Final Examination - 1st Sem 2022-2023

Due No due date **Points** 157 **Questions** 82
Available after Dec 12 at 3pm **Time Limit** 90 Minutes

Instructions

usc logo.jpg

DCISM_logo.png

University of San Carlos

Department of Computer and Information Sciences and Mathematics

Final Examination

ANY FORM OF COMPUTING DEVICE IS NOT ALLOWED DURING THE EXAMINATIONS!

OPENING OF BROWSER OR TABS OTHER THAN CANVAS IS STRICTLY PROHIBITED AND IS CONSIDERED CHEATING!!

CIS 3106 Information Assurance and Security

Answer the given Exam according to what is needed, this exam is composed of multiple-choice with multiple answers, fill in the blanks and Essay question. Take note that the exam is time-limited so make the most of your time, you cannot return to the previous questions, therefore make sure of your answers. If you cannot submit the quiz on time, the system will automatically submit your scores. Good luck!!! Always follow instructions!!!

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	75 minutes	121.95 out of 157

ⓘ Correct answers are hidden.

Score for this quiz: **121.95** out of 157
Submitted Dec 12 at 4:15pm
This attempt took 75 minutes.

Question 1

1 / 1 pts

Match Column A with Column B to identify the common threats to physical facility and its counter measures.

Natural Threats including weather and geographical problems	Develop Business contir
Power interruptions	Develop disaster recove
Theft	Implement asset tagging
Lack of Surveillance	Test building security usi
Social Engineering	Conduct security trainінг

Question 2

1 / 1 pts

What are the two pre-historic computers used by military in Information Assurance?

☑ Bombe

☑ ENIAC

☐ Analytical Engine

☐ UNIVAC

☐ EDSAC

Question 3

1 / 1 pts

Type of encryption processing that processes the input in a block of elements at a time (typically 64-bits)?

○ symmetric cipher

○ asymmetric cipher

● block cipher

○ stream cipher

Incorrect

Question 4

0 / 1 pts

The_____________________ is one or more locations containing the tools that provide administrators with a detailed status of the organization’s network.

answer in lowercase only, no shortcuts, no abbreviation, no acronyms operation centers

Question 5

1 / 1 pts

It is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort rather than employing intellectual strategies.

answer in lowercase only

brute force

Question 6

1 / 1 pts

The oldest and most used cryptographic ciphers, the key that deciphers the ciphertext is the same key that enciphers the plaint text, this key is often referred to as the secret key.

○ asymmetric cipher

● symmetric cipher

○ block cipher

○ stream cipher

Question 7

1 / 1 pts

These devices form the backbone of the Internet and communications between different networks, communicate with one another to identify the best possible path to deliver traffic to different networks

○ wireless access points

● router

○ wireless routers

○ firewall

○ switch

Question 8

1 / 1 pts

These are tools to intercept and log network traffic, shows the values of various fields in the packet, and analyzes its content, it can capture network traffic on both wired and wireless networks.

____

answer in lowercase only, no shortcuts, no abbreviation, no acronyms

packet analyzers

Incorrect

Question 9

0 / 1 pts

What type of state that joins the political entity of a state to the cultural entity of a nation, from which it aims to derive its political legitimacy to rule and potentially its status as a sovereign state?

● Political State

○ Academic State

○ None of the above

○ Nation State

Question 10

1 / 1 pts

It is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document.

○ Digital Certificate

○ Hashing

● Digital Signature

○ Cryptography

Incorrect

Question 11

0 / 1 pts

Process of translating the ciphertext into data.

Answer in lowercase only. No shortcuts, No abbreviation, No acronyms.

deciphering

Question 12

1 / 1 pts

It is an art and science of transforming messages so as to make them secure and immune to attacks.

Answer in lowercase only. No shortcuts, No abbreviation, No acronyms

cryptography

Incorrect

Question 13

0 / 1 pts

Type of cryptography also known as public-key cryptography. It uses public and private keys to encrypt and decrypt data.

Answer in lowercase only. No shortcuts, No abbreviation, No acronyms.

digital certificate

Question 14

1 / 1 pts

What type of encryption that the sender and receiver use different keys (aka two-key, and public-key)?

answer in lowercase only.

asymmetric

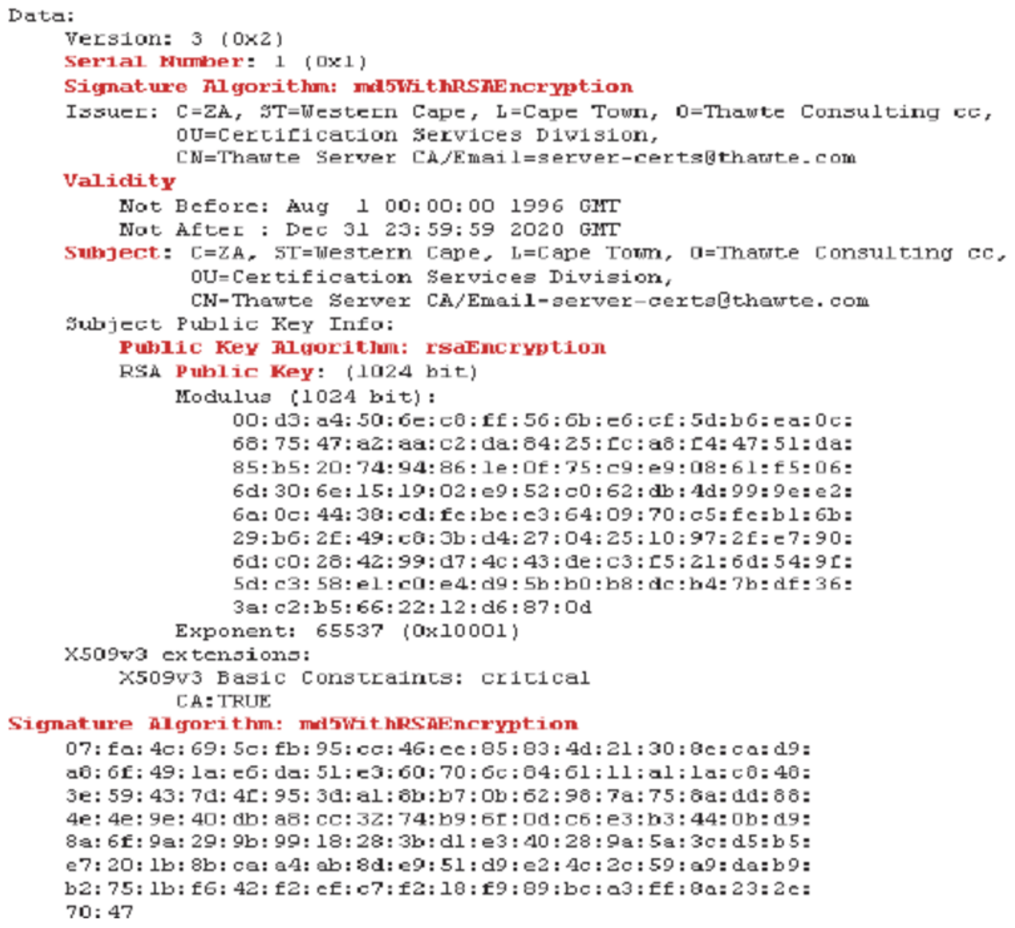
Incorrect

Question 15

0 / 1 pts

Basin on the figure below, this is an example of a ________________?

Answer in lowercase only. No shortcuts, No abbreviation, No acronyms.



```
Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
            OU=Certification Services Division,
            CN=Thawte Server CA/Email=server-certs@thawte.com
    Validity
        Not Before: Aug  1 00:00:00 1996 GMT
        Not After : Dec 31 23:59:59 2020 GMT
    Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
             OU=Certification Services Division,
             CN=Thawte Server CA/Email=server-certs@thawte.com
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                3a:c2:b5:66:22:12:d6:87:0d
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints: critical
            CA:TRUE
Signature Algorithm: md5WithRSAEncryption
    07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
    a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
    3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
    4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
    8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
    e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
    b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
    70:47
```

digital signature

Incorrect

Question 16

0 / 1 pts

What level of focus does information assurance covers information and data manipulation ability maintained in cyberspace, including: data structures, processes and programs, protocols, data content and databases.

Write your answer in lowercase only.

infrastructure

Question 17

1 / 1 pts

These are entities that participate or act in international relations.

- □ Neutral State Actions
- ☑ Non-state actors
- □ Non-state Attributes
- □ Natural Status Alienation

Question 18

1 / 1 pts

It is a pioneering encryption algorithm that helped revolutionize encryption, it is a symmetric type encryption method developed in 1975 and standardized by ANSI in 1981 as ANSI X. It uses 56 bit and 48-bit key and 64-bit block cipher.

- ○ symmetric cipher
- ● data encryption standard
- ○ asymmetric cipher
- ○ advance encryption standard

Question 19

1 / 1 pts

To secure a network, What should an administrator used to provide a way to group devices within a network and on individual switches which use logical connections instead of physical connections.

____

answer in lowercase only, no shortcuts, no abbreviation, no acronyms

virtual local area network

Question 20

1 / 1 pts

What are three different analytic frameworks have been proposed, various international conventions allow a self-defense or “anticipatory self-defense” response to an armed attack. and qualify a cyber attack “equivalent” to an armed attack.

instrument-based ________________________________

effects-based ________________________________

strict liability ________________________________

Answer 1:

Instrument-based

Answer 2:

Effects-based

Answer 3:

Strict liability

Question 21

1 / 1 pts

What category of security solution/policy is phrased in terms of entities (users, processes, etc.) that execute activities and request access to objects.

Write your answer in lowercase only.

● subjects

Question 22

1 / 1 pts

It is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.

○ virus

● worm

○ malware

○ trojan

Question 23

1 / 1 pts

These are raw facts with unknown coding scheme?

- ● noise
- ○ data
- ○ interference
- ○ information
- ○ knowledge

Question 24

1 / 1 pts

What type of encryption that the sender and receiver use different keys (aka two-key, and public-key)?

Answer in lowercase only. No shortcuts, No abbreviation, No acronyms

asymmetric

Question 25

1 / 1 pts

It is the assurance that someone cannot deny the validity of something. It is also a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.

- ● non-repudiation

○ integrity

○ authenticity

○ hashing

Question 26

1 / 1 pts

It is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. Its purpose is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking, and confidential email.

● public key infrastructure

○ private key infrastructure

○ digital certificate

○ digital signature

Question 27

1 / 1 pts

How do you know you have a digital certificate?

Answer in lowercase only.

https

Question 28

1 / 1 pts

What category of security solution/policy is phrased in terms of operations, primitive or complex, that can operate on objects and must be controlled.

Write your answer in lowercase only.

● actions

Question 29

1 / 1 pts

Which of the following statement best describe Hackers?

□ usually politically motivated and may seek to cause maximal damage to information infrastructure as well as endanger lives and property.

☑ one who gains unauthorized access to or breaks into information systems for thrills, challenge, power, or profit.

□ target information that may be of value to them: bank accounts, credit card information, intellectual property, etc.

□ seek the military, diplomatic, and economic secrets of foreign governments, foreign corporations, and adversaries. May also target domestic adversaries.

Question 30

1 / 1 pts

What Cybersecurity Information Websites, developed at Carnegie Mellon University helps government and industry organizations to develop, operate, and maintain software systems that are innovative, affordable, and trustworthy.

● CERT

○ NVD

○ ACSC

○ SEI

Question 31

1 / 1 pts

This is a digitally signed Certificate which is built of complex hashing functions and algorithm that keeps user’s information encrypted during the data transmission from Client to Server and server to client.

○ Digital Certificate

● SSL Certificate

○ Organizational Certificate

○ Developers Certificate

Incorrect

Question 32

0 / 1 pts

A _____________ is a type of defense against cyber attack when taking steps to prevent an attack or to mitigate the damage should an attack occur (access control, secure system design, security administration).

virtual private network

Partial

Question 33

0.5 / 1 pts

Using the steps in RSA algorithm, find the possible number for ***e*** or the encryption key.

if p = 2; q = 13

□ 19

□ 9

☑ 13

☑ 7

☑ 5

□ 3

☑ 11

□ 15

Question 34

1 / 1 pts

it is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

answer in lowercase only.

malware

Incorrect

Question 35

0 / 1 pts

What are two types of defenses against cyber attacks?[

virtual private netw

firewall

Answer 1:

virtual private network

Answer 2:

firewall

Question 36

1 / 1 pts

What step in the digital forensic process involves discovering what type of storage media and what data or information could be recovered relative to the investigation or case.

answer in lowercase only

identification

Question 37

1 / 1 pts

It is a mathematical algorithm, produces a unique digital fingerprint of a file and verifies that binary content of an acquired forensic image is exactly the same as the source media

write your answer in lowercase.

hash

Question 38

1 / 1 pts

This is a tool used to protect data stored in the form of files, transforms data using a complicated algorithm to make it unreadable.

____

answer in lowercase only

file encryption

Question 39

1 / 1 pts

These are "individuals or organizations that have economic, political or social power and are able to influence at a national who employ violence in pursuit of their objectives.

☐ Verifiable Armed Sectors

☑ Violent Non State Actors

☐ Vicious Non State Actors

☐ Arrmed Violent Sector

Question 40

1 / 1 pts

What type of encryption that the sender and receiver use the same key (aka single-key, and secret-key)?

Answer in lowercase only. No shortcuts, No abbreviation, No acronyms

symmetric

Question 41

1 / 1 pts

It means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message.

non-repudiation

Question 42

1 / 1 pts

Which of the following is the Principle #3 in Digital Evidence Principles?

○ The person in charge of the case has overall responsibility for ensuring that a computer has been correctly examined in accordance with the law and these principles.

○ In exceptional circumstances it may be necessary to access the original data held on a target computer.

● An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine these processes and achieve the same result.

○ No action taken by the law enforcement agencies or their agents should change the data held on a computer or other media which may subsequently be relied upon in Court.

Question 43

1 / 1 pts

It is the process of attempting to discover the plain text or the key of an encrypted file.

○ acquisition

○ imaging

● cryptanalysis

○ steganography

Question 44

1 / 1 pts

It is any malicious computer program which is used to hack into a computer by misleading users of its true intent, it does not have the ability to replicate itself however, it can lead to viruses being installed on a machine since they allow the computer to be controlled by the its creator.

○ worm replicator

● trojan horse virus

○ worm viruses

○ malware

Question 45

1 / 1 pts

Write blocker is a multi-function tools that assist with hard drive preparation and duplication, forensic imaging, and verification, what type of forensic tools is a write blocker?

● Forensic Imager

○ Forensic Report generator

○ Forensic analyzer

○ Forensic Aquisitioner

Question 46

1 / 1 pts

It is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort rather than employing intellectual strategies.

Answer in lowercase only. No shortcuts, No abbreviation, No acronyms

brute force

Incorrect

Question 47

0 / 1 pts

A malware which is a variety of software components that together provide services to the attackers. Currently this includes information stealing capabilities and in the background, kernel drivers and injection tools. Part of this malware is written in unknown high-level programming language.

○ flamer

● sKyWIper

○ Stuxnet

○ duqu

Question 48

1 / 1 pts

A type of physical bridge which is stand-alone imaging device multifunction tool with dedicated forensic capabilities)

● write blocker

○ Autopsy

○ ProDiscovery

○ AccessData FTK

Question 49

1 / 1 pts

An artifact from windows OS environment contains events logged by Windows system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined by Windows.

☐ security log

☐ application log

☐ set up log

☑ system log

☐ windows log

Question 50

1 / 1 pts

__________________ refers to digital information that may be used as information in a case, an information being subject to human intervention or not, that can be extracted from a computer system that must be in human-readable format or capable of being interpreted by a person with expertise in the subject

answer in lowercase only.

digital evidence

Question 51

1 / 1 pts

A type of encryption where data is encrypted using a key and the decryption is also done using the same key.

● Symmetric Encryption

○ Asymmetric Encryption

○ Shifting

○ Transpositional

Question 52

1 / 1 pts

It is an art and science of transforming messages so as to make them secure and immune to attacks.

answer in lowercase only

cryptography

Question 53

1 / 1 pts

This is a modular computer malware discovered in 2012 that attacks computers running the Microsoft Windows operating system.The program is being used for targeted cyber espionage in Middle Eastern countries.

○ Titan Rain

○ Moonlight Maze

● sKyWIper

○ Stuxnet

Question 54

1 / 1 pts

________ is the scientific tests or techniques used in connection with the detection of crime.

write your answer in lowercase.

forensic

Question 55

1 / 1 pts

A ___________ is a category of entities, or a circumstance, that poses a potential danger to an asset.

Write your answer in lowercase only.

● threat

Question 56

1 / 1 pts

These are whole numbers greater than 1 whose only factors are 1 and itself. A factor is a whole number that can be divided evenly into another number.

Answer in lowercase only. No shortcuts, No abbreviation, No acronyms.

prime number

Question 57

1 / 1 pts

A verifiable duplicate of all the contents of a storage media or selected files in a form of encapsulated file. Acquired by trained digital forensic examiner using validated hardware and software tools

● digital forensic image

○ digital forensic files

○ digital forensic process

○ digital forensic tool

Question 58

1 / 1 pts

Issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender. This is issued by a Certificate Authority (CA) to verify the identity of the certificate holder.

Answer in lowercase only. No shortcuts, No abbreviation, No acronyms.

digital certificate

Question 59

1 / 1 pts

These are security measures to establish the validity of a transmission, message, or originator.

○ No answer text provided.

○ No answer text provided.

○ No answer text provided.

● authentication

Question 60

1 / 1 pts

It is the process of attempting to discover the plain text or the key of an encrypted file.

○ steganography

○ aquisition

● cryptanalysis

○ imaging

Question 61

12 / 12 pts

In order to be issued an SSL Certificate, you need to purchase one from a web service provider and then go through a process that entails the following:

Purchasing SSL	Place an order for an SS
Private Key and CSR Generation	Prior to applying/enrollin
Private Key and CSR Generation	Digital IDs make use of a
Private Key and CSR Generation	The Private Key will rem
Private Key and CSR Generation	hosting server will gener
Enrollment	Generated a minimum o
Enrollment	This process is done fro
Enrollment	The contact details that y
Verification Process & Certificate Issue	After submitting the requ
Verification Process & Certificate Issue	This process is much fas
Verification Process & Certificate Issue	Ffter the CA is satisfied w
Verification Process & Certificate Issue	After you have done the

Partial

Question 62

9 / 15 pts

Decipher the hidden message, using the table below

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	sp

sp - space

Hidden Message:

s	z	!	!	a	m	z	o	o	!	z	sp	u	x	z	$

Determine the encryption and decryption key

if p = 3; q = 11

33 find N = ______________ -

20 find φN = ____________ -

7 find e = ______________ -

3 find d = _____________ -

message secured! what is the encrypted message? ____________ -

write your answer in plaintext and lower case; plain numbers and no commas.

Answer 1:

33

Answer 2:

20

Answer 3:

7

Answer 4:

3

Answer 5:

message secured!

Incorrect

Question 63

0 / 2 pts

What are the 3 Popular Forms of Encryption? answer in lowercase only

advanced encryptic ______________________

digital encryption st ______________________

rivest-shamir-adlem ______________________

Answer 1:

advanced encryption standard

Answer 2:

digital encryption standard

Answer 3:

rivest-shamir-adleman

Question 64

2 / 2 pts

Which of the following are the basic SSL Certificates?

Choose all that applies.

☑ Positive SSL

□ Positive SSL Wildcard

□ SSL 128

□ Wildcard Server

□ SSL 256

☑ SSL123

Partial

Question 65

1.33 / 2 pts

Which of the following are the Common Threats to the LAN?

□ User Level Access

☑ Unauthorized network probing and port scanning

☑ Unauthorized LAN access,

☑ Network operating system software vulnerabilities,

☑ Improper password authentication

□ Frequent patch updates

Question 66

2 / 2 pts

What are the two reasons why Business planning always involves a tradeoff between cost and benefits.

- □ Potential for loss
- ☑ Costs come in various forms.
- □ Business reputation
- ☑ Business is inherently profit-driven.
- □ Legislative and regulatory mandates

Question 67

2 / 2 pts

Match Column A with column B to identify the different protocols use to protect and Managing Remote Access

SSH	is a protocol that provide
TELNET	protocol that uses unsec
SCP	securely transfers compu
VLAN	

Incorrect

Question 68

0 / 2 pts

What are the 3 Popular Forms of Encryption? answer in lowercase only

advanced encryptic ____________________

digital encryption st ____________________

rivest-shamir-adlem ____________________

Answer 1:

advanced encryption standard

Answer 2:

digital encryption standard

Answer 3:

rivest-shamir-adleman

Question 69

2 / 2 pts

What are the three categories of threat? choose all that apply.

☐ by authenticity

☑ by kind of entity involve

☐ by integrity

☑ by intent

□ by threat actor

☑ by impact

Question 70

2 / 2 pts

What are the two basic principles of encryption? answer in lowercase only

substitution ____________________

transposition ____________________

Answer 1:

substitution

Answer 2:

transposition

Question 71

2 / 2 pts

Enumerate the IA four security engineering domains. **write your answer in lowercase only.**

physical security ____________________

personnel security ____________________

IT security ____________________

operational security ______________________________

Answer 1:

physical security

Answer 2:

personnel security

Answer 3:

it security

Answer 4:

operational security

Partial

Question 72

1.33 / 2 pts

What are the four key attack attributes according to experts when determining whether a cyber attack is an act of cyber war?

☐ Proportionality

☑ Motivation

☐ Effects-based

☑ Sophistication

☑ Consequence

☐ Instrument-based

☐ Distinction

☑ Source

☐ Necessity

☐ Strict liability

Partial

Question 73

4 / 5 pts

Find the totient or φN.

[28200] p=283; q=101; ____________________

[6552] p=22; q=313; ____________________

[163048] p=917; q=179; ____________________

[797280] p=907; q=881; ____________________

[212640] p=241; q=887; ____________________

answer in plain number no commas

Answer 1:

28200

Answer 2:

6552

Answer 3:

163048

Answer 4:

797280

Answer 5:

212640

Partial

Question 74

0.63 / 5 pts

Identify the difference between Signed and Self-Signed Certificates by Matching Column A with Column B

Self-signed certificate	Is a security certificate th
Self-signed certificate	Does not allow any auth
Self-signed certificate	Do not provide all of the
Self-signed certificate	are for testing so there is
Signed Certificate	an authorized certificate
Signed Certificate	When client visits site it
Self-signed certificate	Encrypt the data but flun
Signed Certificate	Certificates provide encr

Incorrect

Question 75

0 / 5 pts

Find the N value in the formula c=m^e mod N,

278584 if p = 389; q = 719; N = ____________________

10186 if p = 23; q = 463; N = ____________________

55224 if p = 79; q = 709; N = ____________________

5306 if p = 380; q = 15; N = ____________________

30772 if p = 197; q = 158; N = ____________________

answer in plain numbers, no commas

Answer 1:

278584

Answer 2:

10186

Answer 3:

55224

Answer 4:

5306

Answer 5:

30772

Partial

Question 76

4.38 / 5 pts

Identify the different types of Digital Certificates by Matching Column A with Column B

Server Certificates	Certificates are installed
Server Certificates	Certificates are installed
Personal Certificates	allow one to authenticate
Personal Certificates	These are perfect for bu:
Corporate Certificates	are used by corporate er
Corporate Certificates	Client Certificates or Dig
Developers Certificates	Prove authorship and re
Developers Certificates	Used to sign software or

Partial

Question 77

4.29 / 5 pts

Identify the following prime numbers. choose all that apply.

☑ 347

□ 6

☑ 19

□ 910

☑ 491

□ 720

☑ 421

☑ 491

□ 770

☑ 751

□ 330

Question 78

5 / 5 pts

Identify the Digital certificate and Digital signature by matching Column A and Column B

like a fingerprint or an attachment to a digital document that ensures its authenticity and integrity.	Digital Signature
Hashed value of original message is encrypted with sender’s secret key	Digital Signature

Authenticity of Sender, integrity of the document and non-repudiation.	Digital Signature ⌄
It follows DSS.	Digital Signature ⌄
a file that ensures holder's identity and provides security.	Digital Certificate ⌄
It is generated by CA (Certifying Authority) that involves four steps: Key Generation, Registration, Verification, Creation.	Digital Certificate ⌄
It provides security and authenticity of certificate holder.	Digital Certificate ⌄
It follows X.509 Standard Format	Digital Certificate ⌄

Question 79

5 / 5 pts

Identify the steps followed in creating a digital signature?

Step 1: [Select] ⌄

Step 2: [Select] ⌄

Step 3: Receiver decrypts the digital signature using the public key of sender.(This assures authenticity, as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender's public key).

Step 4: [Select] ⌄

Step 5: [Select] ⌄

Answer 1:

Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).

Answer 2:

Digital signature is then transmitted with the message.(message + digital signature is transmitted)

Answer 3:

Receiver decrypts the digital signature using the public key of sender.(This assures authenticity, as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender’s public key).

Answer 4:

The receiver now has the message digest.

Answer 5:

The receiver can compute the message digest from the message (actual message is sent with the digital signature).

Question 80

5 / 5 pts

Arrange the order on how digital forensic process is observed to extract data or information could be recovered relative to the investigation or case.

identification ________________

acquisition ________________

analysis ________________

reporting ________________

court presentation ________________

answer in lower case only.

Answer 1:

identification

Answer 2:

acquisition

Answer 3:

analysis

Answer 4:

reporting

Answer 5:

court presentation

Partial

Question 81

2.5 / 5 pts

What are the components of an information that makes it more significant compare from other type of data? Choose all that apply.

☑ timely

□ perceptual

□ available

☑ accurate

☑ comprehensive

□ motivated

☑ verifiable

☑ consistent

□ complete

Question 82

5 / 5 pts

Match Column A with Column B identifying the Common Threats to the Private Cloud

Unautorized network probing and port scanning	Disable ping, probing an ⌄
Unauthorized access to resources	Implement intrusion dete ⌄

Router, firewall or network device operating system software vulnerability	Update Devices with sec ⌄
Remote users download sensitive data	Implement data classifica ⌄
Router, firewall or network device configuration error	conduct pen test post co ⌄

Quiz Score: **121.95** out of 157