Program: BE Computer Engineering

Curriculum Scheme: Revised 2016

Examination: Third Year Semester VI

Course Code:CSC604 and Course Name: Cryptography and System Security

Time: 1 hour

Max. Marks: 50

Note to the students:- All the Questions are compulsory and carry equal marks .

Q1.	Choose from among the following cipher systems, from best to the worst, with
	respect to ease of decryption using frequency analysis.
Option A:	Random Polyalphabetic, Plaintext, Playfair
Option B:	Random Polyalphabetic, Playfair, Vignere
Option C:	Random Polyalphabetic, Vignere, Playfair, Plaintext
Option D:	Random Polyalphabetic, Plaintext, Beaufort, Playfair
Q2.	is the science and art of transforming messages to make them secure
	and immune to attacks
Option A:	Cryptography
Option B:	Cryptoanalysis
Option C:	Cryptocircuit
Option D:	Cryptomap
Q3.	A (n) algorithm transforms ciphertext to plaintext
Option A:	encryption
Option B:	decryption
Option C:	secret
Option D:	cipher
Q4.	A transposition cipher reorders (permutes) symbols in a
Option A:	block of packets
Option B:	block of slots
Option C:	block of signals
Option D:	block of symbols
Q5.	There is a dependency on the previous 's' bits in every stage in CFB mode. Here
	's' can range from
Option A:	8-16 bits
Option B:	8-32 bits
Option C:	4-16 bits
Option D:	8-48 bits
Q6.	Which one of the following modes of operation in DES is used for operating short
	data?

Option A:	Cipher Feedback Mode (CFB)
Option B:	Cipher Block chaining (CBC)
Option C:	Electronic code book (ECB)
Option D:	Output Feedback Modes (OFB)
Q7.	The number of unique substitution boxes in DES after the 48 bit XOR operation
	are
Option A:	8
Option B:	4
Option C:	6
Option D:	12
Q8.	In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via
Option A:	Scaling of the existing bits
Option B:	Duplication of the existing bits
Option C:	Addition of zeros
Option D:	Addition of ones
Q9.	The subject unique identifier of the X.509 certificates was added in which version?
Option A:	1
Option B:	2
Option C:	3
Option D:	4
Q10.	What is a Hash Function?
Option A:	It creates a small flexible block of data
Option B:	It creates a small, fixed block of data
Option C:	It creates an encrypted block of data
Option D:	It creates a decrypted block of data
Q11.	MD5 produces bits hash data
Option A:	128
Option B:	150
Option C:	160
Option D:	112
Q12.	A(n)is a federal or state organization that binds a public key to an entity
	and issues a certificate
Option A:	KDC
Option B:	Kerberos
Option C:	CA
Option D:	KMC
0.10	
Q13.	Password-based authentication can be divided into two broad categories:
	and

Option A:	fixed; variable
Option B:	time-stamped; fixed
Option C:	fixed; one-time
Option D:	time-stamped; variable
Q14.	Sender chooses $p = 107$, $e1 = 2$, $d = 67$, and the random integer is r=45. Find the
	plaintext to be transmitted if the ciphertext is (28,9).
Option A:	45
Option B:	76
Option C:	66
Option D:	13
Q15.	For a client-server authentication, the client requests from the KDC a for
	access to a specific asset.
Option A:	ticket
Option B:	local
Option C:	token
Option D:	user
Q16.	What is the full-form of CMAC
Option A:	Code-based MAC
Option B:	Cipher-based MAC
Option C:	Construct-based MAC
Option D:	Collective-based MAC
Q17.	A tries to formulate a web resource occupied or busy its users by
	flooding the URL of the victim with unlimited requests than the server can handle.
Option A:	Phishing attack
Option B:	DoS attack
Option C:	Website attack
Option D:	MiTM attack
019	A is a sequential comment of the memory leasting that is allowed a few
Q10.	A is a sequential segment of the memory location that is allocated for containing some data such as a character string or an array of integers
Option A:	Stack
Option R.	
Option C	external storage
Option D:	buffer
Q19.	The attack which can be deployed by infusing a malicious code in a website's
	comment section such type of attack is referred as
Option A:	SQL injection
Option B:	HTML Injection
Option C:	Cross Site Scripting (XSS)
Option D:	Cross Site Request Forgery (XSRF)
_	

Q20.	What are the characteristics of anomaly based IDS?
Option A:	It models the normal usage of network as a noise characterization
Option B:	It doesn't detect novel attacks
Option C:	Anything distinct from the noise is not assumed to be intrusion activity
Option D:	It detects based on signature
Q21.	A is a small malicious program that runs hidden on infected system.
Option A:	Virus
Option B:	Trojan
Option C:	Shareware
Option D:	Adware
Q22.	What is not a good practice for user administration?
Option A:	Isolating a system after a compromise
Option B:	Perform random auditing procedures
Option C:	Granting privileges on a per host basis
Option D:	Using telnet and FTP for remote access
Q23.	Using Rivest, Shamir, Adleman cryptosystem with p=7 and q=9. Encrypt M=24 to
	Ind ciphertext. The Ciphertext is:
Option A:	42
Option A: Option B:	42 93
Option A: Option B: Option C:	42 93 114
Option A: Option B: Option C: Option D:	42 93 114 103
Option A: Option B: Option C: Option D:	42 93 114 103
Option A: Option B: Option C: Option D: Q24.	111d ciphertext. The Ciphertext is: 42 93 114 103 In RSA, $\Phi(n) = $ in terms of p and q
Option A: Option B: Option C: Option D: Q24. Option A:	111d ciphertext. The Ciphertext is: 42 93 114 103 In RSA, $\Phi(n) = $ in terms of p and q (p)/(q)
Option A: Option B: Option C: Option D: Q24. Option A: Option B:	Initial ciphertext. The Ciphertext is: 42 93 114 103 In RSA, $\Phi(n) = $ in terms of p and q (p)/(q) (p)(q)
Option A: Option B: Option C: Option D: Q24. Option A: Option B: Option C:	111d ciphertext. The Ciphertext is: 42 93 114 103 In RSA, $\Phi(n) = $ in terms of p and q (p)/(q) (p)(q) (p-1)(q-1)
Option A: Option B: Option C: Option D: Q24. Option A: Option B: Option C: Option D:	Initial ciphertext. The Ciphertext is: 42 93 114 103 In RSA, $\Phi(n) = $ in terms of p and q (p)/(q) (p)/(q)
Option A: Option B: Option C: Option D: Q24. Option A: Option B: Option C: Option D:	Initial ciphertext. The Ciphertext is: 42 93 114 103 In RSA, $\Phi(n) = $ in terms of p and q (p)/(q) (p)(q) (p-1)(q-1) (p+1)(q+1)
Option A: Option B: Option C: Option D: Q24. Option A: Option A: Option B: Option C: Option D: Q25.	Ind cipnertext. The Cipnertext is: 42 93 114 103 In RSA, $\Phi(n) = __\$
Option A: Option B: Option C: Option D: Q24. Option A: Option B: Option C: Option D: Q25. Option A:	Indestruction 42 93 114 103 In RSA, $\Phi(n) = $ in terms of p and q (p)/(q) (p)(q) (p)(q) (p-1)(q-1) (p+1)(q+1) n = 35; e = 5; C = 10. What is the plaintext (use RSA) ? 3
Option A: Option B: Option C: Option D: Q24. Option A: Option B: Option C: Option D: Q25. Option A: Option B:	Indefinite Ciphertext is: 42 93 114 103 In RSA, $\Phi(n) = $ in terms of p and q (p)/(q) (p)(q) (p-1)(q-1) (p+1)(q+1) n = 35; e = 5; C = 10. What is the plaintext (use RSA) ? 3 7
Option A: Option B: Option C: Option D: Q24. Option A: Option A: Option C: Option D: Q25. Option A: Option B: Option B: Option C:	111d 93 114 103 $(p)/(q)$ $(p)/(q)$ $(p)/(q)$ $(p)/(q)$ $(p)/(q)$ $(p-1)(q-1)$ $(p+1)(q+1)$ n = 35; e = 5; C = 10. What is the plaintext (use RSA) ? 3 7 8