Program: SE Information Technology

Curriculum Scheme: Revised 2012

Examination: Second Year Semester IV

Course Code: SEITC **Course Name: Information Theory and Coding**

Time: 1 hour Max. Marks: 50

==========

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

Q1.	How many numbers less than 20 are relatively prime to 20?
Option A:	7
Option B:	8
Option C:	9
Option D:	6
Q2.	Find GCD (1403,1081) using Euclid's algorithm.
Option A:	23
Option B:	20
Option C:	22
Option D:	25
Q3.	Identify Fermat's theorem.
Option A:	$a^p = 1 \bmod p$
Option B:	$a^{p-1} = 1 \bmod p-1$
Option C:	$a^{p-1} = 1 \bmod p$
Option D:	$a = 1 \bmod p$
Q4.	solve using chinses remainder theorem. X=3 mod 4 X=1 mod 5 X=2 mod 2
Option A:	X Ξ 10 mod 60
Option B:	X Ξ 11 mod 60
Option C:	X Ξ 11 mod 100
Option D:	X Ξ 15 mod 60
Q5.	Encrypt 'hello' using ceasor cipher.
Option A:	encrypted text=hello
Option B:	encrypted text=khppr

Option C:	encrypted text=kheer
Option D:	encrypted text=khoor
Q6.	Encrypt 'hello how are you' using monoalphabetic cipher.
Option A:	CIPHERTEXT= KHOOR KRZ DUH BRY
Option B:	CIPHERTEXT= KHEER KEZ DUH BRY
Option C:	CIPHERTEXT= KHOOR KRZ DOH BRY
Option D:	CIPHERTEXT= LHOOR KEZ DUH BRY
Q7.	In which cipher reuse of key is not possible?
Option A:	Data
Option B:	Wave
Option C:	Stream
Option D:	Block
Q8.	Block size of DES is?
Option A:	8 bits
Option B:	16 bits
Option C:	32 bits
Option D:	64 bits
Q9.	How many rounds are there in DES algorithm?
Option A:	4
Option B:	8
Option C:	16
Option D:	32
Q10.	SET TOP BOX is an application of which encryption std?
Option A:	AES
Option B:	DES
Option C:	Diffie-Hellman
Option D:	Robin-Millar
Q11.	The key length for DES algorithm is?
Option A:	58 bits
Option B:	56 bits
Option C:	32 bits
Option D:	64 bits
Q12.	Check whether the number 29 is prime or not using Miller Rabin algorithm.
Option A:	29 is prime
Option B:	29 is not prime
Option C:	29 may or may not be prime
Option D:	Information is not sufficient to check
Q13.	solve using chinese remainder therom

	x=2 mod 3 x=2 mod 7 x=1 mod 4
Option A:	65 mod 21
Option B:	65 mod 28
Option C:	140 mod 84
Option D:	65 mod 84
Q14.	Alice generates her RSA keys by selecting two primes: p=11 and q=13, then the totient of n is?
Option A:	120
Option B:	143
Option C:	11
Option D:	13
Q15.	Alice generates her RSA keys by selecting two primes: p=11 and q=13.Bob wants to send Alice an encrypted message M so he obtains her RSA public key as?
Option A:	120,143
Option B:	143,120
Option C:	143,7
Option D:	7,143
Q16.	Digital signatures use following algorithm.
Option A:	AES
Option B:	DES
Option C:	Robin Millar
Option D:	RSA
Q17.	The serious limitation of Diffie-Hellman key exchange is:
Option A:	Lack of identity
Option B:	Lack of authentication
Option C:	Lack of integrity
Option D:	Lack of consistency
Q18.	In which step of JPEG compression we lose some information?
Option A:	DCT
Option B:	Quantization
Option C:	Compression
Option D:	DST
Q19.	The disadvantage of GIF compression is
Option A:	It’s a lossy compression.
Option B:	It’s a bitmap image format.
Option C:	LZW compression technique is used.
Option D:	Only 256 colours are available in a frame.

Q20.	JPEG stands for
Option A:	Join Pictures Expert Group
Option B:	Joint Property Expert Group
Option C:	Joint Pictures Expert Group
Option D:	Joint Pictures Exponential Group
Q21.	Let $m \neq 0$ be an integer. We say that two integers a and b are *congruent modulo* m if there is an integer k such that $a - b = km$, and in this case we write
Option A:	$a \equiv b \bmod m$
Option B:	$b \equiv a \bmod m$
Option C:	$a \equiv ab \bmod m$
Option D:	$b \equiv ab \bmod m$
Q22.	If $a \equiv b \bmod m$, then $b \equiv a \bmod m$,then which property is true for integers a and b?
Option A:	Reflexivity
Option B:	Symmetry
Option C:	Transitivity
Option D:	Symmetry and Transitivity
Q23.	The _____ is the largest positive integer that divides both “a” and “b”.
Option A:	LCD
Option B:	GCD
Option C:	Totient
Option D:	Prime number
Q24.	For [(a mod n) – (b mod n)] mod n the following is true.
Option A:	(a- b) mod n
Option B:	(a) mod n
Option C:	(b) mod n
Option D:	(a+b) mod n
Q25.	The primitive roots of 10 are:
Option A:	4,1
Option B:	3,7
Option C:	3,5
Option D:	3,4