Id	
Question	**Introduction and Mathematical Foundations:**
A	Cipher text
B	Cryptography
C	Plain Text
D	Symmetric
Marks	1.5
Unit	1

Id	
Question	An asymmetric-key (or public-key) cipher uses
A	1 Key
B	2 Key
C	3 Key
D	4 Key
Marks	1.5
Unit	1

Id	
Question	A straight permutation cipher or a straight P-box has the same number of inputs as
A	Cipher
B	Frames
C	Outputs
D	Bits
Marks	1.5
Unit	1

Id	
Question	The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not
A	Authenticated
B	Joined
C	Submit
D	Separate
Marks	1.5
Unit	1

Id	
Question	Which encryption involve only one key to encrypt and decrypt data.
A	Asymetric key
B	**Symetric Key**
C	One key
D	Transformation
Marks	1.5
Unit	1

Id	
Question	……. Allows authorized user to access data.
A	Intrgrity
B	Availability
C	Confidentiality
D	Security
Marks	1.5
Unit	1

Id	
Question	In asymmetric key cryptography, the private key is kept by _____
A	Sender
B	Receiver
C	sender and receiver
D	all the connected devices to the network
Marks	1.5
Unit	1

Id	
Question	In cryptography, what is cipher?
A	algorithm for performing encryption and decryption
B	encrypted message
C	both algorithm for performing encryption and decryption and encrypted message
D	decrypted message
Marks	1.5
Unit	1

Id	
Question	Cryptanalysis is used _____
A	To find some insecurity in a cryptographic scheme
B	To increase the speed
C	To encrypt the data
D	To make new ciphers
Marks	1.5
Unit	1

Id	
Question	Cryptographic hash function takes an arbitrary block of data and returns _____
A	fixed size bit string
B	variable size bit string
C	both fixed size bit string and variable size bit string
D	variable sized byte string
Marks	1.5
Unit	1

Id	
Question	Which of the following propositions is tautology?
A	(p v q)→q
B	p v (q→p)
C	p v (p→q)
D	Both (b) & (c)
Marks	1.5
Unit	1

Id	
Question	Which of the proposition is p^ (~ p v q) is
A	A tautology
B	A contradiction
C	Logically equivalent to p ^ q
D	All of above
Marks	1.5
Unit	1

Id	
Question	How many bytes of the secret key is generated using Diffie-Hellman encryption/decryption scheme?
A	256
B	871
C	1024
D	962
Marks	1.5
Unit	1

Id	
Question	In which of the following systems, encryption slower than decryption?
A	elliptic curve cryptography
B	parabolic curve cryptography
C	symmetric cryptography
D	antisymmetric cryptography
Marks	1.5
Unit	1

Id	
Question	If there are 256 cipher texts per plain text and a total of 218 plaintexts of length 18 exists. Then determine the number of distinct ciphertexts?
A	761
B	274
C	186
D	289
Marks	1.5
Unit	1

Id	
Question	TEA cipher uses which of the following structure?
A	standard cipher structure
B	pseudo random structure
C	feistel structure
D	block structure
Marks	1.5
Unit	1

Id	
Question	Let A’s public key is n=6, 736, 180, 7817, 961, 456, 267 and e = 5 and B sends the ciphertext. c = 456, 871, 122, 391, 882, 538 to A. Determine B’s message in numeric format?
A	235813
B	57971.89
C	770190.04
D	687651.9
Marks	1.5
Unit	1

Id	
Question	In encryption, which of the following is the best text encoding technique?
A	ASCII encoding
B	Hex-encoding
C	Unicode technique
D	Base64 encoding
Marks	1.5
Unit	1

Id	
Question	_____ are used as the base of the Public Key Infrastructure.
A	SSL certificates
B	TLS certificates
C	X.509 certificates
D	HAS certificates
Marks	1.5
Unit	1

Id	
Question	The default key size of RC2 Feistel cipher is _____
A	64GB
B	64 bits
C	64 bytes
D	64KB
Marks	1.5
Unit	1

Id	
Question	How many combinations of keys can be constructed from a 72 ciphertext stream cipher?
A	4271
B	7345
C	3291
D	2556
Marks	1.5
Unit	1

Id	
Question	What is the block size of RC6 Feistel block cipher?
A	5013 bits
B	128 bits
C	596 bits
D	1768 bits
Marks	1.5
Unit	1

Id	
Question	Suppose that there are two primes, P1 = 229 and p2 = 61. Find the value of z and Φ.
A	13969, 13680
B	5853, 23452
C	7793, 34565
D	17146, 69262
Marks	1.5
Unit	1

Id	
Question	_____ can decrypt traffic to make it available to all other network security functions such as web proxies.
A	SSL visibility appliances
B	RSA appliances
C	Rodriguez cipher system
D	Standard cipher system
Marks	1.5
Unit	1

Id	
Question	The ROT13 caesar cipher system has an offset of _____
A	13
B	45
C	71
D	37
Marks	1.5
Unit	1

Id	
Question	In a public key system, the cipher text received is C = 10 if RSA encryption used with a public key(e = 11, n = 77) to deduce the plain text. Determine the value of $\phi(n)$?
A	49
B	60
C	123
D	70
Marks	1.5
Unit	1

Id	
Question	To encrypt a message _____ is used on the character’s positions.
A	boolean algebra
B	bijective function
C	inverse function
D	surjective function
Marks	1.5
Unit	1

Id	
Question	The public key of given user, in an RSA encryption system is e = 57 and n = 3901. What is the value of Euler's totient function $\phi(n)$ for calculating the private key of the user?
A	4369
B	3772
C	871
D	7892
Marks	1.5
Unit	1

Id	
Question	Using RSA algorithm what is the value of cipher test c if the plain text e = 7 and P = 5, q = 16 & n = 832. Determine the Euler's totient function for the plain text?
A	47
B	584
C	428
D	60
Marks	1.5
Unit	1

Id	
Question	There are 67 people in a company where they are using secret key encryption and decryption system for privacy purpose. Determine the number of secret keys required for this purpose?
A	887
B	6529
C	2211
D	834
Marks	1.5
Unit	1

Id	
Question	In a transposition cipher, the plaintext is constructed by the _____ of the ciphertext.
A	permutation
B	combination
C	sequence
D	series
Marks	1.5
Unit	1

Id	
Question	How many bits of message does the Secure Hash Algorithm produce?
A	160 bits
B	1035 bits
C	621 bits
D	3761 bits
Marks	1.5
Unit	1

Id	
Question	If a source’s entropy is higher than other sources, then the source’s bytes are:
A	less predictable.
B	more predictable.
C	just as predictable.
D	None of A,B,C
Marks	1.5
Unit	1

Id	
Question	If a source’s entropy is lower than other sources, then the source’s bytes are:
A	less compressible.
B	more compressible.
C	just as compressible.
D	All of A,B,C.
Marks	1.5
Unit	1

Id	
Question	If the signal to noise ratio of a Chanel increases,and then the channel capacity:
A	increases.
B	decreases.
C	remains the same.
D	None of these.
Marks	1.5
Unit	1

Id	
Question	The keyspace of a Cæsar-like number coding formed by rotating the digits 0-9 is:
A	7.
B	8.
C	9.
D	10.
Marks	1.5
Unit	1

Id	
Question	The Vigenère cipher is an example of:
A	a Cæsar cipher.
B	a monoalphabetic cipher.
C	a polyalphabetic cipher.
D	None of A,B,C.
Marks	1.5
Unit	1

Id	
Question	In a good cipher system, if you changed a single bit in the plaintext, approximately what percentage of the ciphertext should change?
A	1%.
B	50%.
C	100%.
D	None of A,B,C
Marks	1.5
Unit	1

Id	
Question	If the relative entropy of a 30,000 byte file was, then it may be compressed to about
A	10,000 bytes.
B	30,000 bytes.
C	90,000 bytes.
D	None of A,B,C
Marks	1.5
Unit	1

Id	
Question	Information has _____ if unauthorized writing is prohibited.
A	Confidentiality.
B	Integrity.
C	Security.
D	Availability
Marks	1.5
Unit	1

Id	
Question	Which one is a Substitution Technique
A	Real Fence
B	Keyless
C	Keyed
D	Hill Cipher
Marks	1.5
Unit	1

Id	
Question	In how many number of times we can change plain text into cipher text using transposition technique.
A	(n-1)
B	n!
C	nlogn
D	n+1
Marks	1.5
Unit	1

Id	
Question	Find Cipher text for plain text allthebestforexam using real fence technique with depth=2.
A	saeoteetlmxrfsbhla
B	lmxrfsbhlasaeteetl
C	alhbsfrxmlteetoeas
D	baalhfrmlteetasoem
Marks	1.5
Unit	1

Id	
Question	Divide (HAPPY)26 by (SAD)26. We get quotient –
A	KD
B	LD
C	JC
D	MC
Marks	1.5
Unit	1

Id	
Question	Which one of the following algorithm is not used in asymmetric-key cryptography?
A	rsa algorithm
B	diffie-hellman algorithm
C	electronic code book algorithm
D	dsa algorithm
Marks	1.5
Unit	1

Id	
Question	In cryptography, the order of the letters in a message is rearranged by _____
A	transpositional ciphers
B	substitution ciphers
C	both transpositional ciphers and substitution ciphers
D	quadratic cipher
Marks	1.5
Unit	1

Id	
Question	What is the formula for encrypting message using hill cipher
A	K-P mod 26
B	K+P mod 26
C	K/P mod 26
D	KP mod 26
Marks	1.5
Unit	1

Id	
Question	How we can group the plain text= Hexxoc using play fair. Substitute L=X
A	He xx oc
B	He xl oc
C	He xz xo ez
D	Hx ex xz
Marks	1.5
Unit	1

Id	
Question	Ceaser cipher is also called as
A	Polyalphabeticcipher
B	Transposition cipher
C	Hill cipher
D	Shift cipher
Marks	1.5
Unit	1

Id	
Question	Which is not a type of active attack
A	Repleyz
B	Denial of Service
C	Monoalphabetic
D	Modification of message
Marks	1.5
Unit	1

Id	
Question	The minimum nyquist bandwidth needed for baseband transmission of Rs symbols per second is
A	Rs
B	2Rs
C	**Rs/2**
D	Rs2
Marks	1.5
Unit	1

Id	
Question	The capacity relationship is given by
A	C = W log2 (1+S/N)
B	C = 2W log2 (1+S/N)
C	C = W log2 (1-S/N)
D	C = W log10 (1+S/N)
Marks	1.5
Unit	1

Id	
Question	Which parameter is called as Shannon limit?
A	PB/N0
B	EB/N0
C	EBN0
D	None of the mentioned
Marks	1.5
Unit	1

Id	
Question	Entropy is the measure of
A	Amount of information at the output
B	Amount of information that can be transmitted
C	Number of error bits from total number of bits
D	None of the mentioned
Marks	1.5
Unit	1

Id	
Question	Equivocation is the
A	Conditional entropy
B	Joint entropy
C	Individual entropy
D	None of the mentioned
Marks	1.5
Unit	1

Id	
Question	For a error free channel, conditional probability should be
A	Zero
B	One
C	Equal to joint probability
D	Equal to individual probability
Marks	1.5
Unit	1

Id	
Question	Average effective information is obtained by
A	Subtracting equivocation from entropy
B	Adding equivocation with entropy
C	Ratio of number of error bits by total number of bits
D	None of the mentioned
Marks	1.5
Unit	1

Id	
Question	Turbo codes are
A	Forward error correction codes
B	Backward error correction codes
C	Error detection codes
D	None of the mentioned
Marks	1.5
Unit	1

Id	
Question	Components used for generation of turbo codes are
A	Inter leavers
B	Punching pattern
C	Inter leavers & Punching pattern
D	None of the mentioned
Marks	1.5
Unit	1

Id	
Question	Decoders are connected in series.
A	True
B	False
C	
D	
Marks	1.5
Unit	1

Id	
Question	The inter leaver connected between the two decoders is used to
A	Remove error bursts
B	Scatter error bursts
C	Add error bursts
D	None of the mentioned
Marks	1.5
Unit	1

Id	
Question	In soft decision approach what does -127 mean?
A	Certainly one
B	Certainly zero
C	Very likely zero
D	Very likely one
Marks	1.5
Unit	1

Id	
Question	In soft decision approach 100 means?
A	Certainly one
B	Certainly zero
C	Very likely zero
D	Very likely one
Marks	1.5
Unit	1

Id	
Question	In soft decision approach 0 represents
A	Certainly one
B	Certainly zero
C	Very likely zero
D	Could be either zero or one
Marks	1.5
Unit	1

Id	
Question	For a binary symmetric channel, the random bits are given as
A	Logic 1 given by probability P and logic 0 by (1-P)
B	Logic 1 given by probability 1-P and logic 0 by P
C	Logic 1 given by probability P2 and logic 0 by 1-P
D	Logic 1 given by probability P and logic 0 by (1-P)2
Marks	1.5
Unit	1

Id	
Question	The channel capacity according to Shannon's equation is
A	Maximum error free communication
B	Defined for optimum system
C	Information transmitted
D	All of the above
Marks	1.5
Unit	1

Id	
Question	For M equally likely messages, M>>1, if the rate of information R > C, the probability of error is
A	Arbitrarily small
B	Close to unity
C	Not predictable
D	Unknown
Marks	1.5
Unit	1

Id	
Question	For M equally likely messages, M>>1, if the rate of information R <= C, the probability of error is
A	Arbitrarily small
B	Close to unity
C	Not predictable
D	Unknown
Marks	1.5
Unit	1

Id	
Question	The negative statement for Shannon's theorem states that
A	If R > C, the error probability increases towards Unity
B	If R < C, the error probability is very small
C	None of the above
D	Not applicable
Marks	1.5
Unit	1

Id	
Question	According to Shannon Hartley theorem,
A	the channel capacity becomes infinite with infinite bandwidth
B	the channel capacity does not become infinite with infinite bandwidth
C	Has a tradeoff between bandwidth and Signal to noise ratio
D	Both b) and c) are correct
Marks	1.5
Unit	1

Id	
Question	For a (7, 4) block code, 7 is the total number of bits and 4 is the number of
A	Information bits
B	Redundant bits
C	Total bits- information bits
D	None of the above
Marks	1.5
Unit	1

Id	
Question	Interleaving process permits a burst of B bits, with l as consecutive code bits and t errors when
A	B <= 2tl
B	B >= tl
C	B <= tl/2
D	B <= tl
Marks	1.5
Unit	1

Id	
Question	The code in convolution coding is generated using
A	EX-OR logic
B	AND logic
C	OR logic
D	None of the above
Marks	1.5
Unit	1

Id	
Question	For decoding in convolution coding, in a code tree,
A	Diverge upward when a bit is 0 and diverge downward when the bit is 1
B	Diverge downward when a bit is 0 and diverge upward when the bit is 1
C	Diverge left when a bit is 0 and diverge right when the bit is 1
D	Diverge right when a bit is 0 and diverge left when the bit is 1
Marks	1.5
Unit	1

Id	
Question	Graphical representation of linear block code is known as
A	Pi graph
B	Matrix
C	Tanner graph
D	None of the above
Marks	1.5
Unit	1

Id	
Question	The probability density function of a Markov process is
A	p(x1,x2,x3.....xn) = p(x1)p(x2/x1)p(x3/x2).....p(xn/xn-1)
B	p(x1,x2,x3.....xn) = p(x1)p(x1/x2)p(x2/x3).....p(xn-1/xn)
C	p(x1,x2,x3.....xn) = p(x1)p(x2)p(x3).....p(xn)
D	p(x1,x2,x3.....xn) = p(x1)p(x2 * x1)p(x3 * x2).....p(xn * xn-1)
Marks	1.5
Unit	1

Id	
Question	**The capacity of Gaussian channel is**
A	C = 2B(1+S/N) bits/s
B	C = B^2(1+S/N) bits/s
C	C = B(1+S/N) bits/s
D	C = B(1+S/N)2 bits/s
Marks	1.5
Unit	1

Id	
Question	**For M equally likely messages, the average amount of information H is**
A	$H = \log_{10}M$
B	$H = \log_{2}M$
C	$H = \log_{10}M^{2}$
D	$H = 2\log_{10}M$
Marks	1.5
Unit	1

Id	
Question	**The capacity of a binary symmetric channel, given H(P) is binary entropy function is**
A	1 - H(P)
B	H(P) - 1
C	$1 - H(P)^2$
D	$H(P)^2 - 1$
Marks	1.5
Unit	1

Id	
Question	The Advance Encryption Standard(AES) was designed by
A	National Institute of Standards and Technology
B	IBM
C	HP
D	Intel
Marks	1.5
Unit	2

Id	
Question	AES uses a _____ bit block size and a key size of _____ bits.
A	128; 128 or 256
B	64; 128 or 192
C	256; 128, 192, or 256
D	128; 128, 192, or 256
Marks	1.5
Unit	2

Id	
Question	Which one of the following is not a cryptographic algorithm- JUPITER, Blowfish, RC6, Rijndael and Serpent?
A	JUPITER
B	Blowfish
C	Serpent
D	Rijndael
Marks	1.5
Unit	2

Id	
Question	How many rounds does the AES-192 perform
A	10
B	12
C	14
D	16
Marks	1.5
Unit	2

Id	
Question	For the AES-128 algorithm there are _____ similar rounds and _____ round is different.
A	2 pair of 5 similar rounds ; every alternate
B	9 ; the last
C	8 ; the first and last
D	10 ; no
Marks	1.5
Unit	2

Id	
Question	Which one of the following modes of operation in DES is used for operating short data?
A	Cipher Feedback Mode (CFB)
B	Cipher Block chaining (CBC)
C	Electronic code book (ECB)
D	Output Feedback Modes (OFB)
Marks	1.5
Unit	2

Id	
Question	Which of the following statements are true ? i) In the CBC mode, the plaintext block is XORed with previous ciphertext block before encryption ii) The CTR mode does not require an Initialization Vector iii) The last block in the CBC mode uses an Initialization Vector iv) In CBC mode repetitions in plaintext do not show up in ciphertext
A	iii)
B	ii) and iv)
C	All the Statements are true
D	i) ii) and iv)
Marks	1.5
Unit	2

Id	
Question	Which of the following modes does not implement chaining or “dependency on previous stage computations”?
A	CTR, ECB
B	CTR, CFB
C	CFB, OFB
D	ECB, OFB
Marks	1.5
Unit	2

Id	
Question	The counter value in CTR modes repeats are a regular interval.
A	TRUE
B	FALSE
C	May Be
D	Can’t Be
Marks	1.5
Unit	2

Id	
Question	The last two blocks of the XTS-AES mode are –
A	padded as 10*
B	encrypted/ decrypted using ciphertext-stealing
C	padded as 10*1
D	padded and then swapped after encryption/ decryption
Marks	1.5
Unit	2

Id	
Question	Which algorithm among- MARS, Blowfish, RC6, Rijndael and Serpent -was chosen as the AES algorithm?
A	MARS
B	Blowfish
C	RC6
D	Rijndael
Marks	1.5
Unit	2

Id	
Question	How many rounds does the AES-192 perform?
A	10
B	12
C	14
D	16
Marks	1.5
Unit	2

Id	
Question	How many rounds does the AES-256 perform?
A	10
B	12
C	14
D	16
Marks	1.5
Unit	2

Id	
Question	What is the expanded key size of AES-192?
A	44 words
B	60 words
C	52 words
D	36 words
Marks	1.5
Unit	2

Id	
Question	The 4×4 byte matrices in the AES algorithm are called
A	States
B	Words
C	Transitions
D	Permutations
Marks	1.5
Unit	2

Id	
Question	In AES the 4×4 bytes matrix key is transformed into a keys of size _____
A	32 words
B	64 words
C	54 words
D	**44 words**
Marks	1.5
Unit	2

Id	
Question	There is an addition of round key before the start of the AES round algorithms.
A	TRUE
B	FALSE
C	All
D	None
Marks	1.5
Unit	2

Id	
Question	A= [4 2 2 1] **Is the given matrix 'A', a valid key to be used for encryption**?
A	Data insufficient
B	Yes
C	No
D	Can't be determined
Marks	1.5
Unit	2

Id	
Question	Authentication service that can be used in windows platform is
A	DES
B	RSA
C	MD5
D	KERBEROS
Marks	1.5
Unit	2

Id	
Question	An attack ok authenticity is
A	Interception
B	Interruption
C	Fabrication
D	Violation
Marks	1.5
Unit	2

Id	
Question	The process of writing the text as rows and read it as columns is known as a) b) **c)** d)
A	Vernam cipher
B	Caesar cipher
C	Transposition columnar cipher
D	Homophonic substitution cipher
Marks	1.5
Unit	2

Id	
Question	In IDEA key is of _____ bits.
A	128
B	64
C	25
D	512
Marks	1.5
Unit	2

Id	
Question	Biometric authentication works on the basis of
A	Human characteristics
B	Password
C	Smart cards
D	Pin
Marks	1.5
Unit	2

Id	
Question	In polyalphabetic cipher, the characters in plaintext have a relation with the characters in cipher text
A	One to many
B	One to one
C	Many to one
D	Many to many
Marks	1.5
Unit	2

Id	
Question	There are _____ encryption rounds in IDEA.
A	5
B	16
C	10
D	8
Marks	1.5
Unit	2

Id	
Question	_____ involves trying every possible key until a proper translation of cipher text into plain text is obtained.
A	Man in the middle attack
B	Chosen Plain text Attack
C	Brute Force attack
D	None of these
Marks	1.5
Unit	2

Id	
Question	_____ operates on smaller unit of plain text. a) **b)** c) d)
A	Block cipher
B	Rail fence
C	Stream cipher
D	Both (a) and (b)
Marks	1.5
Unit	2

Id	
Question	In_____ mode, the same plaintext value will always result in the same cipher text value.
A	Cipher Block Chaining
B	Cipher Feedback
C	Electronic code book
D	Output Feedback
Marks	1.5
Unit	2

Id	
Question	The number of tests required to break the DES algorithm are
A	2.8×10^14
B	4.2×10^9
C	1.84×10^19
D	7.2×10^16
Marks	1.5
Unit	2

Id	
Question	The number of test required to break the Double DES are
A	2111
B	2112
C	1312
D	1231
Marks	1.5
Unit	2

Id	
Question	In affine block cipher systems if f(m)=Am + t, what is f(m1+m2+m3) ?
A	f(m1) + f(m2) + f(m3) + t
B	f(m1) + f(m2) + f(m3) +2t
C	f(m1) + f(m2) + f(m3)
D	2(f(m1) + f(m2) + f(m3))
Marks	1.5
Unit	2

Id	
Question	If the key is 110100001, the output of the SP network for the plaintext: 101110001 is
A	110100011
B	110101110
C	10110111
D	11111010
Marks	1.5
Unit	2

Id	
Question	Confusion hides the relationship between the ciphertext and the plaintext.
A	TRUE
B	FALSE
Marks	1.5
Unit	2

Id	
Question	The S-Box is used to provide confusion, as it is dependent on the unknown key.
A	TRUE
B	FALSE
Marks	1.5
Unit	2

Id	
Question	Which of the following slows the cryptographic algorithm . 1) Increase in Number of rounds 2) Decrease in Block size 3) Decrease in Key Size 4) Increase in Sub key Generation
A	1 and 3
B	2 and 3
C	3 and 4
D	2 and 4
Marks	1.5
Unit	2

Id	
Question	What is the size of key in SDES?
A	64 bit
B	10 bit
C	20 bits
D	16 bits
Marks	1.5
Unit	2

Id	
Question	DES is developed by
A	IBM
B	Intel
C	Apple
D	Microsoft
Marks	1.5
Unit	2

Id	
Question	What is the number of possible 3X3 affine cipher transformation?
A	1024
B	840
C	1344
D	168
Marks	1.5
Unit	2

Id	
Question	Rail Fence Technique is an example of
A	Substitution
B	Transposition
C	Product cipher
D	Caesar cipher
Marks	1.5
Unit	2

Id	
Question	SET is
A	Electronic Payment System
B	Security Protocol
C	Credit card payment
D	Internet Payment System
Marks	1.5
Unit	2

Id	
Question	Public key encryption is advantageous over Symmetric key Cryptography because of
A	Speed
B	Space
C	Key exchange
D	Key length
Marks	1.5
Unit	2

Id	
Question	The sub key length at each round of DES is_____
A	32
B	56
C	48
D	64
Marks	1.5
Unit	2

Id	
Question	MAC is used to ensure
A	Authentication
B	Confidentiality
C	Authentication and integrity
D	Authentication and confidentiality
Marks	1.5
Unit	2

Id	
Question	Total no. of messages used in SSL Handshake Protocol is
A	12
B	10
C	8
D	14
Marks	1.5
Unit	2

Id	
Question	A worm _____ modify a program.
A	Does not
B	Does
C	May or may not
D	None of these
Marks	1.5
Unit	2

Id	
Question	Differential Cryptanalysis can be mounted on
A	DES encryption algorithm
B	AES encryption algorithm
C	RSA encryption algorithm
D	Deffie-Hellman key exchange algorithm
Marks	1.5
Unit	2

Id	
Question	Message Digest length in SHA 1 is_____ bits.
A	128
B	160
C	64
D	54
Marks	1.5
Unit	2

Id	
Question	_____ prevents either sender or receiver from denying a transmitted message.
A	Access Control
B	Non repudiation
C	Masquerade
D	Integrity
Marks	1.5
Unit	2

Id	
Question	A Macro virus is
A	Platform dependent
B	Platform independent
C	Idle
D	Hidden
Marks	1.5
Unit	2

Id	
Question	Which one of the following is active attack? **a)**b) c) d)
A	Masquerade
B	Traffic analysis
C	Eavesdropping
D	Shoulder surfing
Marks	1.5
Unit	2

Id	
Question	Which of the following is passive attack?
A	Relay attack
B	Masquerade
C	Traffic analysis
D	Denial of Service
Marks	1.5
Unit	2

Id	
Question	A firewall that uses two TCP connections is
A	Bastion
B	Application gateway
C	Circuit level gateway
D	Packet filtering
Marks	1.5
Unit	2

Id	
Question	IPsec services are available in _____ Layer.
A	Application
B	Data link
C	Network
D	Transport
Marks	1.5
Unit	2

Id	
Question	Caesar cipher is an example of
A	Substitution cipher
B	Transposition cipher
C	Substitution as well as transposition
D	None of these
Marks	1.5
Unit	2

Id	
Question	Tool for implementing security policy may be called as
A	Security process
B	Security authentication
C	Security gaps
D	Security mechanism
Marks	1.5
Unit	2

Id	
Question	To generate the sub-key P1 to P18 we use the hexadecimal equivalent digits of _____
A	0. 7864
B	0. 1415
C	0. 1542
D	0. 7535
Marks	1.5
Unit	3

Id	
Question	How many entries are present in each of the S-boxes present in the blowfish algorithm?
A	256
B	512
C	1024
D	64
Marks	1.5
Unit	3

Id	
Question	How many S-boxes are present in the blowfish algorithm?
A	2
B	4
C	6
D	8
Marks	1.5
Unit	3

Id	
Question	The blowfish algorithm’s key expansion converts a key of at most 448 bits into several subkey arrays totaling _____ bytes.
A	4096
B	4608
C	4168
D	4864
Marks	1.5
Unit	3

Id	
Question	What is the minimum size of the key in blowfish algorithm?
A	64 bits
B	32 bits
C	56 bits
D	48 bits
Marks	1.5
Unit	3

Id	
Question	What is the maximum size of the key in blowfish algorithm?
A	256 bits
B	512 bits
C	56 bits
D	48 bits
Marks	1.5
Unit	3

Id	
Question	Blowfish encrypts blocks of plaintext which have size
A	256 bits
B	64 bits
C	72 bits
D	128 bits
Marks	1.5
Unit	3

Id	
Question	Intel digital random number generator uses which among the following methods to generate random bits?
A	pulse detectors of ionizing radiating events
B	gas discharge tubes
C	wind resistance
D	thermal noise
Marks	1.5
Unit	3

Id	
Question	Which of the following statements are true? i) PRNGs are slower than TRNGs ii) PRNGs are periodic iii) TRNGs are nondeterministic
A	i and ii
B	i
C	ii and iii
D	All are true
Marks	1.5
Unit	3

Id	
Question	Which of the following statements are true? i) Stream Ciphers are fasters than Block Ciphers ii) Block Ciphers can reuse keys iii) Block ciphers use lesser code than stream ciphers
A	i and ii
B	I
C	ii and iii
D	All are true
Marks	1.5
Unit	3

Id	
Question	Which of the following is not a valid design parameter to be considered in designing stream ciphers?
A	Keystream should be truly as random as possible
B	Encryption sequence should have a large value
C	Output of the PRNG (the key) should be sufficiently large
D	All of the mentioned are valid points that should be considered while designing stream cipher blocks
Marks	1.5
Unit	3

Id	
Question	What is the Seed length (seedlen) length for AES-192 ?
A	428
B	384
C	320
D	512
Marks	1.5
Unit	3

Id	
Question	The CTR mode uses a Key K and an Initial Vector V. The Intel Digital Random Number generator has these values initially as
A	K = 0 ; V = 1
B	K = 0 ; V = 0
C	K = 1 ; V = 1
D	K = 1 ; V = 0
Marks	1.5
Unit	3

Id	
Question	Which of the following PRNGs is used in most recent Intel Chips?
A	ANSI X9.17 PRNG
B	NIST CTR_DRBG
C	ANSI standard X9.82
D	None of the mentioned
Marks	1.5
Unit	3

Id	
Question	ANSI X9.17 uses a seed of size
A	56 bits
B	64 bits
C	32 bits
D	128 bits
Marks	1.5
Unit	3

Id	
Question	Which mode is less prone to decryption : PRNG using CTR / PRNG using OFB?
A	OFB
B	CTR
C	Both are equally prone
D	Both can’t be decrypted
Marks	1.5
Unit	3

Id	
Question	The above algorithm is for the CTR mode.
A	True
B	False. It is for the ECB mode
C	False. It is for the OFB mode
D	False. It is for the CFB mode
Marks	1.5
Unit	3

Id	
Question	Which mode is recommend for the RFC 4086 Random number generator?
A	CFB
B	CBC
C	OFB
D	CTR
Marks	1.5
Unit	3

Id	
Question	The CTR algorithm for PRNG is known as
A	CTR_PRNG
B	X-SESS
C	CTR-SESS
D	CTR_DRBG
Marks	1.5
Unit	3

Id	
Question	Which mode is recommend for the ANSI standard X9.82 Random number generator?
A	OFB
B	CTR
C	CFB
D	CFB
Marks	1.5
Unit	3

Id	
Question	Which mode is recommend for the X9.82 Random number generator?
A	OFB
B	CBC
C	CFB
D	CTR
Marks	1.5
Unit	3

Id	
Question	Which of these modes is an appropriate mode for PRNG?
A	ECB
B	CBC
C	CFB
D	CTR
Marks	1.5
Unit	3

Id	
Question	Find the first 8 bits for Blum Blum Shub Bit Generator when seed = 101355 and n = 192649.
A	10101010
B	11100010
C	11001011
D	11001110
Marks	1.5
Unit	3

Id	
Question	A CSPRBG is defined as one that passes the ----- test.
A	Runs test
B	Maurer’s Universal statistical test
C	Frequency Test
D	On-bit test
Marks	1.5
Unit	3

Id	
Question	The appropriate value for m (in LCM) is
A	$2^{(31)} – 1$
B	$2^{(31)}$
C	$2^{(32)}$
D	$2^{(32)} – 1$
Marks	1.5
Unit	3

Id	
Question	Using the Linear Congruential Method, for a=5, c=0 and m=32. The period is
A	8
B	4
C	9
D	11
Marks	1.5
Unit	3

Id	
Question	Using the Linear Congruential Method (LCM), for a=7, c=0 and m=32. The period is
A	13
B	4
C	11
D	7
Marks	1.5
Unit	3

Id	
Question	With reference to stream ciphers, the output of the generator is called
A	Byte Stream
B	Re-Seed Interval
C	Key Length
D	Keystream
Marks	1.5
Unit	3

Id	
Question	What is the output value of the mathematical function 16 mod 3?
A	0
B	1
C	3
D	5
Marks	1.5
Unit	3

Id	
Question	XOR and addition operations take place on bytes of size
A	8 bits
B	16 bits
C	32 bits
D	64 bits
Marks	1.5
Unit	3

Id	
Question	Which of the following statements are true? i) Stream Ciphers are fasters than Block Ciphers ii) Block Ciphers can reuse keys iii) Block ciphers use lesser code than stream ciphers
A	i and ii
B	i
C	ii and iii
D	All are true
Marks	1.5
Unit	3

Id	
Question	ANSI X9.17 uses which cryptographic algorithm?
A	DES
B	AES
C	RC5
D	3DES
Marks	1.5
Unit	3

Id	
Question	Which one of the following is not a RC5 mode of operation?
A	RC5 block cipher
B	RC5-Cipher Block Chaining
C	RC5-Cipher Padding
D	RC5-CipherText Stealing
Marks	1.5
Unit	3

Id	
Question	The number of transistors used in the INTEL DRNG
A	8
B	2
C	4
D	5
Marks	1.5
Unit	3

Id	
Question	Pretty Good Privacy(PGP) uses which PRNG?
A	ANSI X9.82
B	RFC 4086
C	NIST SP 800-90
D	ANSI X9.17
Marks	1.5
Unit	3

Id	
Question	Which mode is recommend for the NIST SP 800-90 Random number generator?
A	OFB
B	CBC
C	CFB
D	CTR
Unit	3

Id	
Question	Key used in the symmetric key cryptography is
A	Public key
B	Private key
C	Permanent key
D	Session key
Marks	1.5
Unit	2

Id	
Question	A polymorphic virus undergoes
A	Crossover
B	Mutation
C	Genetic processing
D	None of these.
Marks	1.5
Unit	2

Id	
Question	For confidentiality, data to be sent is
A	Encrypted
B	Decrypted
C	Corrected
D	Both (a) and (b)
Marks	1.5
Unit	2

Id	
Question	In MD-5 the length of the message digest is
A	160
B	128
C	64
D	54
Marks	1.5
Unit	2

Id	
Question	Firewall may be described as specified form of
A	Router
B	Bridge
C	Operating system
D	Architecture
Marks	1.5
Unit	2

Id	
Question	Vigenere cipher is an example of
A	Polyalphabetic cipher
B	Caesar cipher
C	Mono alphabetic cipher
D	Product cipher
Marks	1.5
Unit	2

Id	
Question	No. of keys used in Asymmetric key Cryptography is
A	10
B	2
C	4
D	1
Marks	1.5
Unit	2

Id	
Question	The secure socket layer provides
A	Encryption of messages sent by both client and server
B	Server authentication
C	Optional client authentication
D	All of these.
Marks	1.5
Unit	2

Id	
Question	To verify a digital signature we need the
A	Sender’s Private key
B	Sender’s Public key
C	Receiver’s Private key
D	Receiver’s Public key
Marks	1.5
Unit	2