King Saud University

College of Computer and Information Sciences
Computer Science Department

Course Code:	CSC 429
Course Title:	Computer Security
Semester:	Winter 2024
Type of Examination:	Midterm Exam.

Student Name:	
Student ID:	
Student Section No.	
Instructor Name:	

	Full Mark	Student's Mark
Question No.1	7	5
Question No.2	4	4
Question No.3	5	5
Question No.4	5	4
Question No.5	4	3.5
Total	25	22.5

لا تنسونا من دعائكم

Winter Semester 2024 | CSC429 | Midterm Exam | 16-4-2024

Student's Name:.... .Student's ID

Please copy your answer for question 1 to 5 the following tables

1.1.	1.2.	1.3.	1.4.	1.5.	1.6.	1.7.	1.8.	1.9.	1.10.
B	A D	A	B A	A	D	C X B	D	D X B	A
1.11.	**1.12.**	**1.13.**	**1.14.**						
D	C	D	D						

2.1	The First method is by using an old key that one of the part is have to exchange and deliver the new key (RSA) The second method by letting a third party to creat and deliver one key for both the party (Diffi-Helman)	2.2	used in stream cipher used in SHA
2.3			

3.1	
3.2	3.3
EID MoBARAK	2 keys or 3 key because it have many version

4.1.1	4.1.2	4.2.1	4.2.2	4.3
T	F	C	A	e = 7 or 23 d = 29

4.4	Algorithm	Digital Signature	Symmetric Key Distribution	Encryption of Secret Keys
	RSA	yes	yes	yes
	Diffie-Hellman	No	yes	No
	DSS	yes	No	No
	Elliptic Curve	yes	yes	yes

5.1	fingerprint ~~Iris~~ قزحية Voice pattern Facial recognation Neaf شبكية العين	is something that Indivioals ~~Iris~~ have or does or it is the general characteristic of the human

5.2.1	5.2.2	5.2.3	5.2.4	5.2.5	5.2.6
dictionary attack	~~Iris~~ قزحية	DDoS	Replay	~~SHA~~ Salt	SHA

Bloom filter

Student's Name:.....Student's ID.....

Question 1. [7 Marks] Select ONLY ONE ANSWER (the best answer).
Copy your answer for question 1-1 to 1-10 in the table on page2. ONLY THAT TABLE WILL BE GRADED.

1.1.	The three main security objectives or CIA Triad are
A.	confidentiality, authenticity, and availability
B.	confidentiality, integrity, and availability
C.	confidentiality, authenticity, and integrity
D.	integrity and availability

1.2.	The following Service is not provided by Cryptography:
A.	encryption
B.	authenticity
C.	access control
D.	availability

1.3.	A type of network attack where attackers try to overwhelm a target system by sending a flood of traffic from multiple sources:
A.	DDoS (Distributed Denial of Service) x
B.	malware
C.	spyware
D.	ransomeware

1.4.	Adversary is defined as:
A.	individual, group, organization, or government that conducts or has the intent to conduct detrimental activities x
B.	any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself
C.	a device or techniques that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage
D.	a measure of the extent to which an entity is threatened by a potential circumstance or event

1.5.	Passive Attacks are:
A.	attempt to learn or make use of information from the system that does not affect system resources
B.	attempt to alter system resources or affect their operation
C.	initiated only by an entity inside the security parameter
D.	initiated only by an entity from outside the perimeter

1.6.	For security requirements and as part of System and Information Integrity, security personnel need to:
A.	identify, report, and correct information and information system flaws in a timely manner
B.	provide protection from malicious code at appropriate locations within organizational information systems
C.	monitor information system security alerts and advisories and take appropriate actions in response
D.	all of the above

Student's Name:.....Student's ID.....

1.7.	For security requirements and as part of Audit and Accountability, security personnel need to:
A.	ensure that managers and users of organizational information systems are made aware of the security risks
B.	create, protect, and retain information system audit records to the extent needed x
C.	periodically assess the security controls in organizational information systems
D.	establish and maintain baseline configurations and inventories of organizational information systems

1.8.	Least Privilege principle means
A.	least privilege people are forbidden from accessing a system
B.	every process and every user of the system should operate with maximum privileges and functionalities
C.	every process and every user of the system should have the least privileges for complete protection of the system
D.	every process and every user of the system should operate using the least set of privileges necessary to perform the task

1.9.	When a working program is modified to cause it to fail during execution is an example of a threat effecting .....
A.	the integrity of a hardware
B.	the integrity of a software
C.	the confidentiality of the user
D.	the availability of the software

1.10.	when the attacker try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
A.	brute-force attack
B.	passive attack
C.	Cryptanalytic attack
D.	ultimate attack

1.11.	Countermeasures are means used to deal with security attacks to
A.	recover
B.	detect
C.	prevent
D.	all of the above

1.12.	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
A.	countermeasure
B.	adversary
C.	vulnerability
D.	risk

1.13.	A ..... processes the input elements continuously, producing output one element at a time, as it goes along
A.	pseudorandom number generator
B.	XOR
C.	block cipher
D.	stream cipher

1.14.	Examples of symmetric algorithms, which are block ciphers, are the DES, triple DES, and the _____.
A.	DSS
B.	SHA
C.	RSA
D.	AES

Student's Name:.....Student's ID.....

Question 2. [4 Marks]

2.1 [2 Marks] Key Distribution is the means of delivering a key to two parties that wish to exchange data without allowing others to see the key, explain two methods to achieve it between party A and B.

1M) The first meathod is by using an old key that one of the parties have to exchange (delivering) the new key

2 M) is by letting a third party to creat and delive a new key for both the party

2.2 Random numbers has many applications in the computer security fields, list two of its applications [2 Marks]

Student's Name:.....Student's ID.....

Question 3. [5 Marks]

3.1 [2 Marks] Encrypt the following plaintext "Let the cat out of the bag" using Playfair Cipher, giving the key is "SECRET", show your answer

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

Le tx th ec at ou to ft he ba gx
IR cz SM cR GS PN EU GR IS DB DZ

IR cz S M cR GS P N EU GR IS DB DZ

3.2 [2 Marks] If you have the following letter assignment (plaintext to –ciphertext) using Homophones cipher, the following ciphertext "97N Y3O8KPG" stands for

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
-P	-O	A	-N	B	Z	M	C	F	D	-G	E	-Y	H	J	U	T	-K	I	S	L	R	V	Q	X	W
8			-9				-7						5	3				4	6						
			2																						
			1																						

EID MOBARAK

3.3 [1 Mark] How many unique keys are required for Triple DES to encrypt and decrypt ?

2 keys or 3 keys

Student's Name:.....Student's ID.....

Question 4. [5 Marks]

4.1 [1 Mark] T/F answer. Please mark T or F.

4.1.1 SHA-1 and SHA-2 share the same structure and mathematical operations. T

4.1.2 Chosen ciphertext attacks are the type of attack that exploits properties of the RSA algorithm.

4.2 [1 Mark] MCQ answer. Please select right answer.

4.2.1 Which encryption algorithm is commonly used to secure internet communications (i.e. key exchange)

(A) MD5
(B) RC4
(C) RSA
(D) DES

4.2.2 Which encryption algorithm is commonly used to secure data transmission over the internet?

(A) SHA-1
(B) MD-5
(C) AES
(D) DES

4.3 [1 Mark] In RSA, if chosen prime numbers p=17 and q=11, what are the possible e and d values?

$n = p \times q = 17 \times 11 = 187$

$\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$

$gcd(e, \phi(n)) = 1 \quad 1 < e < \phi(n)$ e = 7

$de \equiv 1 \mod \phi(n) \quad d \equiv e^{-1} \mod \phi(n)$ d = 23

4.4 [2 Marks] In a table, contrast the algorithms of RSA, Diffie-Hellman, DSS, and ECC in terms of digital signature, symmetric key exchange, and encryption.

$gcd(e^{-1}, \phi) = gcd(7, 160)$

$160 = 22 \times 7 + 6$

$7 = 1 \times 6 + 1 \Rightarrow gcd$

$1 = 7 - 1 \times 6$

$= 7 - 1(160 - 22 \times 7)$

$= -1 \times 160 + 23 \times 7$

this is the inverse

Student's Name:.....Student's ID.....

Question 5. [4 Marks]

5.1 [1 Mark] What do we mean by Biometric Authentication? List 5 possible methods.

is indevi

5.2 [3 Mark] Please fill in the blank.

5.2.1 dictionary attack attacks are performed by developing a large dictionary of possible passwords and try each against the password file.

5.2.2 Iris..... is costly but considered the most accurate biometric authentication method

5.2.3 D.o.S.... attempts to disable a user authentication service by flooding the service with numerous authentication attempts

5.2.4 Replay. is the type of attack where adversary repeats a previously captured user response

5.2.5 In Unix password, we use ~~SHA~~ Salt..... to increase password complexity and make them unique and secure.

5.2.6 ~~Salt~~ Bloom filter... is used to build a table based on hash values and check desired password against this table.

End of the Exam.