Question 1

One of the major roles of public-key encryption is to address the problem of key distribution. ?

True

False

Question 2

If an opponent captures an unexpired service granting ticket and tries to use it they will be denied access to the corresponding service. ?

True

False

Question 3

___ are entities that obtain and employ data maintained and provided by identity and attribute providers, which are often used to support authorization decisions and to collect audit information.

Federations

Principals

CAs

Data Consumers

Question 4

Federated identity management is a concept dealing with the use of a common identity management scheme across multiple enterprises and numerous applications and supporting many thousands, even millions, of users. ?

True

False

Question 5

It is not necessary for a certification authority to maintain a list of certificates issued by that CA that were not expired but were revoked. ?

True

False

Question 6

Kerberos version 4 did not fully address the need to be of general purpose. ?

True

False

Question 7

The ___ extension lists policies that the certificate is recognized as supporting, together with optional qualifier information.

policy mappings

directory attribute

certificate policies

authority key identifier

Question 8

For symmetric encryption to work the two parties to an exchange must share the same key, and that key must be protected from access by others.

True

False

Question 9

The ____ knows the passwords of all users and stores these in a centralized database and also shares a unique secret key with each server.

authentication server

key distribution server

management server ?

ticket server

Question 10

The ticket-granting ticket is encrypted with a secret key known only to the authentication server and the ticket granting server. ?

True

False

Question 11

____ is a centralized, automated approach to provide enterprise wide access to resources by employees and other authorized individuals, with a focus of defining an identity for each user, associating attributes with the identity, and enforcing a means by which a user can verify identity.

Registration authority

Federated managing authority

Identity management

PKIX management

Question 12

It is not required for two parties to share a secret key in order to communicate securely with conventional encryption. ?

True

False

Question 13

In order to solve the problem of minimizing the number of times that a user has to enter a password and the problem of a plaintext transmission of the password a ____ server is used.

ticket granting

password ciphering

access code

authentication

Question 14

A _____ is a service or user that is known to the Kerberos system and is identified by its principal name.

Kerberos key

Kerberos ticket

Kerberos principal

Kerberos realm

Question 15

An ____ manages the creation and maintenance of attributes such as passwords and biometric information. ?

attribute service

authenticator

identity provider

authorizing agent

Question 16

User certificates generated by a CA need special efforts made by the directory to protect them from being forged. ?

True

False

Question 17

Message encryption alone provides a secure form of authentication.

True

False

Question 18

Public key algorithms are useful in the exchange of conventional encryption keys.

True

False

Question 19

When using encryption for the purposes of non reputation it always provides protection of confidentiality.

True

False

Question 20

The two important aspects of encryption are to verify that the contents of the message have not been altered and that the source is authentic.

True

False

Question 21

Public key cryptography is ____ . ?

bit patterned

one key

symmetric

asymmetric

Question 22

Cryptographic hash functions generally execute slower in software than conventional encryption algorithms such as DES. ?

True

False

Question 23

In the ECB mode of encryption if an attacker reorders the blocks of ciphertext then each block will still decrypt successfully, however, the reordering may alter the meaning of the overall data sequence.

True

False

Question 24

The private key is known only to its owner.

True

False

Question 25

The most important hash function is ____ .

MAC

SHA

OWH

ECB

Question 26

Based on the use of a mathematical construct known as the elliptic curve and offering equal security for a far smaller bit size, ____ has begun to challenge RSA.

DSS

TCB

RIPE-160

ECC

Question 27

The key exchange protocol is vulnerable to a man-in-the-middle attack because it does not authenticate the participants.

True

False

Question 28

The readable message or data that is fed into the algorithm as input is the ____ . ?

ciphertext

plaintext

encryption algorithm

private key

Question 29

Because of the mathematical properties of the message authentication code function it is less vulnerable to being broken than encryption.

True

False

Question 30

The purpose of a _____ is to produce a "fingerprint" of a file, message, or other block of data.

hash function

public key

message authentication

cipher encryption

Question 31

The security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo a prime, it is very easy to calculate discrete logarithms.

True

False

Question 32

____ is a procedure that allows communicating parties to verify that received messages are authentic. ?

ECB

Message authentication

Passive attack

Encryption

Question 33

Data origin authentication provides protection against the duplication or modification of data units. ?

True

False

Question 34

Information access threats exploit service flaws in computers to inhibit use by legitimate users. ?

True

False

Question 35

The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity is ___ .

accountability

authenticity

privacy

integrity

Question 36

____ attacks attempt to alter system resources or affect their operation.

Active

Release of message content

Passive

Traffic analysis

Question 37

There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.

True

False

Question 38

___ is a variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Data integrity

Authentication exchange

Trusted functionality

Event detection

Question 39

___ is a professional membership society with worldwide organizational and individual membership that provides leadership in addressing issues that confront the future of the Internet and is the organization home for the groups responsible for Internet infrastructure standards, including the IETF and the IAB.

ITU-T

ISO

FIPS

ISOC

Question 40

A ____ takes place when one entity pretends to be a different entity.

passive attack

masquerade

modification of message

replay

Question 41

Pervasive security mechanisms are not specific to any particular OSI security service or protocol layer. ?

True

False

Question 42

___ is the insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Notarization

Authentication exchange

Routing control

Traffic padding

Question 43

. There are clear boundaries between network security and internet security. ?

True

False

Question 44

The CIA triad embodies the fundamental security objectives for both data and for information and computing services.

True

False

Question 45

Triple DES was first standardized for use in financial applications in ANSI standard X9.17 in 1985.

True

False

Question 46

The ciphertext-only attack is the easiest to defend against because the opponent has the least amount of information to work with.

True

False

Question 47

If both sender and receiver use the same key the system is referred to as ___ encryption.

asymmetric

two-key

symmetric

public-key

Question 48

Random numbers play an important role in the use of encryption for various network security applications.

True

False

Question 49

The most common key length in modern algorithms is ____ .

64 bits

128 bits

32 bits

256 bits

Question 50

The Feistel structure is a particular example of the more general structure used by all symmetric block ciphers.

True

False

Question 51

A ____ processes the input elements continuously, producing output one element at a time, as it goes along.

block sipher

cryptanalysis

keystream

stream cipher

Question 52

The ___ algorithm performs various substitutions and transformations on the plaintext.

keystream

cipher

encryption

codebook

Question 53

___ is the original message or data that is fed into the algorithm as input.

DES

Plaintext

Encryption key

Ciphertext

Question 54

The essence of a symmetric block cipher is that a single round offers inadequate security but that multiple rounds offer increasing security.

True

False

Question 55

If the sender and receiver each use a different key the system is referred to as ____ encryption.

secret-key

conventional

single-key

asymmetric

Question 56

One desirable property of a stream cipher is that the ciphertext be longer in length than the plaintext.

True

False

Question 57

The ___ key size is used with the Data Encryption Standard algorithm.

128 bits

168 bit

56 bit

32 bits

Question 58

A symmetric block cipher processes ___ of data at a time.

two blocks

one block

four blocks

three blocks

Question 59

A ___ approach involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.

triple DES

brute-force

block cipher

computational

Question 60

Ciphertext is the scrambled message produced as output.

True

False

END of Test 01

Question 1

___ attacks include impersonating another user, altering messages in transit between client and server and altering information on a Web site.

Active

Passive

Shell

Psuedo

Question 2

With each element of the list defining both a key exchange algorithm and a CipherSpec, the list that contains the combination of cryptographic algorithms supported by the client in decreasing order of preference is the ____ .

CipherSuite

Random

Session ID

Version

Question 3

An SSL session is an association between a client and a server and is created by the _____ .

Handshake Protocol

user

Spec Protocol

Administrator

Question 4

The ___ is used to convey SSL-related alerts to the peer entity.

Change Cipher Spec Protocol

Alert Protocol

SSL Record Protocol

Handshake Protocol

Question 5

Defined as a Proposed Internet Standard in RFC 2246, ___ is an IETF standardization initiative whose goal is to produce an Internet standard version of SSL.

SSH

CCSP

TLS

SHA-1

Question 6

The shared master secret is a one-time 48-byte value generated for a session by means of secure key exchange.

True

False

Question 7

The World Wide Web is fundamentally a client/server application running over the Internet and TCP/IP intranets.

True

False

Question 8

The final message in phase 2, and one that is always required, is the _____ message, which is sent by the server to indicate the end of the server hello and associated messages.

server_done

no_certificate

goodbye

finished

Question 9

Microsoft Explorer originated SSL.

True

False

Question 10

The certificate message is required for any agreed on key xchange method except fixed Diffie-Hellman. ?

True

False

Question 11

An arbitrary byte sequence chosen by the server to identify an active or resumable session state is a ___

peer certificate

session identifier

compression

cipher spec

Question 12

Phase ___ of the Handshake Protocol establishes security capabilities.

4

1

2

3

Question 13

The symmetric encryption key for data encrypted by the client and decrypted by the server is a ___ .

server write key

client write key

sequence key

sequence key

Question 14

One way to classify Web security threats is in terms of the location of the threat: Web server, Web browser, and network traffic between browser and server.

True

False

Question 15

The SSL Record Protocol is used before any application data is transmitted.

True

False

Question 16

A Pseudorandom Function takes as input:

a secret value

an identifying label

a seed value

all of the above

Question 17

___ provides secure, remote logon and other secure client/server facilities.

SLP

HTTPS

TLS

SSH

Question 18

The The SSL Internet standard version is called ___ .

SSH

HTTP

SLP

TLS

Question 19

The ____ approach is vulnerable to man-in-the-middle attacks.

Anonymous Diffie-Hellman

Fixed Diffie-Hellman

Fortezza

Ephemeral Diffie-Hellman

Question 20

The most complex part of SSL is the ____ . ?

SSL Record Protocol

Handshake Protocol

Change Cipher Spec Protocol

Alert Protocol

Question 21

The TLS Record Format is the same as that of the SSL Record Format.

True

False

Question 22

Server authentication occurs at the transport layer, based on the server possessing a public/private key pair.

True

False

Question 23

Sessions are used to avoid the expensive negotiation of new security parameters for each connection that shares security parameters.

True

False

Question 24

ISSI/TLS includes protocol mechanisms to enable two TCP users to determine the security mechanisms and services they will use.

True

False

Question 25

The encryption of the compressed message plus the MAC must increase the content length by more than 1024 bytes.

True

False

Question 26

Unlike traditional publishing environments, the Internet is three-way and vulnerable to attacks on the Web servers.

True

False

Question 27

The Change Cipher Spec Protocol is one of the three SSL-specific protocols that use the SSL Record Protocol.

True

False

Question 28

Phase 3 completes the setting up of a secure connection of the Handshake Protocol.

True

False

Question 29

?___ is organized as three protocols that typically run on top of TCP for secure network communications and are designed to be relatively simple and inexpensive to implement.

SSL

SSH

TLS

SSI

Question 30

The first element of the CipherSuite parameter is the key exchange method.

True

False

Question 31

The key legitimacy field is derived from the collection of signature trust fields in the entry.

True

False

Question 32

For the ____ subtype the order of the parts is not significant.

multipart/mixed

multipart/digest

multipart/alternative

multipart/parallel

Question 33

To enhance security an encrypted message is not accompanied by an encrypted form of the session key that was used for message encryption.

True

False

Question 34

As a default, PGP compresses the message after applying the signature but before encryption.

True

False

Question 35

Key IDs are critical to the operation of PGP and ____ key IDs are included in any PGP message that provides both confidentiality and authentication.

two

four

six

three

Question 36

Native form is a format, appropriate to the content type, that is standardized for use between systems.

True

False

Question 37

The ___ accepts the message submitted by a Message User Agent and enforces the policies of the hosting domain and the requirements of Internet standards.

Message Store

Mail Submission Agent

Message Transfer Agent

Mail Delivery Agent

Question 38

For the text type of body no special software is required to get the full meaning of the text aside from support of the indicated character set.

True

False

Question 39

PGP provides confidentiality through the use of asymmetric block encryption.

True

False

Question 40

The ____ subtype is used when the different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.

multipart/digest

multipart/parallel

multipart/mixed

multipart/alternative

Question 41

MIME is an extension to the ____ framework that is intended to address some of the problems and limitations of the use of SMTP.

RFC 821

RFC 5322

RFC 3852

RFC 4871

Question 42

The ____ MIME field is a text description of the object with the body which is useful when the object is not readable as in the case of audio data.

Content-Type

Content-Description

Content-ID

Content-Transfer-Encoding

Question 43

E-mail is the most common distributed application that is widely used across all architectures and vendor platforms.

True

False

Question 44

E-banking, personal banking, e-commerce server, software validation and membership-based online services all fall into the VeriSign Digital ID ___

Class 4

Class 3

Class 1

Class 2

Question 45

____ is an Internet standard approach to e-mail security that incorporates the same functionality as PGP.

Question options:

S/MIME

MIME

DKIM

HTTPS

Question 46

PGP incorporates tools for developing public-key certificate management and a public-key trust model.

True

False

Question 47

A means of generating predictable PGP session keys is needed.

True

False

Question 48

The MIME-Version field must have the parameter value 1.0 in order for the message to conform to RFCs 2045 and 2046.

True

False

Question 49

A message component includes the actual data to be stored or transmitted as well as a filename and a timestamp that specifies the time of creation.

True

False

Question 50

Typically housed in the user's computer, a ___ is referred to as a client e-mail program or a local network e-mail server.

Mail Submission Agent

Message Transfer Agent

Message Store

Message User Agent

Question 51

The ____ field is used to identify MIME entities uniquely in multiple contexts.

Content-Transfer- Encoding

Content-ID

Content-Description

Content-Type

Question 52

PGP has a very rigid public-key management scheme.

True

False

Question 53

Each PGP entity must maintain a file of its own public/private key pairs as well as a file of private keys of correspondents.

True

False

Question 54

Only single user IDs may be associated with a single public key on the public-key ring.

True

False

Question 55

Video content will be identified as ___ type.

GIF

MPEG

BMP

JPEG

Question 56

PGP provides e-mail compatibility using the ____ encoding scheme.

radix-64

MIME

digital signature

symmetric block

Question 57

PGP provides authentication through the use of ___ .

asymmetric block encryption

symmetric block encryption

radix-64

digital signatures

Question 58

The objective of MIME Transfer Encodings is to provide reliable delivery across the largest range of environments.

True

False

Question 59

The ____ enables the recipient to determine if the correct public key was used to decrypt the message digest for authentication.

key ID of the sender's public key

timestamp

filename

leading two octets of message digest

Question 60

S/MIME cryptographic algorithms use ____ to specify requirement level.

CAN and MUST

SHOULD and CAN

SHOULD and MIGHT

SHOULD and MUST

Question 61

The ____ is the information that is delivered as a unit between MAC users.

MSDU

DS

MPDU

BSS

Question 62

IEEE 802.11 defines seven services that need to be provided by the wireless LAN to achieve functionality equivalent to that which is inherent to wired LANs.

True

False

Question 63

The layer of the IEEE 802 reference model that includes such functions as encoding/decoding of signals and bit transmission/reception is the ___ .

physical layer

control layer

logical link layer

media access layer

Question 64

IEEE 802.11 is a standard for wireless LANs.

True

False

Question 65

Wireless networks, and the wireless devices that use them, introduce a host of security problems over and above those found in wired networks.

True

False

Question 66

The ____ layer keeps track of which frames have been successfully received and retransmits unsuccessful frames.

transmission

media access control

logical link control

physical layer

Question 67

The use of encryption and authentication protocols is the standard method of countering attempts to alter or insert transmissions.

True

False

Question 68

The purpose of the discovery phase in the _____ is for a STA and an AP to recognize each other, agree on a set of security capabilities, and establish an association for future communication using those security capabilities.

WPA

RSN

TKIP

WAE

Question 69

The term used for certified 802.11b products is _____ .

WAP

Wi-Fi

WEP

WPA

Question 70

The first 802.11 standard to gain broad industry acceptance was ___.

802.11i

802.11a

802.11g

802.11b

Question 71

The actual method of key generation depends on the details of the authentication protocol used.

True

False

Question 72

____ can occur when a company's wireless LAN or wireless access points to wired LANs in close proximity and may create overlapping transmission ranges. A user intending to connect to one LAN may unintentionally lock on to a wireless access point from a neighboring network.

Network injection

Denial of service attacks

Man-in-the-middle attacks

Accidental association

Question 73

The DS can be a switch, a wired network, or a wireless network.

True

False

Question 74

The ___ is used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake.

MIC key

EAPOL-KEK

EAPOL-KCK

TK

Question 75

The use of 802.1X cannot prevent rogue access points and other unauthorized devices from becoming insecure backdoors.

True

False

Question 76

The specification of a protocol along with the chosen key length is known as a ____ .

extended service

distribution system

cipher suite

RSN

Question 77

A ____ is any device that contains an IEEE 802.11 conformant MAC and physical layer.

station

MPU

service data unit

MSDU

Question 78

_____ and links, such as personal network Bluetooth devices, barcode readers, and handheld PDAs, pose a security risk in terms of both eavesdropping and spoofing.

DoS

Accidental association

Nontraditional networks

Ad hoc networks

Question 79

You should allow only specific computers to access your wireless network.

True

False

Question 80

The function of the ____ is to on transmission assemble data into a frame, on reception disassemble frame and perform address recognition and error detection, and govern access to the LAN transmission medium.

transmission layer

logical layer

media access control layer

physical layer

Question 81

The pairwise master key is derived from the group key.

True

False

Question 82

The PMK is used to generate the ___ which consists of three keys to be used for communication between a STA and AP after they have been mutually authenticated.

AAA Key

GTK

PTK

PSK

Question 83

Sensors and robots, are not vulnerable to physical attacks.

True

False

Question 84

Security policies for mobile devices should assume that any mobile device will not be stolen or accessed by a malicious party.

True

False

Question 85

The principal threats to wireless transmission are eavesdropping, altering or inserting messages, and disruption.

True

False

Question 86

Handheld PDAs pose a security risk in terms of both eavesdropping and spoofing.

True

False

Question 87

The integration service enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN.

True

False

Question 88

The master session key is also known as the ____ key.

AAA

GTK

MIC

STA

Question 89

In a(n) ____ situation, a wireless device is configured to appear to be a legitimate access point, enabling the operator to steal passwords from legitimate users and then penetrate a wired network through a legitimate wireless access point.

malicious association

identiy theft

network injection

ad hoc network

Question 90

MAC spoofing occurs when an attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network privileges.

True

False

Question 91

___ enables customers to combine basic computing services, such as number crunching and data storage, to build highly adaptable computer systems.

IaaS

EAP peer

CP

SaaS

Question 92

For many clients, the most devastating impact from a security breach is the loss or leakage of data.

True

False

Question 93

With a ___ infrastructure, the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns.

community cloud

public cloud

private cloud

hybrid cloud

Question 94

___ saves the complexity of software installation, maintenance, upgrades, and patches.

IaaS

SaaS

EAP

DHCP

Question 95

___ is a client computer that is attempting to access a network.

EAP peer

PSK

NAC

RAS

Question 96

Data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

True

False

Question 97

Cloud computing gives you the ability to expand and reduce resources according to your specific service requirement.

True

False

Question 98

The ___ is the node that is attempting to access the network and may be any device that is managed by the network access control system.

AR

RAS

IP

PS

Question 99

The threat of data compromise decreases in the cloud.

True

False

Question 100

The ____ is an Internet protocol that enables dynamic allocation of IP addresses to hosts.

VLAN

IEEE 802.1X

EAPS

DHCP

Question 101

The Extensible Authentication Protocol supports multiple authentication methods.

True

False

Question 102

Broad network access, measured service, resource pooling, and rapid elasticity are essential characteristics of _____.

PaaS

network access control

cloud computing

EAP-TLS

Question 103

_____ is an umbrella term for managing access to a network.

NAS

ARC

NAC

RAS

Question 104

The ____ determines what access should be granted.

authentication server

policy server

supplicant

access requestor

Question 105

Access requestors are also referred to as clients.

True

False

Question 106

In using cloud infrastructures, the client necessarily cedes control to the CP on a number of issues that may affect security.

True

False

Question 107

The NIST cloud computing reference architecture focuses on the requirements of what cloud services provide, not a how to design solution and implementation.

True

False

Question 108

The cloud provider in a private cloud infrastructure is responsible for both the infrastructure and the control.

True

False

Question 109

___ is the provision of security applications and services via the cloud either to cloud-based infrastructure and software or from the cloud to the customers' on-premise systems.

IaaS

PaaS

SaaS

SecaaS

Question 110

A cloud broker is useful when cloud services are too complex for a cloud consumer to easily manage.

True

False

Question 111

EAPOL operates at the network layers and makes use of an IEEE 802 LAN, such as Ethernet or Wi-Fi, at the link level.

True

False

Question 112

There is a decreasing trend in organizations to move information technology operations to a cloud computing infrastructure.

True

False

Question 113

A network access server does not include its own authentication services.

True

False

Question 114

A ___ is a person or organization that maintains a business relationship with, and uses service from, cloud providers.

cloud auditor

cloud broker

cloud carrier

cloud consumer

Question 115

Network access control authenticates users logging into the network and determines what data they can access and actions they can perform.

True

False

Question 116

A ____ is a party that can conduct independent assessment of cloud service, information system operations, performance, and security of the cloud implementation.

cloud auditor

cloud carrier

cloud broker

all of the above

Question 117

With a ___ infrastructure, the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

hybrid cloud

private cloud

public cloud

hybrid cloud

Question 118

VLANs are common NAC enforcement methods.

True

False

Question 119

A ____ is a person, organization, or entity responsible for making a service available to interested parties.

cloud broker

cloud auditor

cloud provider

cloud carrier

Question 120

In effect, ____ is an operating system in the cloud.

IEEE 802.1X

PaaS

IaaS

DHCP