November 8th, 2018

German University in Cairo
Media Engineering and Technology
Lecturer: Mervat AbuElkheir
TA: Mohamed Abdelrazik

Information Security

Winter term 2018
2nd Chance Midterm Exam

Bar Code

Instructions: Read carefully before proceeding.

1) Duration of the exam: 2 hours (120 minutes).
2) (Non-programmable) Calculators are allowed.
3) No books or other aids are permitted for this test.
4) This exam booklet contains 10 pages, including this one. **Note that if one or more pages are missing, you will lose their points. Thus, you must check that your exam booklet is complete.**
5) Write your solutions in the space provided. If you need more space, write on the back of the sheet containing the problem or on the extra sheets and make an arrow indicating that.
6) When you are told that time is up, stop working on the test.
7) Include any assumptions that you need to make.
8) Follow the instructions of your proctors under all circumstances.

Good Luck!

Don't write anything below ;-)

	1	2	3	4	5	Σ
Marks	10	10	10	10	10	50
Final Marks						

Question 1:

Specify if the following statements are True (T) or False (F). If you need to justify your answer, please do so in the space provided.

1) The one-time pad is not practical to implement.	T
2) Stream ciphers are suitable for real-time applications.	T
3) In cryptography, diffusion is to make the relationship between the ciphertext and the key as complex as possible.	F
4) Non repudiation is a service to ensure an entity in the system cannot deny their actions.	T
5) Asymmetric cryptography can never be used to provide authentication.	F
6) Rotor machines rely on multiple stages of permutation.	F
7) In link encryption, the routers need to know the key in order to forward the message.	T
8) The Feistel cipher is based on multiple stages on substitution and permutation.	T
9) In cipher block chaining (CBC), an error occurring in a block of ciphertext at the receiver will result in all subsequent blocks to be decrypted incorrectly.	F
10) Digital envelopes use public key cryptography to send a message along with a symmetric key.	T

Extra space for justification (only if needed):

Question 2:

An encryption scheme uses a monoalphabetic cipher followed by a transposition cipher. The substitution in the monoalphabetic cipher is done according to:

Plain	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
Cipher	-	-	U	-	-	-	-	A	B	C	D	E	F	G	H	J	L	M	O	Q	R	V	W	X	Y	Z

In addition, the transposition cipher is done according to the key: 42513867

The following ciphertext was generated using the aforementioned encryption scheme:

SQNQHGYNMHQQYBTGRKPXHRMNNOQBKQNF

a) Deduce the missing letters of the monoalphabetic cipher key [3 Marks]
b) Decrypt the ciphertext. Assume that the most frequent letter in the ciphertext would be guessed as the letter "e". [7 Marks – 3 Marks for matrix, 2 for cipher before transposition, and 2 for decryption]

Answer 2:

First rearrange the ciphertext to decrypt the transposition cipher

Y	H	R	S	M	N	K	H
B	G	K	Q	H	O	Q	R
T	Y	P	N	Q	Q	N	M
G	N	X	Q	Q	B	F	N

Then read the letters row by row to get the output of the substitution cipher:

YHRSMNKHBGKQHOQRTYPNQQNMGNXQQBFN

You can decrypt most of these letters according to the table in the question

Y	H	R	S	M	N	K	H	B	G	K	Q	H	O	Q	R	T	Y	P	N	Q	Q	N	M	G	N	X	Q	Q	B	F	N
y	o	u		r			o	i	n		t	o	s	t	u		y			t	t		r	n		x	t	t	i	m	

The letter "N" is repeated the most number of times in the ciphertext so we can guess it corresponds to "e".

Y	H	R	S	M	N	K	H	B	G	K	Q	H	O	Q	R	T	Y	P	N	Q	Q	N	M	G	N	X	Q	Q	B	F	N
y	o	u		r	e		o	i	n		t	o	s	t	u		y		e	t	t	e	r	n	e	x	t	t	i	m	e

It is now easy to guess that S→a, K →g, T→d, P→b, leaving the only possibility for "f" to be "I"

Thus, the keyword is SPUTNIK

The decrypted phrase is:

You are going to study better next time

Question 3:

Let a block cipher with secret key *K* be chained in the following way:

$$C_i = M_{i-1} \oplus E\big((M_i \oplus C_{i-1}), K\big) \qquad \text{for } i > 0$$

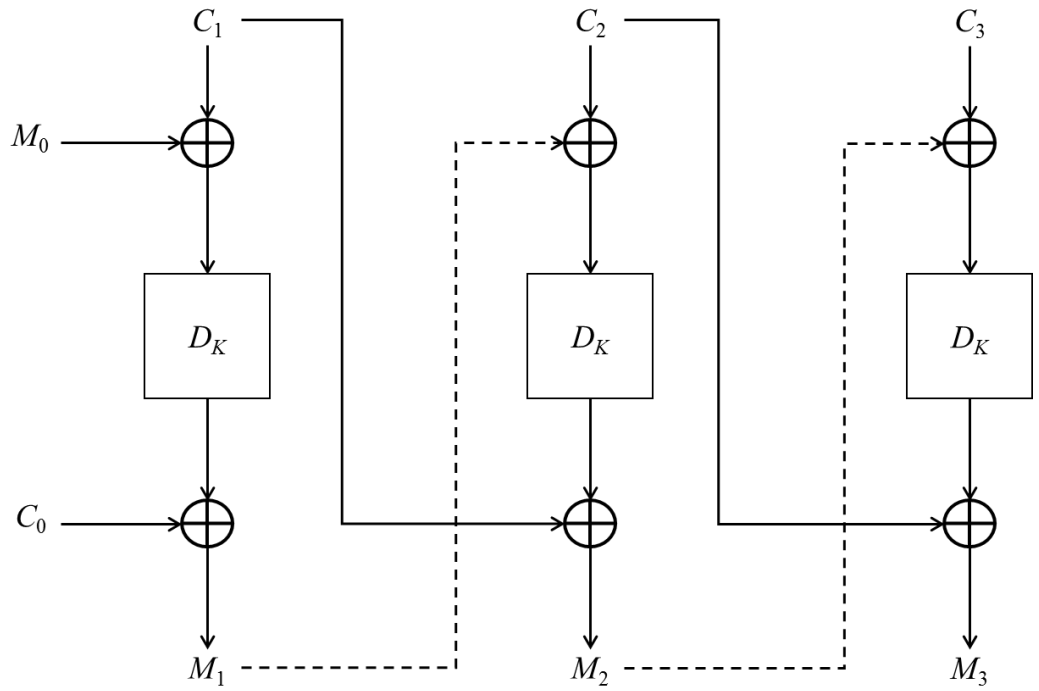
where M_i and C_i are plaintext and ciphertext blocks, and M_0 and C_0 are fixed public initialization vectors, *K* is the secret key known to both transmitter and receiver, and *E* and *D* represent encryption and decryption, respectively.

a) Determine the equation for decryption and draw the block diagram for the first three block ciphers. [6 Marks – 4 for equation and 2 for diagram]

b) Suppose that ciphertext C_j is damaged in transmission, which plaintext blocks will be decrypted incorrectly? [4 Marks]

Answer 3:

$M_i = D(C_i \oplus M_{i-1}, K) \oplus C_{i-1}$



Chaining depends, not on the previous ciphertext, but on the previous message. Thus, an error C_j results in all subsequent blocks to be decrypted incorrectly.

Question 4:

For this problem, assume that Alice wants to send **a single message *M*** to Bob. To do so, Alice and Bob can potentially use a number of different approaches and cryptographic technologies, which we will describe using the following terminology:

M	Plaintext for a single message
S_K	Symmetric cryptography key
$\text{DES}s_K$	Symmetric-key encryption using CBC mode, with the key s_k
K_A K_A^{-1}	Alice's public key Alice's corresponding private key
K_B K_B^{-1}	Bob's public key Bob's corresponding private key
E_K	Public-key encryption with the key *K*

You can assume that the public keys have been securely distributed, so Alice and Bob know their correct values. Symmetric keys have not been exchanged.

Consider the following properties that Alice and Bob might desire their communication to have: *Confidentiality, Integrity,* and *Non-Repudiation.*

For each of the following possible communication approaches, **Mention (and explain why)** which of these properties will securely hold (or not hold) in the presence of Mallory, a Man In-The-Middle (MITM) attacker, who is attempting to eavesdrop and intercept communication between Alice and Bob. Mention **None** if none of the properties hold. If an approach fails entirely (will not result in Bob being able to read a given message *M*), mention **Broken**.

a) Alice sends to Bob: $E_{K_B}(s_K)$ [5 Marks]

b) Alice generates a new symmetric key s_K and sends to Bob: $E_{K_B}(s_K), \text{DES}_{s_K}(M)$ [5 Marks]

Answer 4:

a) Confidentiality, as Bob can decrypt with his private key and read the message. Integrity will also hold because Mallory does not have Bob's private key and thus cannot decrypt and modify the message contents. However, non-repudiation will not hold because anyone can generate a fake message since the encryption key is public.

b) Confidentiality and Integrity. Only Bob will be able to decrypt with his private key. However anyone can generate the message using Bob's public key.

[Each property that holds gets 2.5, divided 2 for property and 1 for explanation. If one is missing or incorrect and non-repudiation is stated correctly it gets 1.5 Marks]

Question 5:

Consider the RSA scheme with the following parameters:

$$p = 19, q = 23, e = 17, M = 74$$

i. Compute the decryption key d. [5 Marks]

ii. Encrypt M using the parameters above. [5 Marks]

Answer 5:

i. $\phi(n) = 18 * 22 = 396$ [1 Mark]

$d = \frac{(1+k\times\phi(n))}{e} = \frac{(1+10\times396)}{17} = 233$ [4 Marks – 2 for k and 2 for computation]

ii.

$n = 437$

$C = M^e \bmod n = 74^{17} \bmod 437$ [1 Mark]

$= [(74^4 \bmod 437)(74^4 \bmod 437)(74^4 \bmod 437)(74^4 \bmod 437)\ (74 \bmod 437)] \bmod 437$ [2 Marks]

$= (73\times73\times73\times73\times74) \bmod 437 = 199$ [2 Marks]

Plaintext

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

RSA Formulas:

Key Generation

1. Select two large primes at random: $p,\ q$
2. Compute their system modulus $n = p \times q$
3. Compute Euler's Totient $\phi(n) = (p-1) \times (q-1)$
4. Select encryption key e , where $3 \leq e < \phi(n)$, $gcd(e, \phi(n)) = 1$
5. Compute decryption key d
   - $e \times d \equiv 1 \, mod \, \phi(n) \;\; and \, d < \phi(n) \rightarrow \; e \times d = 1 + k \times \phi(n) \quad for \, some \, k$
6. Publish the public encryption key: $PU = \{e, n\}$
7. Keep secret the private decryption key: $PR = \{d, n\}$

Encryption

- Ciphertext $C = M^e \, mod \, n$

Decryption

- Plaintext $M = C^d \, mod \, n$