 3 7 0 15
C2: 0011 0111 0000 1111 (4 pts)
L R
C: 0000 1111 0011 0111 (1pts)
0 F 3 7

2. Let the input to the MixCols (during AES encryption) be $\begin{bmatrix} A0 & 74 & 65 & \mathbf{B7} \\ 2B & 8D & 2E & \mathbf{C6} \\ 99 & 1F & C8 & \mathbf{EB} \\ C5 & E5 & F7 & \mathbf{23} \end{bmatrix}$.

What's the output in row 2 col 4? (The matrix by which to "multiply" is $\begin{bmatrix} 02 & 03 & 01 & 01 \\ \mathbf{01} & \mathbf{02} & \mathbf{03} & \mathbf{01} \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$

We must compute
01 x B7 = 1011 0111 (no change to original) (1 pt)

C6 = 1100 0110
1 1000 1100 (1 pts) (shift left by 1 bit)
xor 1 0001 1011 (1 pts)
2 x C6 = 1001 0111 (1 pts)

EB = 1110 1011
2 x EB = 1 1101 0110 (1 pts)
xor 1 0001 1011 (1 pts)
2 x EB = 1100 1101 (1 pts)

EB = 1110 1011
xor 2 x EB = 1100 1101
3 x EB = 0010 0110 (1 pts)

01 x 23 = 0010 0011 (no change to original) (1 pt)

01x B7 = 1011 0111
02xC6 = 1001 0111
03xEB = 0010 0110
01 x 23= 0010 0011
Ans = 0010 0101 (1pts)
$(25)_H$

Question 3: Number Theory

1. (**15 pts**) Using the Extended Euclidean Algorithm determine 65^{-1} mod 147. Please answer with an integer in between 0 and 146, inclusive. **Note: most of the credit will be for the steps of the algorithm and not the final answer.**

   147 = 2 x 65 + 17
   65 = 3 x 17 + 14
   17 = 1 x 14 + 3
   14 = 4 x 3 + 2
   3 = 1 x 2 + 1
   2 = 2 x 1+0, so GCD(147, 65) = 1, as required**. (Grading: 5 pts)**

   3 - 1 x 2 = 1
   3 - (14 - 4 x 3) = 1
   5 x 3 - 1 x 14 = 1
   5(17 - 14) - 1 x 14 = 1
   5 x 17 - 6 x 14 = 1
   5 x 17 - 6(65 - 3 x17) = 1
   5 x 17 - 6 x 65 + 18 x 17 = 1
   23 x 17 - 6 x 65 = 1
   23(147 - 2 x 65) - 6 x 65 = 1
   23 x 147 - 46 x 65 - 6 x 65 = 1
   23 x 147 - 52 x 65 = 1 **(Grading: 8 pts)**

   Taking the equation mod 147, we find 65^{-1} mod 147 = -52 ≡ 95.
   Thus, the desired inverse is 95. (1 pt for -52, 1 pt to map to 95.)

2. (**15 pts**) Using the Chinese Remainder Theorem, find all solutions to the following system:

$$7x \equiv 4(\text{mod } 11)$$
$$x \equiv 3(\text{mod } 7)$$

   gcd(11,7)=1

   $x = 4\ (7^{-1})$ (mod 11)

   11 = 7x1+ 4
   7 = 4x1+ 3
   4 = 3x1+ 1
   3 = 1x3+ 0

   1 = 4 - 3x1
   = 4 - (7 - 4x1)
   = 2x4 - 7
   = 2x(11-7) -7
   = 2x11 - 3x7

   Taking the equation mod 11. Thus 7^{-1} mod 11= -3 = 8 (**5pts**)
   x = 32 (mod 11) = 10 (mod 11)
   x = 3 (mod 7)

a_i	**M= 11x7= 77**	**y_i**	**$a_iM_iy_i$**	
a_1=10	M_1=7	y_1= 8	560	**(4pts)**
a_2=3	M_2=11	y_2=2	66	**(4pts)**
			626	

   7^{-1} mod 11= 8
   11^{-1} mod 7 = 2

***x* = 626 mod 77 = 10 (2pts)**

Question 4: Block Cipher Operation and random numbers

1. What is the biggest advantage of CBC mode of operation

A ciphertext block depends on all blocks before it. The same plaintext block, if repeated, produces different ciphertext blocks. The input to the encryption function for each plaintext block bears no fixed relationship to the plaintext block.

2. For Output FeedBack (OFB) mode of operation, if ***E_K(P)*** denotes an encryption of the plaintext block ***P*** with the key ***K*** by the block cipher ***E***, then write the equations that describe the cipher:

   $C_i = P_i$ XOR O_i
   $O_i = E_K(O_{i-1})$
   O_{-1} = IV

3. What are the characteristics of the "Counter" mode of operation

   Complete answer should briefly elaborate the following characteristics:
   a. Hardware efficiency
   b. Software efficiency
   c. Preprocessing
   d. Random access
   e. Provable security
   f. Simplicity

Question 5: Alice is using a linear congruential generator, $(ax_i + b)\ mod\ 13$, to generate pseudo-random numbers. Eve sees three numbers in a row, 7, 6, 4, that are generated from Alice's function. What are the values of a and b?

$$x_0 = 7, x_1 = 6, x_2 = 4$$

$$x_{i+1} = (ax_i + b) mod\ 13$$

$$6 = (7a + b) mod\ 13 \dots eq(1)$$
$$4 = (6a + b) mod\ 13 \dots eq(2)$$

subtract $eq(1)\ -\ eq(2)$

$$\underline{a\ = 2\ mod\ 13}$$

substitute a=2 in $eq(1)$

$$6 = (14 + b) mod\ 13$$
$$-8 = b\ mod\ 13$$
$$\underline{b{=}5\ mod\ 13}$$

BIRZEIT UNIVERSITY
Faculty of Engineering and Technology
Electrical and Computer Engineering Department

ENCS 532: Data and Network Security
Midterm Exam
Tuesday, December 13, 2016
Time: 14:00 - 16:30

Dr. Ahmad Alsadeh

Student's Name: Solutions **ID**:

Instructions:

1. This is a closed book exam.
2. Make sure your mobile phone is switched off.
3. Write your solutions in the space provided. If you need more space, write on the back of the sheet containing the problem.
4. No calculators or programmable devices are permitted.
5. The exam is worth a total of 100 marks.

Good luck!

Question 1: 36 points) Circle the one answer that best answers the question. Each question worth 3 points.

1. Eve has bet Bob that she can figure out the AES secret key he shares with Alice if he will simply encrypt 20 messages for Eve using that key. For some unknown reason, Bob agrees. Eve gives him 20 messages, which he then encrypts and emails back to Eve. What kind of attack is Eve using here?

A. This is a chosen-plaintext attack
B. This is a ciphertext-only attack
C. This is a chosen-ciphertext attack
D. This is a known-plaintext attack

2. How many elements are contained in the group of units Z_{77}, where Z_{77} contains the elements that have multiplicative inverse

A. 11
B. 60
C. 75
D. 77
Answer: 77 = 11x7 = φ(77)= (11-1)(7-1)= 60

3. What is the greatest common divisor of 654 and 123?

A. 2
B. 3
C. 6
D. 19

Solution: We have
654 = 5 · 123 + 39
123 = 3 · 39 + 6
39 = 6 · 6 + 3
6 = 2 · 3 + 0

4. The Euler Totient Function $\phi(24)$ is

A. 8
B. 14
C. 15
D. 23

ø(24)= ø(8.3)= ø(2^3)ø(3)=4.2=8

$ø(p^k) = p^k - p^{(k-1)} = p^{(k-1)}\ (p - 1)$
ø(2^3)=2^{3-1} (2-1)=4

5. What is the remainder when 38^{133} is divided by 69? (Hint: 69= 23×3)

A. 3
B. 23
C. 38
D. 44

φ(69) = φ((23)(3)) = φ(23) φ(3) = (23 – 1)(3 – 1) = 22. 2= 44.
Thus, $38^{44} \equiv 1 \bmod 69$.

$$38^{133} \equiv (38^{44})^3(38) \bmod 69$$
$$\equiv (1)^3(38) \bmod 69$$
$$\equiv 38 \bmod 69$$

6. Recall that we can represent the field of 256 elements as polynomials $F_2[x]$ modulo $x^8 + x^4 + x^3 + x + 1$. The inverse of x in this field is

A. 1

B. x+1

C. x^3+1

D. x^7+x^3+x^2+1

Solution: We start to use the Euclidean algorithm:
$X^8 + X^4 + X^3 + X + 1 = (X^7 + X^3 + X^2 + 1) \cdot X + 1$
and after 1 step we are done: this equation says that
$X \cdot (X^7 + X^3 + X^2 + 1) = 1$ (mod $X^8 + X^4 + X^3 + X + 1$) and so the inverse of X is $X^7 + X^3 + X^2 + 1$.

7. The Shannon principle of "*diffusion*"

A. makes relationship between ciphertext and key as complex as possible

B. diffuses the plaintext among huge subset of plaintexts

C. dissipates statistical structure of plaintext over bulk of ciphertext.

D. diffuses the key and the plaintext among a subset of plaintexts

8. To encrypt a series of plaintext blocks $P_1, P_2, \ldots P_n$ using a block cipher E operating in electronic code book (ECB) mode, each ciphertext block $C_1, C_2, \ldots C_n$ is computed as $C_i = E_K(P_i)$. Which of the following **is not** 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.

Answer: The correct answer is (c). In ECB, altering a ciphertext block only affects a single plaintext block.

9. To encrypt a series of plaintext blocks $P_1, P_2, \ldots, P_n$ using a block cipher E operating in cipher block chaining (CBC) mode, each ciphertext block $C_1, C_2, \ldots, C_n$ is computed as $C_i = E_K(P_i \oplus C_{i-1})$, 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.

Answer: The correct answer is (B). Each plaintext block can be computed using only two ciphertext blocks, independent of the other plaintext blocks: $P_i = D_k(C_i) \oplus C_{i-1}$
Note that (C) is not a property of CBC. A modification to a ciphertext block will affect that plaintext block and the one immediately following it, but none after that.

10. If by $E_K(\ )$ we denote the encryption function of a block cipher with a key K, and if the mode of operation is $C_i = E_K(P_i \oplus C_{i-1})$ then the mode of operation is ______.

A. CFB

B. CBC

C. OFB

D. CTR

11. Why is the Double version of the 56-bit DES much less secure than a single 112-bit DES?

A. Because the plaintext is encoded twice, with different keys

B. Because Double DES can be attacked by "meet-in-the-middle"

C. Because Double DES can be attacked by "man-in-the-middle"

D. Because Double DES can be attacked by "brute- force"

12. Alice knows that she will want to send a single 128-bit message to Bob at some point in the future. To prepare, Alice and Bob first select a 128-bit key $k \in \{0, 1\}^{128}$ uniformly at random. When the time comes to send a message $x \in \{0, 1\}^{128}$ to Bob, Alice considers two ways of doing so. She can use the key as a one-time pad, sending Bob $k \oplus x$. Alternatively, she can use AES to encrypt x. Recall that AES is a 128-bit block cipher which can use a 128-bit key, so in this case she would encrypt x as a single block and send Bob $\text{AES}_k (x)$.

Assume Eve will see either $k \oplus x$ or $\text{AES}_k(x)$, that Eve knows an initial portion of x (a standard header), and that she wishes to recover the remaining portion of x.

If Eve is an all powerful adversary and has time to try out every possible key $k \in \{0, 1\}^{128}$, which scheme would be more secure?

A. The one time pad would be more secure. Even if Eve tried all possible keys, she would not be able to recover the unknown portion of x. If AES was used, Eve could eventually learn the unknown portion of x.

B. AES would be more secure. Even if Eve tried all possible keys, she would not be able to recover the unknown portion of x. If the one time pad was used, Eve could eventually learn the unknown portion of x.

C. They would be equally secure. Either way, Eve could eventually learn the unknown portion of x.

D. They would be equally secure. Either way, Eve would not be able to learn the unknown portion of *x*.

Answer: The correct answer is (D). Even after trying every possible key (including the actual one), Eve will have no way of recognizing the correct plaintext or even narrowing down the possibilities in any way.

Why is this? Well, since AES is a distinct permutation on $\{0, 1\}^{128}$ under each possible key, and the key was selected uniformly at random, given any plaintext, each possible ciphertext is equally likely. So when AES is used for a single block with a random key of the same length, the effect is exactly the same as using a one-time pad: the ciphertext reveals no information about the plaintext.

<u>Question 2:</u> (**20 points**) Find the smallest positive integer x which leave a remainder of 1, 2, 3, and 4 when divided by 5, 7, 9, and 11 respectively. (Hint: use the Chinese Remainder Theorem (CRT)

CRT: Let m_1, m_2... m_k be a pairwise relatively prime integers. If a_1, a_2, …, a_k are any integers, then there exists a unique integer x modulo $M = m_1m_2 \ldots m_k$, that satisfies the system of linear congruencies

$$x \equiv a_1 \bmod m_1$$
$$x \equiv a_2 \bmod m_2$$
$$\ldots.$$
$$x = a_k \bmod m_k$$

Moreover, $x = a_1M_1y_1 + a_2M_2y_2 + \ldots + a_kM_ky_k (\mathrm{mod}\ M)$,
where M_i=M/m_i and $M_i\, y_i = 1 \bmod m_i$ for $i = 1,2, \ldots, k$

We are asked to solve the system of congruences:

x ≡ 1 (mod 5)

x ≡ 2 (mod 7)

x ≡ 3 (mod 9)

x ≡ 4 (mod 11)

Notice that the moduli are pairwise relatively prime, as required by the theorem.

We have M = 5 · 7 · 9 · 11 = 3465 and

M1 = M/5 = 693

M2 = M/7 = 495

M3 = M/9 = 385

M4 = M/11 = 315.

A small calculation gives

y1 = 2

y2 = 3

y3 = 4

y4 = 8.

Hence

x = 1 · 693 · 2 + 2·495·3+ 3·385·4+ 4·315·8 = 19056.

So

x = 19056 mod M = 1731 mod M.

In fact, 1731 is the smallest positive integer solution. The full solution is x ≡ 1731 (mod M).

Question 3: (**20 points**) Vigenere and Playfair Cipher

1. Decrypt the ciphertext PVWMAMKOBUXGAZXMFDIL. It was encrypted using the Vigenere cipher with the keyword "TRAIN".

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext = Cipher – Key

Cipher	P	V	W	M	A	M	K	O	B	U	X	G	A	Z	X	M	F	D	I	L
	15	21	22	12	0	12	10	14	1	20	23	6	0	25	23	12	5	3	8	11
Key	T	R	A	I	N	T	R	A	I	N	T	R	A	I	N	T	R	A	I	N
	19	17	0	8	13	19	17	0	8	13	19	17	0	8	13	19	17	0	8	13
Plaintext	-4	4	22	4	-13	-7	-7	14	-7	7	4	-11	0	17	10	-7	-12	3	0	-2
	22	4	22	4	13	19	19	14	19	7	4	15	0	17	10	19	14	3	0	24
	W	E	W	E	N	T	T	O	T	H	E	P	A	R	K	T	O	D	A	Y

We went to the park today

2. Construct a table for the Playfair Cipher with the keyword EFFECTIVENESS? Encrypt the phrase: “INFORMATIONSECURITY”

E	**F**	**C**	**T**	**I/J**
V	**N**	**S**	A	B
D	G	H	K	L
M	O	P	Q	R
U	W	X	Y	Z

Using X as a break letter

Plaintext	IN	FO	RM	AT	IO	NS	EC	UR	IT	YX

Ciphertext	FB	NW	MO	KA	FR	SA	FT	ZM	EI	ZY

<u>Question 4:</u> (**20 points**) AES Cipher

Let the input to the MixCols (during AES encryption) be $\begin{bmatrix} A0 & 74 & \mathbf{65} & B7 \\ 2B & 8D & \mathbf{2E} & C6 \\ 99 & 1F & \mathbf{C8} & EB \\ C5 & E5 & \mathbf{F7} & 23 \end{bmatrix}$.

Using multiplication in the field defined in AES GF(2^8) with irreducible polynomial $x^8+x^4+x^3+x+1$,

what is the output in row 2 col 3 in hexadecimal? (The matrix by which to “multiply” is $\begin{bmatrix} 02 & 03 & 01 & 01 \\ \mathbf{01} & \mathbf{02} & \mathbf{03} & \mathbf{01} \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$

01.65 $\oplus$ 02.2E $\oplus$ 03. C8 $\oplus$ 01. F7

01. 65 = **0110 0101**

02. 2E = {10}. {0010 1110} = **0101 1100**

03. C8 = {11}.{1100 1000} = 1100 1000

1001 0000 $\oplus$

0101 1000

0001 1011 $\oplus$

0100 0011 **0100 0011**

01. F7 = **1111 0111**

10000 1101= (8D)

جامعة بيرزيت
BIRZEIT UNIVERSITY
Faculty of Engineering and Technology
Electrical and Computer Engineering Department

ENCS 532: Data and Network Security
Midterm Exam
Tuesday , 11/04/2017
Time: 14:00 - 15:30

Dr. Ahmad Alsadeh

Student's Name: **ID**:

Question 1: Classical Encryption

1) (**10 pts**) The ciphertext "PAPCIJGXCV" was encrypted using the shift cipher with an encryption key of 15. What is the corresponding plaintext?

2) (**10 pts**) Encrypt the plaintext "WEAREWORKING" using the Vigenere cipher and the keyword "HOUSE".

3) (**10 pts**) Encrypt "LASTQUESTION" using the playfair cipher and the keyword "LEMONS".

Question 2: Number Theory

1) (**10 pts**) Determine 59^{-1} mod 107

2) (**10 pts**) Use the Chinese Remainder Theorem (CRT) for solving the system of congruences:
   $x \equiv 1 \pmod 3$
   $x \equiv 2 \pmod 5$
   $x \equiv 3 \pmod 7$

3) **(10 pts)** Determine the product of the two polynomials $x^4 + x^2 + 1$ and $x^5 + x^3 + x + 1$ with coefficients in $\mathbb{Z}_2$ mod $x^8 + x^4 + x^3 + x + 1$.

4) **(10 pts**) The Miller-Rabin Primality Test is shown below. Apply the test for 49.

Question 3: DES and AES Ciphers

1) **(10 pts)** Draw and label the basic structure of a single round of a Feistel cipher.

2) **(10 pts)** Consider the process of AES Key Expansion. Imagine that we have:
   w[36] = 3A 74 E5 8D (in hex)
   w[39] = 8F 17 60 C2 (in hex)

   Calculate w[40], showing each of the following intermediate results.

3) (**10 pts**) In the AES Mix Columns operation, multiplication between terms must be performed. These multiplications are really in the field GF(2^8) with irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. Perform the following two multiplications in that field:
   a) 03 x D3
   b) 04 x C9

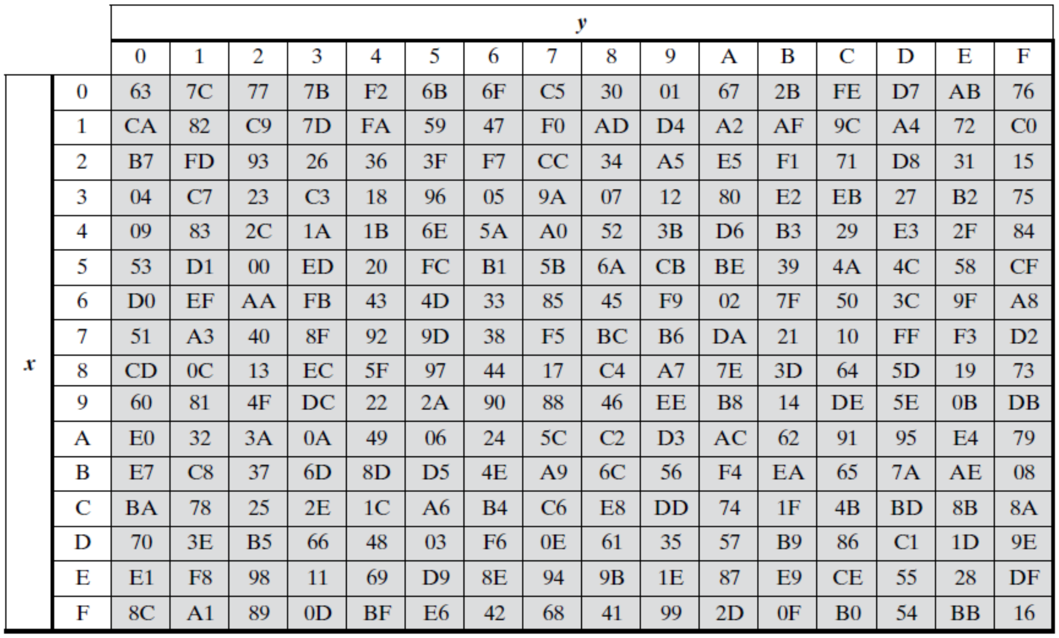
Reference Sheet

Miller–Rabin primality test

```
Input: $n > 2$, an odd integer to be tested for primality;
       $k$, a parameter that determines the accuracy of the test
Output: composite if $n$ is composite, otherwise probably prime
write $n-1$ as $2^s \cdot d$ with $d$ odd by factoring powers of 2 from $n-1$
LOOP: repeat $k$ times:
    pick $a$ randomly in the range $[2, n - 1]$
    $x \leftarrow a^d \bmod n$
    if $x = 1$ or $x = n - 1$ then do next LOOP
    for $r = 1 .. s - 1$
        $x \leftarrow x^2 \bmod n$
        if $x = 1$ then return composite
        if $x = n - 1$ then do next LOOP
    return composite
return probably prime
```

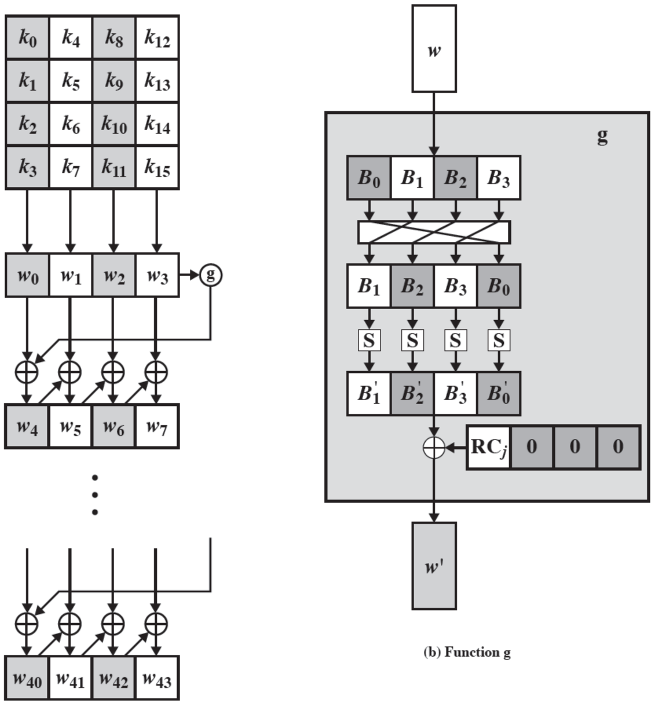
Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Number	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Number	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**

AES S-Box



		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

AES Key Expansion



(b) Function g

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

BIRZEIT UNIVERSITY
Faculty of Engineering and Technology
Electrical and Computer Engineering Department

ENCS 532: Data and Network Security
Midterm Exam
Sunday , 19/11/2017
Time: 8:00 - 9:30

Dr. Ahmad Alsadeh

Student's Name: **ID**:

Problem 1 (20 pts): Classical Encryption

1) (**5 pts**) Use the shift cipher to encrypt the plaintext "CRYPTO" with a key of 9.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext	C	R	Y	P	T	O
	2	17	24	15	19	14
Cipher= Key + Plaintext	11	26	33	24	28	23
Cipher mod 26	11	0	7	24	2	23
	L	A	H	Y	C	X

2) (**5 pts**) The MOGZD ciphertext was encrypted using the Vigenere cipher with the keyword "FORK". What was the original plaintext?

Plaintext Ciphertext	M	O	G	Z	D
	12	14	6	25	3
	F	O	R	K	F
Key	5	14	17	10	5
Plaintext =Cipher- Key	7	0	-11	15	-2
Plaintext mod 26	7	0	15	15	24
	H	A	P	P	Y

3) (**10 pts**) Using the Playfair cipher with keyword " DECRYPTION" decrypt the message NBNMNMSCLCQZKHBR

D	**E**	**C**	**R**	**Y**
P	**T**	**I**	**O**	N
A	B	F	G	H
K	L	M	Q	S
U	V	W	X	Z

Ciphertext	NB	NM	NM	SC	LC	QZ	KH	BR
Plaintext	TH	IS	IS	MY	ME	SX	SA	GE

Plaintext **: This is my message**

Problem 2 (30 pts): Number Theory

1) (**8 pts**) Use the Extended Euclidean Algorithm to and the greatest common divisor of 1394 and 337 and write it as an integer linear combination of 1394 and 337. (**2 pts**) Does 337 have a multiplicative inverse modulo 1394? If so, what is it?

r_i	q_i	x_i	y_i
1394	--	1	0
337	--	0	1
46	4	1	-4
15	7	-7	29
1	3	22	-91
0			

GCD(1394,337) = 1 = (22)1394 + (-91) 337

337^{-1} mod 1394 = -91 = 1303 mod 1394

2) (**10 pts**) Suppose that $x \equiv 7 \bmod 8$, $x \equiv 10 \bmod 11$, and $x \equiv 3 \bmod 5$. Find $x \bmod 440$ using Chinese Remainder Theorem (CRT).

gcd(8,11)=1
gcd(8,5)=1
gcd(5,11)=1

a_i	M=8×11×5= 440	y_i	$a_iM_iy_i$
a_1=7	M_1=55	7^{-1} mod 8= 7	2695
a_2=10	M_2 =40	7^{-1} mod 11= 8	3200
a_3=3	M_3=88	3^{-1} mod 5= 2	528
			6423

$$x=a_1M_1y_1+ a_2M_2y_2 + a_3M_3y_3 \ (\text{mod } M)$$

6423 mod 440 = 263

3) (**10 pts**) Compute $(345^{28567} \times 23^{567} + 1078) \bmod 29$ given that 29 is a prime.

$(345^{1020\times28+7} \times 23^{20\times28+7} + 1078) \bmod 29$

$\text{Ø}(p)=p-1;\ a^{\text{Ø}(n)} = 1(\bmod n)$

$\text{Ø}(29)=28$

$(345^{1020\times28+7} \times 23^{20\times28+7} + 1078) \bmod 29$

$(345^{7} \times 23^{7} + 1078) \bmod 29$

$(23\times3\times5)^{7}\times23^{7}+(2\times 7\times7\times 11) \bmod 29$

$(23\times3\times5)^{7}\times23^{7}+(2\times 7\times7\times 11) \bmod 29$

$(3\times5)^{7}\times23^{2\times7}+ (2\times 7^{2}\times 11) \bmod 29$

$(12\times28) \bmod 29 \times1+ (2\times20\times11) \bmod 29$

$(17 \times 1 + 5) \bmod 29$

$22 \bmod 29$

Problem 3 (10 pts): DES Cipher

1) (**2 pts**) Alice and Bob are passing messages encrypted with DES. C=Encrypt(K,M). Consider the following S-Box for the DES algorithm:

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Given input $(100011)_2$, the output of the S-Box is: ________**12**__________

Row = 11_2 : 3

Col = 0001_2 : 1

2) (**3 pts**) If Trudy obtained a plaintext/ciphertext pair, how many cryptographic operations would she need to perform to find Alice and Bob's shared key K?

2^{56} encrypt or decrypt operations

3) (**5 pts**) Alice and Bob know that double encrypting with the same algorithm doesn't provide much additional protect. Alice suggested using the NOTDES algorithm which operates with a 32 bit key with the DES algorithm, i.e. C=NOTDES-Encrypt(K_1,DES-Encrypt(K_2,M)). If Eve has a plaintext/ciphertext pair, how many cryptographic operations would she need to perform to recover the keys?

Meet in the middle still works.
The attacker would brute force the DES key performing 2^{56} encryptions.
The attacker would in addition perform a NOTDES decrypt using the first (or last or some fixed subset of) 32 bits in the current 56 bit key.

Results in 2^{57} encrypt/decrypt operations. Or 2^{56} + 2^{32} encrypt/decrypt operations if we are being clever about not rechecking if the selected 32 bits in the current 56 bit key have been checked.

<u>Problem 4 (10 pts)</u>: AES Cipher

In the mix columns operation of AES, "multiplications" such as $03 \cdot C5$ have to be performed. We covered the mechanism for doing this, (which really involves a number of XORs). What is the value (in HEX) of $03 \cdot C5$? (Note: The polynomial used in AES is $x^8 + x^4 + x^3 + x + 1$.

```
    1100  0101
            11
    -------------
    1100  0101
  1 1000 1010   ⊕
  1 0100 1111

 1 0100 1111
 1 0001 1011
0 0101  0100
```

$(54)_{Hex}$

<u>Problem 5 (10 pts)</u>: Mode of Operations

Consider the following encryption mode for applying AES-128 with a key *k* to a message M that consists of 128-bit blocks, M_1, M_2, … , M_l. The sender first picks a random 128-bit string, C_0, which is the first block of ciphertext. Then for i > 0, the ith ciphertext block is given by $C_i = C_{i-1} \oplus AES128_k(k, M_i)$. The ciphertext is the concatenation of these individual blocks: $C = C_0 \parallel C_1 \parallel C_2 \parallel . . . \parallel C_l$

1) (**2 pts**) What is the intent behind the random value C_0? (i.e., what is it meant to achieve.

C_0 is an *Initialization Vector*. The intent behind using it is to ensure that if the same text is encrypted in two distinct messages, the ciphertexts will differ, so an eavesdropper cannot infer the relationship between the messages.

2) (**4 pts**) Is this mode of encryption secure? If so, state what desirable properties it has that make it secure. If not, sketch a weakness.

It is not secure. Since the ciphertext is visible to an eavesdropper, the eavesdropper knows C_i for all values of *i*. This allows them to directly determine AES-128$_K$(M_i) for all *i* due to the inverse nature of exclusive-or ⊕, which makes the scheme equivalent to ECB in terms of revealing whenever two message blocks contain the same text.

Another valid criticism is that because the scheme uses the Initialization Vector C_0 in a *reversible* manner, an attacker can deduce when two separate ciphertexts in fact encode the same text.

3) (**4 pts**) Suppose we replace the computation of C_i with $C_i = AES128_K(C_{i-1} \oplus M_i)$. Does this make the mode of encryption more secure, less secure, or unchanged? Briefly explain your answer.

The mode is more secure. This alternate form is exactly the definition of CBC mode, which has been proven secure in the face of chosen plaintext attacks.

Good luck!

جامعة بيرزيت
BIRZEIT UNIVERSITY

Electrical and Computer Engineering Department

First Semester 2018

ENCS 532: Data and Network Security
Midterm Exam

Time: 09:45 - 11:15 (90 minutes) Date: Sunday, 18/11/2018 Room: Masri109

Dr. Ahmad Alsadeh

Student Name: _____________**Key**____________________**Student ID**: ______________

Question #	**Full Mark**	**Student's Mark**
Q1	**20**	
Q2	**25**	
Q3	**25**	
Q4	**20**	
TOTAL	**90**	

Question 1 (20): General

1. A loss of ___________ is the unauthorized disclosure of information.

A. trust
B. integrity
C. authenticity
D. reliability
E. confidentiality

2. If the information has been a subject of an unauthorized modification then we say that it lost its___.

A. purity (نقاء)
B. integrity
C. reliability
D. validity
E. originality

3. If a cipher has the property that given limited computing resources (for example time needed for calculations is greater than age of universe), the cipher cannot be broken, then the cipher is offering a(n) _____ .

A. unconditional security
B. conditional security
C. computational security
D. ultimate security
E. universal security

4. The Shannon principle of "*diffusion*"

A. makes relationship between ciphertext and key as complex as possible
B. diffuses the plaintext among huge subset of plaintexts
C. dissipates statistical structure of plaintext over bulk of ciphertext.
D. diffuses the key and the plaintext among a subset of plaintexts

5. What is the block cipher structure in DES?

A. SAC
B. Shannon
C. Feistel
D. Rendell
E. One Way Permutation

6. The function F provides the element of ___________ in a Feistel cipher.

A. clarification
B. alignment
C. confusion
D. stability
E. amplification

7. A _________ attack involves trying every possible key until an intelligible translation of the ciphertext is obtained.

- **A. brute-force**
- B. Caesar attack
- C. ciphertext only
- D. chosen plaintext
- E. replay attack

8. The RC4 stream cipher is:

- A. bit oriented
- **B. byte oriented**
- C. 16 bit oriented
- D. Big-endian oriented
- E. Little-endian oriented

9. An encryption scheme that requires large quantities of random keys that are as long as the messages that have to be encrypted, and are distributed on a regular basis to both sender and receiver, is known as:

- A. Key-pad scheme
- B. iPad scheme
- C. crypto-pad scheme
- D. time-pad scheme
- **E. one-time pad scheme**

10. What is correct?

- A. DES uses a 56-bit message block and a 64-bit key.
- B. DES uses a 56-bit message block and a 48-bit key.
- **C. DES uses a 64-bit message block and a 56-bit key.**
- D. DES uses a 64-bit message block and a 64-bit key.
- E. DES uses a 128-bit message block and a 64-bit key.

11. The size of the block in AES is:

- A. 64 bits
- **B. 128 bits**
- C. 192 bits
- D. 250 bits
- E. 256 bits

12. In AES, the cipher consists of N rounds, where the number of rounds depends on the ______.

- **A. key length**
- B. output matrix
- C. State
- D. number of columns
- E. S-boxes

13. Using a one-time pad for encryption, followed by a CBC-MAC on the resulting ciphertext, provides

A. unconditional secrecy and computationally secure authentication
B. conditional secrecy and computationally secure authentication
C. conditional secrecy and computationally insecure authentication
D. security compromising computationally secure authentication
E. security compromising computationally insecure authentication

14. 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
E. Differential cryptanalysis attack

15. If by $E_K(\ )$ we denote the encryption function of a block cipher with a key K, and if the mode of operation is $C_i = E_K (P_i \oplus C_{i-1})$ then the mode of operation is ______.

A. Cipher Feedback (CFB)
B. Electronic Codebook (ECB)
C. Cipher Block Chaining (CBC)
D. Output Feedback (OFB)
E. Counter (CTR)

16. You are encrypting with AES in ECB mode. You encrypt plaintext blocks A, B, C, D, E. However, the D block is garbled during transmission; in particular, the high-order bit is flipped. Which blocks can the receiver successfully decrypt?

A. Receiver will get only block A correctly
B. Receiver will get only block B correctly
C. Receiver will get only block E correctly
D. Receiver will get only block D correctly
E. Receiver will get blocks A, B, C, and E correctly

17. If an efficient algorithm for factoring large numbers is discovered, which of the following schemes will be known to be not secure:

A. Advanced Encryption Standard (AES)
B. Diffie-Hellman
C. RSA
D. El Gamal
E. Elliptic-curve cryptography (ECC)

18. In RSA, for a given modulus N, any prime larger than 2 may be used as the public exponent e if

A. e is relatively prime N
B. e is relatively prime to $\varphi(N)$
C. e is odd number
D. e is even number
E. e is positive number

19. On which claimed unsolved mathematical “hard problem” is the ElGamal cryptosystem based?

A. Discrete logarithm problem
B. Integer factoring
C. Elliptic Curve Discrete Logarithm Problem
D. Discrete exponential problem
E. Discrete linear problem

20. Alice wishes to send a confidential and signed message to Bob using public key cryptography. Which is correct:

A. Alice signs with her public key, and encrypts with her private key
B. Alice signs with her public key and encrypts with Bob’s public key
C. Alice signs with her private key and encrypts with Bob’s public key
D. Alice signs with Bob’s public key and encrypts with her private key
E. Alice signs with Bob’s public key and encrypts with Bob’s private key

Question 2 (25): Number Theory

1. (**5** pts) What is Ø(6300)?

φ(6300) = φ(9) φ(7) φ(25) φ(4);

φ(6300) = φ(3^2). φ(7). φ(5^2). φ(2^2), note that $ø(pk) = pk - p^{k-1} = p^{k-1}\,(p-1)$

φ(6300)= 6x6x20x2 = 1440

2. (**6 pts**) Calculate 3^{64} modulo 67 using Fermat's little theorem.

We know $3^{66} \equiv 1$ (mod 67).
So $3^2 \cdot 3^{64} \equiv 1$ (mod 67) .
so we just need to invert 9 mod 67.
You can either do this by the Euclidean algorithm

		q_i	x_i	y_i
	67		1	0
	9		0	1
1	4	7	1	-7
2	1	2	-2	15

(15)(9) mod 67 = 1 , thus $9^{-1} \equiv 15$ (mod 67)

Or by inspection. For example, 67 · 2 + 1 = 135 = 15.9, so it follows that $9^{-1} \equiv 15$ (mod 67).

3. (**6 pts**) show that 3 is a generator mod 7.

3^1 = 3 mod 7 = 3

3^2 = 9 mod 7 = 2

3^3 = 2x3 mod 7 = 6

3^4 = 6x3 mod 7 = 4

3^5 = 4x3 mod 7 = 5

3^6 = 5x3 mod 7 = 1

{1, 2, 3, 4, 5, 6} the set has be generated
Thus, 3 is a generator.

4. (**8 pts**) Using the Chinese Remainder Theorem, find all solutions to the following system:

$$2x \equiv 3 \pmod 7$$
$$4x \equiv 5 \pmod 9$$

$2x \equiv 3 \bmod 7$

$x \equiv 3.2^{-1} \bmod 7,\ \ 2^{-1} \bmod 7 = 4$

$x \equiv 3.4 \bmod 7$

$\underline{x \equiv 5 \bmod 7}$

$4x \equiv 5 \bmod 9$

$x \equiv 5\ .\ 4^{-1} \bmod 9,\ 4^{-1} \bmod 9 = 7$

$x \equiv 5\ .\ 7 \bmod 9$

$\underline{x \equiv 8\ \bmod 9}$

	ai	$M = 7 \times 9 = 55$	yi	$aiMiyi$
mod 7	**5**	**9**	**4**	**180**
mod 9	**8**	**7**	**4**	**224**
				404

404 mod 63 = 26

Question 3 (25): DES and AES Ciphers with its mode of operations

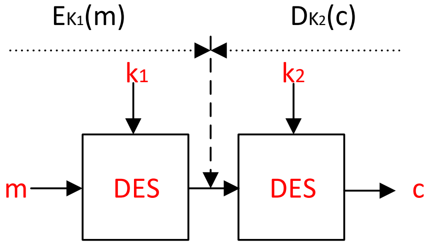
1. (**6 pts**) Consider a sensor X that periodically sends a 64-octet measurement to a receiver Y. One day the administrator decides that X should encrypt the measurement data using DES in CBC mode. How many octets does X now send for each measurement? Explain your answer.

   DES takes a 8-octet (64-bit) plaintext block and yields a 8-octet cipherblock. [2 points]
   CBC requires a 8-octet initialization vector (IV) to be sent along with the cipherblocks. [2 points]
   So X now sends 64 octets of cipherblocks [1 point]
   plus 8 octets of IV, for a total of 72 octets. [1 point]

   [3 points if you don't say anything wrong and you say that CBC sends cipherblocks + IV.]

2. (**6 pts**) Explain why "Double-DES" would not be as effective as a strong cipher system with a 112-bit key. (Note: Double-DES with two DES keys would have a total of 112 bits between the two keys.)

   Due to meet in the middle attack, which takes not much more time than 2^{56} (but it requires a lot of memory in turn).



   Given a plaintext-ciphertext pair (m, c), write two lists of length 2^{56} each.

   $2^{56} + 2^{56} = 2*2^{56} = 2^{57}$

3. (**4 pts**) Given the following state matrix right before the shift row operation in AES, show the state matrix right after the shift row operation:

```
4F  71  90  EA
F3  D6 46  2B
85  7E  99  1C
84  57  6C  95
```

4F	**71**	**90**	**EA**	
D6	**46**	**2B**	**F3**	1-byte circular left shift
99	**1C**	**85**	**7E**	2-byte circular left shift
95	**84**	**57**	**6C**	3-byte circular left shift

4. (**6 pts**) In the mix columns operation of AES, "multiplications", such as 03. C5 have to be performed. We covered the mechanism for doing this, (which really involves a number of XORs). What is the value of 03. C5 in HEX? (Note: The irreducible polynomial used in AES is $x^8 + x^4 + x^3 + x + 1$ with coefficients in Z_2.

```
1100 0101
       11
  -------------
  1100 0101
1 1000 1010
1 0100 1111
1 0100 1111
1 0001 1011
0 0101 0100
```

(54)Hex

5. (**3 pts**) In the key expansion algorithm of AES, if w[26] = AE8F236B and w[23] = 6AB57C93, what is w[27]?

Since 27 isn't divisible by 4, all we need to do is XOR the two given values:

1010   1110 1000 1111 0010 0011 0110 1011

0110   1010 1011 0101 0111 1100 1001 0011

1100   0100 0011 1010 0101 1111 1111 1000

In Hex, this is C43A 5FF8.

Question 4 (20): Public Key Encryptions

1. (**10 pts**) Perform the following RSA key generation steps. Each step must satisfy the requirements for a legitimate RSA key.

(a) (2 pts) Suppose *n* is 55. Find suitable *p* and *q* values.

p = 5 and q = 11.

(b) (2 pts) Compute *Ø(n)*.

$\varphi(n) = (p-1)(q-1) = 4 * 10 = 40$.

(c) (6 pts) If *d* = 7, compute a valid value for *e* and specify the public and private keys.

d*e mod $\varphi(n)$ = 7 ∗ e mod40 (2pt)

By using Extended Euclidean Algorithm

ri	qi	xi	yi
40	*	1	0
7	*	0	1
5	5	1	-5
2	1	-1	6
1	2	3	-17
0	2		

(3)40 + (-17)7 =1

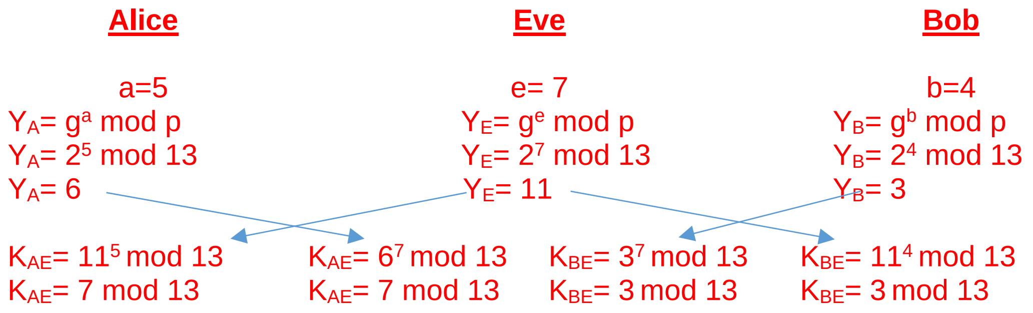
7^{-1} mod 40 = -17 mod 40 = 23

7*e mod 40 = 1 when e = 23

Private key is {7, 55} (1pt)
public key is {3, 55}. (1pt)

2. (**10 pts**) Suppose Alice and Bob wish to do Diffie-Hellman key exchange. Alice and Bob have agreed upon a prime p = 13, and a generator g = 2. Alice has chosen her private exponent to be a = 5, while Bob has chosen his private exponent to be b = 4. Unknown to Alice and Bob, Eve is listening and is able to intercept their messages as well as inject her own messages. Suppose Eve chooses an exponent e = 7. Explain how Eve can use *e* to perform the Intruder-in-the-Middle attack on the Alice-Bob Diffie-Hellman key exchange.

D.H general parameters
P=13, g=2



Alice

a=5
$Y_A = g^a \bmod p$
$Y_A = 2^5 \bmod 13$
$Y_A = 6$

Eve

e= 7
$Y_E = g^e \bmod p$
$Y_E = 2^7 \bmod 13$
$Y_E = 11$

Bob

b=4
$Y_B = g^b \bmod p$
$Y_B = 2^4 \bmod 13$
$Y_B = 3$

$K_{AE} = 11^5 \bmod 13$
$K_{AE} = 7 \bmod 13$

$K_{AE} = 6^7 \bmod 13$
$K_{AE} = 7 \bmod 13$

$K_{BE} = 3^7 \bmod 13$
$K_{BE} = 3 \bmod 13$

$K_{BE} = 11^4 \bmod 13$
$K_{BE} = 3 \bmod 13$

Electrical and Computer Engineering Department

Second Semester 2018

ENCS 532: Data and Network Security
Midterm Exam

Time: 08:00 - 09:30 (90 minutes) Date: 22/04/2018 Room: Al-Juraysi001

Dr. Ahmad Alsadeh

Student Name: ____________**Key**___________________**Student ID**: _____________

Question #	**Full Mark**	**Student's Mark**
Q1	**30**	
Q2	**40**	
Q3	**30**	
TOTAL	**100**	

Question 1 (30): Classical Encryption

1. (**10 pts**) You have intercepted a message encrypted with Vigenere and have managed to determine the corresponding plaintext. The ciphertext is “kcszjwvfabdlzgzslsygym” and the corresponding plaintext is “sallywenttotheseashore”. What is the key?

K –S = 10 –18 = -8 ≡ 18	**(S)**
C –A = 2 –0 = 2	**(C)**
S –L = 18 –11 = 7	**(H)**
Z –L = 25 –11 = 14	**(O)**
J –Y = 9 –24 = 15 ≡ 11	**(L)**
W –W = 22 –22 = 0	**(A)**
V –E = 21 –4 = 17	**(R)**
F –N = 5 –13 = -8 ≡ 18	**(S)**
A –T = 0 –19 = -19 ≡ 7	**(H)**
B –T = 1 –19 = -18 ≡ 8	**(I)**
D –O = 3 –14 = -11 ≡ 15	**(P)**
L –T = 11 –19 = -8 ≡ 18	**(S)**

Z –H = 25 –7 = 18	**(S)**
G –E = 6 –4 = 2	**(C)**
Z –S = 25 –18 = 7	**(H)**
S –E = 18 –4 = 14	**(O)**

Keyword: SCHOLARSHIPS

2. (**10 pts**) You are attempting to decrypt a cipher created using the Playfair cipher. Your ciphertext is "FMQWSWIQTENMCV" and you have stolen the key used for encryption. It is as follows:

T	E	L	G	R
A	M	B	C	D
F	H	I	K	N
O	P	Q	S	U
V	W	X	Y	Z

What is the plaintext that corresponds to the ciphertext above?

FM = HA
QW = PX
SW = PY
IQ = BI
TE = RT
NM = HD
CV= AY

Plaintext: HAPPY BIRTHDAY

3. (**10 pts**) Using the encryption matrix $\begin{pmatrix} 7 & 4 \\ 3 & 5 \end{pmatrix}$ for the Hill cipher, what is the result of encrypting the plaintext "CIPHER"?

$$\begin{bmatrix} C \\ I \end{bmatrix} = \begin{bmatrix} 2 \\ 8 \end{bmatrix}, \qquad \begin{bmatrix} P \\ H \end{bmatrix} = \begin{bmatrix} 15 \\ 7 \end{bmatrix}, \qquad \begin{bmatrix} E \\ R \end{bmatrix} = \begin{bmatrix} 4 \\ 17 \end{bmatrix}$$

$$\begin{bmatrix} 7 & 4 \\ 3 & 5 \end{bmatrix} * \begin{bmatrix} 2 \\ 8 \end{bmatrix} = \begin{bmatrix} 7 \times 2 + 4 \times 8 \\ 3 \times 2 + 5 \times 8 \end{bmatrix} = \begin{bmatrix} 46 \\ 46 \end{bmatrix} = \begin{bmatrix} 20 \\ 20 \end{bmatrix} = \begin{bmatrix} U \\ U \end{bmatrix}$$

$$\begin{bmatrix} 7 & 4 \\ 3 & 5 \end{bmatrix} * \begin{bmatrix} 15 \\ 7 \end{bmatrix} = \begin{bmatrix} 7 \times 15 + 4 \times 7 \\ 3 \times 15 + 5 \times 7 \end{bmatrix} = \begin{bmatrix} 133 \\ 80 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix} = \begin{bmatrix} D \\ C \end{bmatrix}$$

$$\begin{bmatrix} 7 & 4 \\ 3 & 5 \end{bmatrix} * \begin{bmatrix} 4 \\ 17 \end{bmatrix} = \begin{bmatrix} 7 \times 4 + 4 \times 17 \\ 3 \times 4 + 5 \times 17 \end{bmatrix} = \begin{bmatrix} 96 \\ 97 \end{bmatrix} = \begin{bmatrix} 18 \\ 19 \end{bmatrix} = \begin{bmatrix} S \\ T \end{bmatrix}$$

Ciphertext: UUDCST

Question 2 (40): Number Theory and Finite Fields

1. (**10 pts**) Use the Extended Euclidean Algorithm to and the greatest common divisor of 112 and 163 and write it as an integer linear combination of 112 and 163. Does 112 have a multiplicative inverse modulo 163? If so, what is it?

r_i	q_i	x_i	y_i
163		1	0
112		0	1
51	1	1	-1
10	2	-2	3
1	5	11	-16

1= 163 (11) + 112(-16)

Yes. The 112^{-1} mod 163 = -16 mod 163 = 147 mod 163

2. (**7** pts) What is φ(888)?

φ(888) = φ(8) φ(3) φ(37); **$\varphi(8) = \varphi(2^3) = 2^{3-1}(2-1) = 4$**

φ(888)= 4. 2. 36 = 288

3. (**7 pts**) Using Fermat's Theorem, determine 171^{3822} mod 383.

$a^{p-1} \equiv 1$ mod p

$171^{10(382)+2}$ mod 383

1. 171^2 mod 383

29241 mod 383 = 133

4. (**6 pts**) Prove that 2 is a generator mod 13.

2^1 = 2 mod 13 = 2

2^2 = 4 mod 13 = 4

2^3 = 8 mod 13 = 8

2^4 = 16 mod 13 = 3

2^5 = 32 mod 13 = 6

2^6 = 64 mod 13 = 12

2^7 = 128 mod 13 = 11

2^8 = 256 mod 13 = 9

2^9 = 512 mod 13 = 5

2^{10} = 1024 mod 13 = 10

2^{11} = 2048 mod 13 = 7

2^{12} = 4096 mod 13 =1

$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ the set has be generated
Thus, 2 is a generator.

5. (**10 pts**) Using the Chinese Remainder Theorem, find all solutions to the following system:

$$2x \equiv 3 \bmod 5$$
$$x \equiv 5 \bmod 11$$

$2x \equiv 3 \bmod 5$, $x \equiv 3.2^{-1} \bmod 5$, $2^{-1} \bmod 5 = 3$

$x \equiv 3.2^{-1} \bmod 5$ → $x \equiv 9 \bmod 5$

$x \equiv 9 \bmod 5$
$x \equiv 5 \bmod 11$

	ai	$M = 5 \times 11 = 55$	yi	$aiMiyi$
mod 5	**9**	**11**	**1**	**99**
mod 11	**5**	**5**	**9**	**255**
				324

324 mod 55 = 49

Question 3 (30): DES and AES Ciphers with its mode of operations

1. (**3 pts**) Consider the following S-Box for the DES algorithm:

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

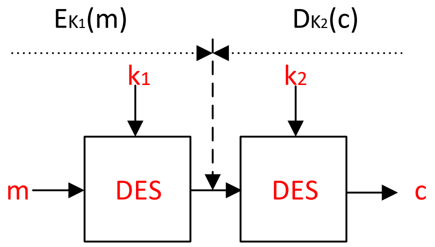
Given input $(110011)_2$, the output of the S-Box is:

Row = 11 col= 1001

The output is 11

2. (**5 pts**) Explain why "Double-DES" would not be as effective as a strong cipher system with a 112-bit key. (Note: Double-DES with two DES keys would have a total of 112 bits between the two keys.)

Due to meet in the middle attack, which takes not much more time than 2^{56} (but it requires a lot of memory in turn).



Given a plaintext-ciphertext pair (m, c), write two lists of length 2^{56} each.

$2^{56} + 2^{56} = 2*2^{56} = 2^{57}$

3. (**4 pts**) Given the following state matrix right before the shift row operation in AES, show the state matrix right after the shift row operation:

4F 71 90 EA
F3 D6 46 2B
85 7E 99 1C
84 57 6C 95

4F	**71**	**90**	**EA**	
D6	**46**	**2B**	**F3**	1-byte circular left shift
99	**1C**	**85**	**7E**	2-byte circular left shift
95	**84**	**57**	**6C**	3-byte circular left shift

4. (**7 pts**) Determine the product of the two polynomials $x^4 + x^2 + 1$ and $x^5 + x^3 + x + 1$ with coefficients in Z_2 mod $x^8 + x^4 + x^3 + x + 1$.

$x^4 + x^2 + 1$ and $x^5 + x^3 + x + 1$ => 101011

$x^4 + x^2 + 1$ => 10101

```
     101011
   10101100
 1010110000
 1000110111
```

```
1000110111
1000110110 xor
0000000001
```

Answer = 1

5. (**7 pts**) In the key expansion algorithm of AES, if w[26] = AE8F236B and w[23] = 6AB57C93, what is w[27]?

Since 27 isn't divisible by 4, all we need to do is XOR the two given values:

```
1010   1110 1000  1111  0010  0011  0110  1011
0110   1010 1011  0101  0111  1100  1001  0011
______________________________________________
1100   0100 0011  1010  0101  1111  1111 1000
```

In Hex, this is C43A 5FF8.

6. (**4 pts**) The largest version of AES uses a 256 bit key. How many keys would have to be searched per second in order for a brute force attack to break this version of AES in ten years? Express your answer in scientific notation. Please show your work. Write down answers from your calculator.

Number of keys = 2^{256}
Seconds in ten years = 60 sec/min x 60 min/hr x 24 hr/day x 365.25 day/year x 10 years
= 315576000 sec/(10 years)

Keys per second = 2^{256}/315576000 ~ 3.669 x 10^{68}