October 29th, 2018

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

Information Security

Winter term 2018
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 Caesar Cipher is a stream cipher.	T
2) The S-Box in AES is the same for every plaintext block.	T
3) Non-repudiation can be achieved by encrypting a message with the receiver's public key.	F
4) In the Advanced Encryption Standard (AES) cipher, "shift rows" is a step that contributes to diffusion.	T
5) In end-to-end encryption (such as encryption of application layer data), only the original source and the final destination need to have the key.	T
6) The CBC mode considered preferable to ECB mode.	T
7) A particular function in a system not executing properly is a violation of system integrity.	T
8) The output feedback (OFB) mode of encryption does not propagate errors when one of the ciphertext blocks is damaged.	T
9) To send a confidential message using public key cryptography, the sender would encrypt the message with their own private key.	F
10) Confusion is the process by which the encryption algorithm hides the relationship between the ciphetext and the plaintext.	F

Extra space for justification (only if needed):

Question 2:

The Vigenère autokey cipher is a modification over the traditional Vigenère cipher, where the key that is used for encryption is generated from a passphrase plus the plaintext itself. For example, to encrypt the phrase "*Ilovesecurity*" using the passphrase "*frog*", the encryption key becomes "*frogIlovesecu"*. A two-stage encryption algorithm is built using a Vigenère autokey cipher followed by a transposition cipher. The passphrase for the Vigenère autokey cipher is "goal" and the key for the transposition cipher is 3 5 4 1 2. Decrypt the following ciphertext to obtain the plaintext.

LFTWUXNQVKSOUWASRHTBCZZJJ

(*Hint*: Rearrange the ciphertext into a 5×5 matrix according to the transposition key 3 5 4 1 2, and then produce the ciphertext before transposition. Proceed to decrypt the resulting ciphertext following the Vigenère autokey scheme explained above.)

Answer 2:

Ciphertext transposition encryption

3	5	4	1	2
S	C	S	L	X
O	Z	R	F	N
U	Z	H	T	Q
W	J	T	W	V
A	J	B	U	K

Decryption of transposition is SCSLXOZRFNUZHTQWJTWVAIJBUK

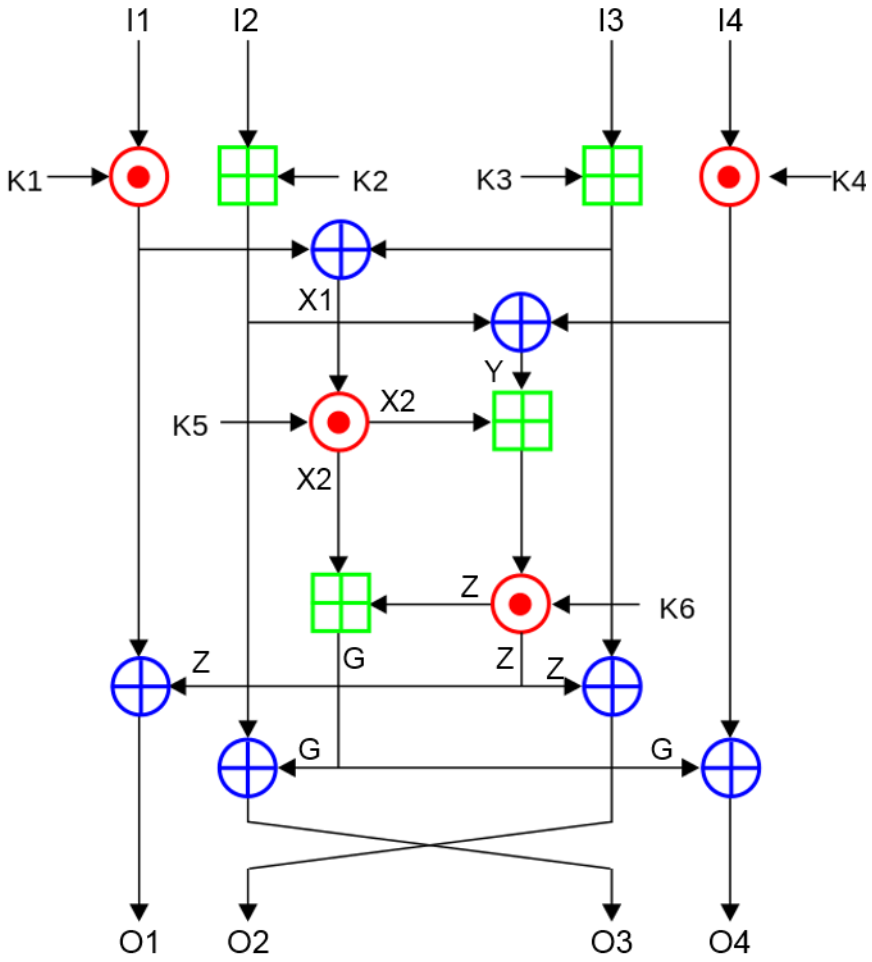
Decrypt the first 4 letters SCSL using the passphrase "goal" gives MOSA. Thus, we decrypt the next 4 letters XOZR using MOSA to get LAHR, and decrypt the next 4 letters FNUZ using LAHR to get UNNI, and so on.

We continue to get the phrase MOSALAHRUNNINGDOWNTHEWING

Or *Mo Salah Running Down The Wing*

Question 3:

The following figure shows an encryption round of an encryption algorithm known as the International Data Encryption Algorithm (IDEA).



The algorithm accepts plaintext blocks of size 64 bits and a key of size 128 bits. The plaintext is divided into 4 sub-blocks, each having size 16 bits. These sub-blocks are the input to the first round, as the figure shows. They key is used to generate 6 subkeys for each round, each subkey having size 16 bits. On the figure, the symbol $\oplus$ denotes an XOR operation, $\odot$ denotes multiplication, while $\boxplus$ denotes addition. Write the equations for $X1, X2, Y, Z, G, O1, O2, O3, and\ O4$.

Answer 3:

$X1 = (I_1 \odot K_1) \oplus (I_3 \boxplus K_3)$

$X2 = X1 \odot K_5$

$Y = (I_2 \boxplus K_2) \oplus (I_4 \odot K_4)$

$Z = (Y \boxplus X2) \odot K_6$

$G = X2 \boxplus Z$

Thus we have the 4 outputs of the IDEA round

$O1 = (I_1 \odot K_1) \oplus Z$

$O2 = (I_3 \boxplus K_3) \oplus Z$

$O3 = (I_2 \boxplus K_2) \oplus G$

$O4 = (I_4 \odot K_4) \oplus G$

Question 4:

In a particular system, Alice wishes to send a message, M, to Bob using public key cryptography. Each time, Alice is going to desire to achieve some (or all) the objectives of **Confidentiality, Integrity, and Non-repudiation.** Alice's public and private keys are denoted by (PU_A, PR_A), while the keys of Bob are denoted by (PU_B, PR_B). An encryption process in this system is denoted by $E(K, M)$, where K is the key (could be a public or private key) and M is the plaintext. For each of the following situations, specify which of these objectives is achieved and explain why.

a) Alice sends $E(PU_B, M)$

b) Alice sends $E(PR_A, M)$

c) Alice sends $E(PU_B, E(PR_A, M))$

d) Alice sends $E(PR_A, E(PU_B, M))$

Answer 4:

a) Confidentiality. Bob will decrypt with his private key

b) Non-repudiation. No one could generate the message but Alice.

c) Confidentiality and non-repudiation due to double encryption.

d) Same as c), the order does not matter.

Question 5:

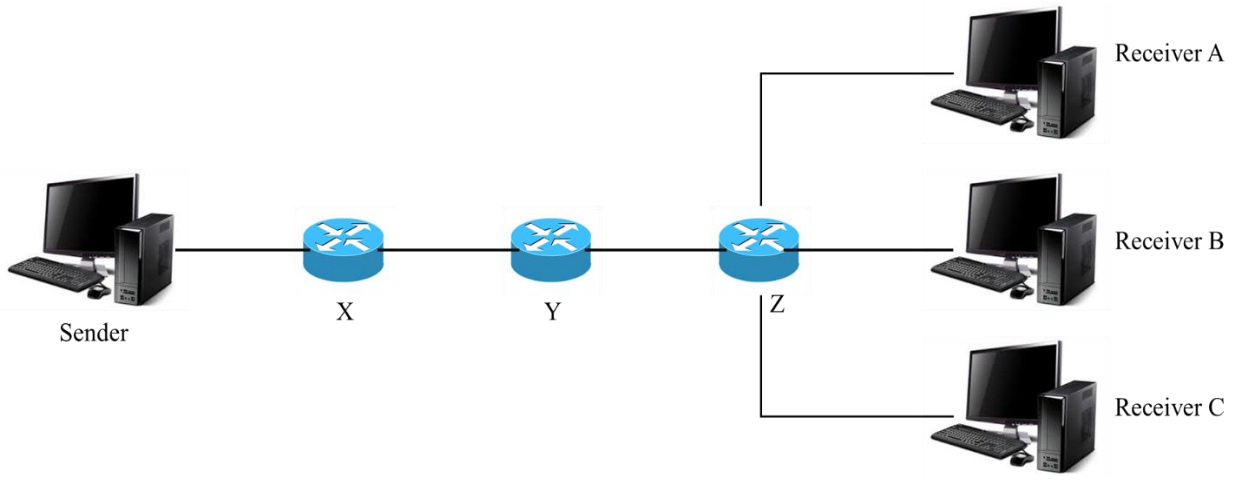
a) Consider the RSA scheme with the following parameters:

$$p = 5, q = 7, e = 5, M = 3$$

i. Compute the decryption key d.

ii. Encrypt M using the parameters above.

b) In the following diagram, the sender is trying to send a packet to each of the three receivers (A, B, C), through routers (X, Y, Z). If link encryption is used (using a symmetric cryptography technique), how many keys are needed to send all three packets? How many keys are needed if end-to-end encryption is used?



Answer 5:

a)

i. $n = 5 \times 7 = 35$

$\phi(n) = (5-1) \times (7-1) = 24$

$(5 \times d)\ mod\ 24 = 1 \rightarrow 5d = 1 + 24k \rightarrow d = \frac{(1+24k)}{5}$

$trying\ k = 1\ we\ find\ d = 5$

ii. $C = M^e\ mod\ n = 3^5\ mod\ 35 = 33$

b) Link encryption needs one key per hop. Thus, a total of 6 keys are needed. If end-to-end encryption is used then only 3 keys are needed.

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