	College of Co	King Saud University College of Computer and Information Sciences Computer Science Department			
	Course Code:	ourse Code: CSC 429			
	Course Title:	Computer Secur	rity		
	Semester:	Winter 2024	1 4 2 2 3		
	Type of Examination:	Midterm Exar	m.		
Student Name:	CALL DOWN	-			
Student ID:		1			
Student Section No.					
Instructor Name:					
	Fi	ull Mark	Student's Mark		
Question No.1	100	7	5		
Quemini i ini			-		
Question No.2		4	4		
		5	4		
Question No.2			4 5 4		
Question No.2 Question No.3		5	3.5		

16-4-2024

Page 2 of 8

Student's Name:..

.Student's ID

The First method of the part is have to exchange and deliver and deliver and key for Doth the part years of the part yea	rease cor	DV VALLE BREEZE	e for quartion 1	to 5 the fall	owing tables		
B A A B A D C D D A  1.11. 1.12. 1.13. 1.14.  D C D D  2.1 The First method is by hsins an all key that one at the part it have to exchange and referent the new Key (18A)  The first creat and reflect a third fatty to ereat and reflect a new Key for Dobt the earth  2.2 Used in SHA  The first method by litting a third fatty to ereat and reflect a new Key for Dobt the earth  2.3 3.3  EID Mobbara A R  2 Keys of 2 Key because it have many  4.1.1 4.1.2 4.2.1 4.2.2  For A C = 2 d = 29  4 Algorithm  Digital Signature  Digital Signature  Distribution  Secret Keys  Per S		12				1.7. 1.8.	1.9. 1.10.
1.11. 1.12. 1.13. 1.14.  D C D D  2.1 The First Method is by hsins an all key that one of the Part it have to exchange and deliver the new key (Isa)  This even is method by littling a third party to exect and deliver ance key first the rarby  (Jiffi-Helman)  3.1  3.2  EID Mobara ARA  2 Keys of 3 Key because it have many version  4.1.1 4.1.2 4.2.1 4.2.2  4.2.1 4.2.2 94.3  For C A C = Z d = 29  4 Algorithm  Digital Signature  Distribution  Secret Keys  Possion  No Distribution  Secret Keys  Possion  No Distribution  Distribution  Secret Keys  Possion  No Distribution  Distribution  Secret Keys  Possion  No Distribution  Secret Keys  Possion  No Distribution  Distribution  Secret Keys  Possion  No Distribution  Distribution  Secret Keys  Possion  No Distribution  Secret Keys  Possion  No Distribution  Distribution  Secret Keys  Possion  No Distribution  Distribution  Secret Keys  Possion  No Distribution  Distribution  Secret Keys  Possion  Distribution  Secret Keys  Possion  Distribution  Secret Keys  Possion  Distribution  Distribution  Secret Keys  Possion  Distribution  Dis		AD					DXA
The First method is by  2.1 The First method is by  hsins an a) deventation of the partit have to exchange  and devent the new key (154)  The first method by litting  a third farty to exchand derives  ance key for both the farty  (166:-Helman)  3.1  3.2  EID Mob ARA R  2 keys or 3 key because it have many  4.1.1 4.1.2 4.2.1 4.2.2  For C A C = 7 d = 29  4 Algorithm  Digital Signature  Digital Signature  Symmetric Key  Distribution  Secret Keys  Pes  Diffie-Hellman  No  Distribution  Distribution  Secret Keys  Pes  Diffie-Hellman  No  Distribution  Distribution  Distribution  Distribution  Secret Keys  Pes  Diffie-Hellman  No  Distribution						2	B
2.1 The first method is by  hsing an all key that are of the part is have to exchange and detert the new key (15A)  This exemple method by litting a third farty to creat and derives ance key for Doth the farty  (3165: -Halvary)  3.1  3.2  EID Mob ARA R  2 Keys or 3 Key because it have many  Version  4.1.1 4.1.2 4.2.1 4.2.2  For C A = 2 2  4 Algorithm  Digital Signature  Digital Signature  Digital Signature  Distribution  Secret Keys  Person  No Diffie-Hellman  No Distribution  Distribution  Secret Keys  No Diffie-Hellman  DSS		-					
The First Methad 156y hsins an all Key that one of the Part is have to exchange and deliver the new Key (15A) The fee-not method by litting a third party e- epent and deliver ane v Key fer both the party  (Jiffi:-Helman)  3.1  3.2  EID Mobbarah  2 Keys of 3 Key because it have many version  4.1.1  4.1.2  4.2.1  4.2.2  The formal deliver and version  3.3  Symmetric Key Distribution  Secret Keys  Post Diffie-Hellman  No Distribution  No					722		
the part is have to exchange  and deliver the new Key (85A)  The second method by littling a third party to creat and deliver  and very for both the carty  (3:66: - Helivar)  3.1  3.2  EID Mobara A R  2 Keys or 3 Key because it have many  Version  4.1.1  4.1.2  4.2.1  4.2.2  Algorithm  Digital Signature  Digital Signature  Symmetric Key  Distribution  Secret Keys  Poss  Diffie-Hellman  No  Diss  No  No  No  No  No  No  No  No  No	2.1	The Firs	+ wepper	15 6x		used in sti	reasm eigher
The part is have to exchange  and deliver the new Key (SA)  The excend method by litting a third party to open and deliver  and very for Both the party  (difficultinate)  3.1  3.2  Et D Mabara R  2 Keys of 3 Key because it have many  version  4.1.1  4.1.2  4.2.1  4.2.2  Algorithm  Digital Signature  Digital Signature  Symmetric Key  Distribution  Secret Keys  RSA  9 cs  No  No  Distribution  Distribution  Distribution  Secret Keys  Poss  Po		hsins an	ald Keytr	nat ore o	+	1 :- 51	IA /
3.1  3.2  EID Mobara And Service of the farty  (3166:-Helman  Digital Signature  Digital Signature  Symmetric Key  Diffie-Hellman  Dissolution  No  No  No  No  No  No  No  No  No	100	the Part	is have t.	exchan		recount to	1/0
3.1  3.2  EID Mobarda Rale  2.3  2 Keys of They because it have many  Version  4.1.1  4.1.2  4.2.1  Algorithm  Digital Signature  Digital Signature  Symmetric Key  Distribution  Secret Keys  RSA  Person  Person  Diffie-Hellman  No  Person  No  No  No  No  No  No  No  No  No						The same of the sa	
3.1  3.2  EID Mobara RA R  2 Keys of 3 Key because it have many version of Secret Keys  Algorithm  Digital Signature  Symmetric Key Encryption of Secret Keys  Poss  Diffie-Hellman  DSS  No N							
3.1  3.2  EID Mobara RAN  2 Keys of 3 Key because it have many  4.1.1  4.1.2  4.2.1  Algorithm  Digital Signature  Symmetric Key  Distribution  Secret Keys  Proposition  RSA  Proposition  Distribution  Distribution  Secret Keys  Proposition  No  Proposition  Distribution  Distribution  Distribution  Distribution  Secret Keys  Proposition  Distribution		a thing o	elty de	1 6 9 1	itting		A 100 A
3.1  3.2  ETD MoBARA R  2 Keys or 3 Key because it have many  Version  4.1.1 4.1.2 4.2.1 4.2.2  For C A e= Z d= 29  Algorithm  Digital Signature  Symmetric Key Encryption of Secret Keys  Possible RSA  Diffie-Hellman  DSS  No  No  No  No  No  No  No  No  No							
3.1  3.2  ETD MoBARA R  2 Keys or 2 Key because it have many  Version  4.1.1  4.1.2  4.2.1  4.2.2  Algorithm  Digital Signature  Symmetric Key  Distribution  Secret Keys  Person  No  Diffie-Hellman  DSS  No  No  No  No  No  No  No  No  No	1	nec wellen	)	the far	ty		
3.1  3.2  EID MoBARAR  2 Keys or 3 Key because it have many  4.1.1  4.1.2  4.2.1  Algorithm  Digital Signature  Symmetric Key  Distribution  RSA  Diffie-Hellman  No  Yes  No  No  No  No  No  No  No  No  No  N		164	<u></u>			PERSONAL PROPERTY.	
3.2  EID MoBARAR  2 keys of 3 key because it have many  4.1.1  4.1.2  4.2.1  Algorithm  Digital Signature  Symmetric Key  Distribution  RSA  Diffie-Hellman  DSS  No  No  No  No  No  No  No  No  No						distribution of	
3.2  EID MoBARAR  2 keys of 3 key because it have many  4.1.1  4.1.2  4.2.1  Algorithm  Digital Signature  Symmetric Key  Distribution  RSA  Diffie-Hellman  DSS  No  No  No  No  No  No  No  No  No		Market Land		100000	-11 5		
EID MoBARAR  2 Keys of 3 Key because it have many  4.1.1 4.1.2 4.2.1 4.2.2  For C A C = Z d = 29  4. Algorithm  Digital Signature  Symmetric Key  Distribution  RSA  Diffie-Hellman  No Yes  No  No  No  No  No  No  No  No  No  N		- 1275	1 - 200 - 11		3.1		1
EID MoBARAR  2 keys or 3 key because it have many  4.1.1 4.1.2 4.2.1 4.2.2  For C A C = Z d = 29  4 Algorithm  Digital Signature  Symmetric Key  Distribution  RSA  Diffie-Hellman  No  Yes  No  No  No  No  No  No  No  No  No  N						and the same	-
4.1.1 4.1.2 4.2.1 4.2.2  Algorithm  Digital Signature  Symmetric Key  Distribution  RSA  Diffie-Hellman  DSS  DSS  Vers  No  No  No  No  No  No  No  No  No  N				/	79 7 -		The state of the s
4.1.1 4.1.2 4.2.1 4.2.2  For C A C A C C A C C A C C C A C C C C A C C C C C C C C C C C C C C C C C C C C	ET	DMOB	ARAK		2 Keys o	11 3 KEY beco	iuse it have many
Algorithm  Digital Signature  Symmetric Key Distribution  RSA  Poss  No	-				Velsion		
Algorithm  Digital Signature  Symmetric Key Distribution  RSA  Ves Ves No							
RSA Diffie-Hellman Distribution Secret Keys  yes  No		_	4.2.1	4.2.2		0 4.3	NAME OF THE OWNER OWNER OF THE OWNER
RSA Diffie-Hellman Distribution Secret Keys  yes  No		_		4.2.2 A_	e= 7	0 = 29	
RSA  Diffie-Hellman  No  No  No  No  No  No  No  No  No  N	*	FX		A	e= 7	0 = 29	Energation of
Diffie-Hellman  No  Yes  No  No  No  No  No  No  No  No  No  N	*	FX		A	e = 7	d = 29 Symmetric Key	
DSS XCS NO	4	F 🖔		A Digita		Symmetric Key Distribution	Secret Keys
V. C	4 RSA	F		A Digita	yes	Symmetric Key Distribution y e 5	Secret Keys
Emple curv	4 RSA Diffic	F		Digita	yes No	Symmetric Key Distribution  ye 5  Yes	Secret Keys  y · 5  N °
	RSA Diffie DSS	Algorithm		Digita	yes No	Symmetric Key Distribution ye 5 ye 5 N 9	Secret Keys  y · 5  N °
	RSA Diffic DSS Ellipt	Algorithm e-Hellman tic Curve	C	Digita	yes No yes yes	Symmetric Key Distribution  ye 5  N 9  Ye 5	Secret Keys  y · 5  N °
	RSA Diffic DSS Ellipt	Algorithm e-Hellman tic Curve	/ is	Digit	yes No yes yes	Symmetric Key Distribution ye 5 ye 5 N 9	Secret Keys  y · 5  N °  N °
TEXIS TO SE Shave or does bot	RSA Diffic DSS Ellipt	Algorithm  e-Hellman  tic Curve	C is	Digita	yes No yes yes hiny tha	Symmetric Key Distribution  ye 3  Yes  No  Yes  L Indivious	Secret Keys  y · 5  N °  N  Secret Keys
Voice pattern of it is the general charieteristic	RSA Diffic DSS Ellipt	Algorithm  e-Hellman  tic Curve	n or is	Digita	yes No yes yes hiny tha	Symmetric Key Distribution  ye 3  Yes  No  Yes  L Indivious	Secret Keys  y · 5  N °  N  Secret Keys
Voice pattern of the general charieteristic	RSA Diffic DSS Ellipt	Algorithm  e-Hellman  tic Curve	ov is	Digita	yes No yes yes hiny tha	Symmetric Key Distribution  ye 3  Yes  No  Yes  L Indivious	Secret Keys  y · 5  N °  N  Secret Keys
Voice pattern of the general charieteristice  focial recognition of the homen  Nenture	RSA Diffic DSS Ellipt	Algorithm  e-Hellman  tic Curve  fis acceptations  e patter  cal recognitions	n or ha	Digit:	yes No yes yes hiny tha dacs bar he yene	Symmetric Key Distribution  ye 5  ye 5  No  ye 5  Lal chariet	Secret Keys  yes  No  No  No  No  No  No  No  No  No  N
Voice pattern of the general charieteristice  focial recognition of the horen  Nenture 5.2.2 5.2.3 5.2.4 5.2.5 5.2.6	RSA Diffic DSS Ellipt	Algorithm  e-Hellman  tic Curve  fis acceptations  e patter  cal recognitions	n or ha	Digit:	yes No yes yes hiny tha dacs bar he yene	Symmetric Key Distribution  ye 5  ye 5  No  ye 5  Lal chariet	Secret Keys  yes  No  No  No  Servistie
Voice pattern of the general charieteristice  Facial Vecayantion of the haven  Nentucian  5.2.1 5.2.2 5.2.3 5.2.4 5.2.5 5.2.6	RSA Diffic DSS Ellipt Voice for c	Algorithm  e-Hellman  tic Curve  fis acres  e patter  cial recognition  5.2.2	n or ha	Digit:	yes No yes hiny tha does haven	Symmetric Key Distribution  ye 5  N 9  L Indivious  tal chariet	Secret Keys  yes  No  No  No  Servistie

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

perimeter

Question 1. [7 Marks] Select ONLY ONE ANSWER (the best answer).

1.1	The three main security objectives or CIA Triad are	1.2.	The following Service is not provided by Cryptography:
	A. confidentiality, authenticity, and availability	A.	encryption
4	confidentiality, integrity, and availability	B.	authenticity
	C.   confidentiality, authenticity, and integrity	C.	access control
I	D. integrity and availability	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:	1.4.	Adversary is defined as:
(	DDoS (Distributed Denial of Service) x	A.	individual, group, organization, or government that conducts or has the intent to conduct detrimental activities x
В	malware	B.)	any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself
C.	spyware	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.	ransomeware		a measure of the extent to which an entity is threatened by a potential circumstance or event
5.	Passive Attacks are:	1.6.	For security requirements and as part of System and Information Integrity, security personnel need to:
1	attempt to learn or make use of information from the system that does not affect system resources	Α.	identify, report, and correct information and information system flaws in a timely manner
В.	attempt to alter system resources or affect their operation	В.	provide protection from malicious code at appropriate locations within organizational information systems
	initiated only by an entity inside the security parameter	C.	monitor information system security alerts and advisories and take appropriate actions in response
	initiated only by an entity from outside the	6	all of the above

1	1.7.	For security requirements and as part of Audit and Accountability, security personnel need to:	1.8.	Least Privilege principle means	
	Α.	ensure that managers and users of organizational information systems are made aware of the security risks	A.	least privilege people are forbidden from accessing a system	
L	B.	The state of the s	В.	every process and every user of the system should operate with maximum privileges and functionalities	
1	c.	periodically assess the security controls in organizational information systems	C.	every process and every user of the system	
	D.	establish and maintain baseline configurations and inventories of organizational information systems	<b>(D)</b>	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	1.10.	when the attacker try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained	
1	A. 1	the integrity of a hardware	(A)	brute-force attack	
E		the integrity of a software	B.	passive attack	
_	_	he confidentiality of the user	C.	Cryptanalytic attack	
C	DI	he availability of the software	D.	ultimate attack	
.11		Countermeasures are means used to deal with security attacks to	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.	re	cover	A.	countermeasure	
B.	de	tect	B.	adversary	
C.	pre	event	(0)	vulnerability	
D.)	all	of the above	D.	risk	
-					
3.	con at a	processes the input elements tinuously, producing output one element time, as it goes along	1.14.	Examples of symmetric algorithms, which are block ciphers, are the DES, triple DES, and the	
	pseu	udorandom number generator	A.	DSS .	
-	XOI	R	B.	SHA	
-	bloc	k cipher	C.	RSA	

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 meathed is by using anold key that one chapter to exchapte the new Key

2 m) is by Letting athird carty to delive for both the party

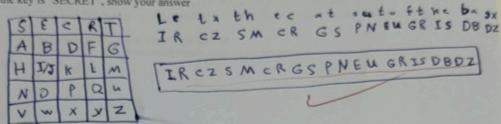
2.2 Random numbers has many applications in the computer security fields, list two of its applications [2 Marks]

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



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

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:...

16-4-2024

.....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. 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

(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

signature, symmetric key exchange, and encryption.

CSC429

Midterm Exam

16-4-2024

Question 5. [4 Marks]
5.1 [1 Mark] What do we mean by Biometric Authentication? List 5 possible methods.

.....Student's ID.....

is indevi

5.2 [3 Mark] Please fill in the blank.
5.2.1 dictionary of possible passwords and try each against the password file.

5.2.2 **3.2.5....** is costly but considered the most accurate biometric authentication method 5.2.3 **3.2.5...** attempts to disable a user authentication service by flooding the service with

numerous authentication attempts

and secure.

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

End of the Exam.