SF-Quiz #5: Test 1

Due No due date **Points** 45 **Questions** 30
Available after Nov 23 at 3pm **Time Limit** 45 Minutes

Instructions

Answer the quiz according to what is needed, this quiz is composed of multiple choice with multiple answers, fill in the blanks and Essay question. Take note that the quiz 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!!!

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	34 minutes	30.3 out of 45

Correct answers are hidden.

Score for this quiz: **30.3** out of 45
Submitted Nov 23 at 3:35pm
This attempt took 34 minutes.

Question 1

1 / 1 pts

It is an electronic attachment document used for security purposes that is used to identify an individual, a server, a company, or some other entity, and to associate that identity with a public key.

- private key infrastructure
- digital certificate

- digital signature
- public key infrastructure

Question 2

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.

- digital certificate
- digital signature
- public key infrastructure
- private key infrastructure

Question 3

1 / 1 pts

It is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It guarantees that the contents of a message have not been altered in transit.

- advance encryption standard
- data encryption standard
- digital certificate

- digital signature

Question 4

1 / 1 pts

It is a cryptographic algorithm that can be used to protect electronic data, its main strength rests in the option for various key lengths, a 128-bit, 192-bit or 256-bit key, the algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

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

Incorrect

Question 5

0 / 1 pts

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

- asymmetric cipher
- stream cipher
- symmetric cipher
- block cipher

Question 6

1 / 1 pts

It is a pioneering encryption algorithm that helped revolutionize encryption, it is 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.

- (●) data encryption standard
- ( ) symmetric cipher
- ( ) asymmetric cipher
- ( ) advance encryption standard

Question 7

1 / 1 pts

A type of cryptography that uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical. One key in the pair can be shared with everyone; it is called the public key, while the other key serves as the private key used to decipher the encrypted data.

- ( ) symmetric cipher
- ( ) data encryption standard
- (●) asymmetric cipher
- ( ) advance encryption standard

Question 8

1 / 1 pts

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

answer in lowercase only.

prime number

Incorrect

Question 9

0 / 1 pts

It is one of the first public-key cryptosystems and is widely used for secure data transmission, in such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret or private. It is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

- dsa
- aes
- rsa
- des

Question 10

1 / 1 pts

These are number of positive integers that are relatively prime to (or do not contain any factor in common with the given numbers) and where 1 is counted as being relatively prime to all numbers.

totient

Incorrect

Question 11

0 / 1 pts

Write the formula of the euler's function:

totient = ?

answer in lowercase only, no spacing.

(prime1-1)*(prime2-1)

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

cryptography

Question 13

2 / 2 pts

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

substitution _____

transposition _____

Answer 1:

substitution

Answer 2:

transposition

Question 14

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.

symmetric

Question 15

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

Question 16

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
- stream cipher
- block cipher

Question 17

1 / 1 pts

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

- cryptanalysis

- imaging
- aquisition
- steganography

Question 18

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.

- malware
- worm
- trojan
- virus

Question 19

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 viruses
- worm replicator
- trojan horse virus

malware

Question 20

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

Partial

Question 21

2.8 / 4 pts

Identify the following prime numbers. choose all that apply.

- [x] 19
- [x] 491
- [ ] 770
- [ ] 910
- [ ] 720
- [x] 751
- [ ] No answer text provided.

- [ ] 6
- [x] 347
- [x] 421
- [x] 7
- [ ] No answer text provided.
- [ ] 330
- [x] 643

Incorrect

Question 22

0 / 3 pts

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

des _____

rsa _____

aes _____

Answer 1:

des

Answer 2:

rsa

Answer 3:

aes

Question 23

1 / 1 pts

Find the N value in the formula c=m^e mod N, if p = 389; q = 719.

answer in plain numbers, no commas

279691

Partial

Question 24

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 25

1.5 / 2 pts

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

if p = 2; q = 13

- [ ] 13
- [ ] 9
- [x] 11
- [ ] 3
- [ ] 19

- [ ] 15
- [x] 5
- [x] 7

Incorrect

Question 26

0 / 1 pts

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

if p = 2; q = 13; e = 11

- [ ] 41
- [x] 7
- [x] 11
- [ ] 37
- [ ] 23

Question 27

1 / 1 pts

It is widely accepted type of digital certificated by international public key infrastructure standards to verify that a public key belongs to the user, computer or service identity contained with in the certificate.

answer in lowercase only

x.509

Question 28

1 / 1 pts

Is a trusted entity that manages and issues security certificates and public keys that are used for secure communication in a public network. Its job is to issue certificates, to verify the holder of a digital certificate, and to ensure that holders of certificates are who they claim to be.

answer in lowercase only, no abbreviation.

certificate authority

Incorrect

Question 29

0 / 1 pts

Find the co-primes of the result and given numbers, if p = 3 and q = 7

1. what is the phi(N) = [a] _____

5

Partial

Question 30

1 / 5 pts

Find the co-primes of the result and given numbers, if p = 3 and q = 7

1. What are the co-primes?

- [ ] 12
- [ ] 19
- [ ] 20
- [ ] 9
- [ ] 15
- [x] 7
- [x] 17
- [x] 13
- [ ] 6
- [ ] 18
- [ ] 10
- [ ] 3

Quiz Score: **30.3** out of 45