University of Mumbai

Program: BE Information Technology

Curriculum Scheme: Revised 2016

Examination: Third Year Semester V

Course Code: ITC504 and Course Name: Cryptography & Network Security

Time: 1hour Max. Marks: 50

==========

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

Q1.	In cryptography, the order of the letters in a message is rearranged by _____cipher.
Option A:	Monoalphabetic
Option B:	Substitutional
Option C:	Polyalphabetic
Option D:	Transpositional
Q2.	A(n) _____ is a trusted third party that assigns a symmetric key to two parties.
Option A:	KDC
Option B:	CA
Option C:	KDD
Option D:	CCA
Q3.	A packet filter firewall operates at
Option A:	Network Layer
Option B:	Transport Layer
Option C:	Application Layer
Option D:	Session Layer
Q4.	How many subkeys are generated for AES-192?
Option A:	44
Option B:	60
Option C:	52
Option D:	36
Q5.	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:	KDD

Q6.	_____ Cryptography deals with traditional characters, i.e., letters & digits directly.
Option A:	Modern
Option B:	Classic
Option C:	Asymmetric
Option D:	Latest
Q7.	A system that lures an attacker into an environment that can be both controlled and monitored is called
Option A:	Packet filter Firewall
Option B:	Honeypot
Option C:	Intrusion Detection System
Option D:	Application proxy firewall
Q8.	Identify the Kerberos component which is encrypted and used for passing between systems as a mode of authentication.
Option A:	Ticket
Option B:	Client
Option C:	Server
Option D:	Network
Q9.	The principal of _____ ensures that only the sender and the intended recipients have access to the contents of message
Option A:	Confidentiality
Option B:	Authentication
Option C:	Integrity
Option D:	Access control
Q10.	How many S-boxes are used in simple DES algorithm and how many entries are available in each S-Box?
Option A:	8,64
Option B:	8,256
Option C:	8,256
Option D:	8,196
Q11.	The responsibility of certification authority for digital signature is to authenticate the
Option A:	Hash functions used.
Option B:	Private keys of subscribers.
Option C:	Public keys of subscribers.
Option D:	Keys used in DES
Q12.	The KDC functions as an
Option A:	Authentication server

Option B:	Trusted third party
Option C:	Certification authority
Option D:	Timestamp authority
Q13.	In which authentication, the claimant proves that she knows a secret without actually sending it.
Option A:	Password based
Option B:	Token based
Option C:	Challenge-response
Option D:	Biometric
Q14.	Which is the characteristics of anomaly based IDS?
Option A:	It doesn't detect novel attacks
Option B:	It models the normal usage of network as a noise characterization
Option C:	It detects based on signature
Option D:	It does not give false alarms to administrator.
Q15.	15 parties want to exchange messages securely using some symmetric key encryption technique like AES. The number of distinct key values required will be _____
Option A:	102
Option B:	105
Option C:	115
Option D:	92
Q16.	Which of the following can prevent ACK scan attack
Option A:	Packet filter firewall
Option B:	Stateful Packet filter firewall
Option C:	Application Proxy firewall
Option D:	Intrusion Detection System
Q17.	A _____ signature is included in the document; a _____ signature is a separate entity.
Option A:	Secret ,digital
Option B:	Digital, secret
Option C:	Conventional, digital
Option D:	Digital,Conventional
Q18.	Which of the following protocols use Transport and Tunnel modes of operations?
Option A:	PGP
Option B:	SSL
Option C:	IPsec
Option D:	SMIME

Q19.	The data represented in 4×4 byte matrices in the AES algorithm are called
Option A:	State
Option B:	Words
Option C:	Permutations
Option D:	Transitions
Q20.	Which functional area of following is not governed by IPsec protocol?
Option A:	Authentication
Option B:	Confidentiality
Option C:	Key management
Option D:	Availability
Q21.	Which Algorithm is used for encryption in S/MIME?
Option A:	DES
Option B:	RSA
Option C:	Diffie–Hellman
Option D:	AES
Q22.	What is a Security Parameter Index?
Option A:	Unique number given to each IP packet
Option B:	Unique number given to security association
Option C:	Unique number given to cipher text
Option D:	Unique number given to server
Q23.	In knapsack cryptosystem, Super increasing knapsack: (3, 5, 15, 25, 54, 110, 225) n=439 m=10 Private key for the same is ----------
Option A:	(3, 5, 15, 25, 54, 110, 225) and 44
Option B:	(3, 5, 15, 25, 54, 110, 225) and 46
Option C:	(50,150,250,101,222,55) and 33
Option D:	(50,150,250,101,222,55) and 44
Q24.	In a RSA cryptosystem a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of A is 17 Then the private key of A is _____.
Option A:	23
Option B:	113
Option C:	45
Option D:	103
Q25.	What is the Needham-Schroeder Protocol?

Option A:	It is a third-party key distribution protocol
Option B:	It is a direct key-exchange protocol
Option C:	It is an identity confirmation protocol
Option D:	It is a protocol for exchanging public keys