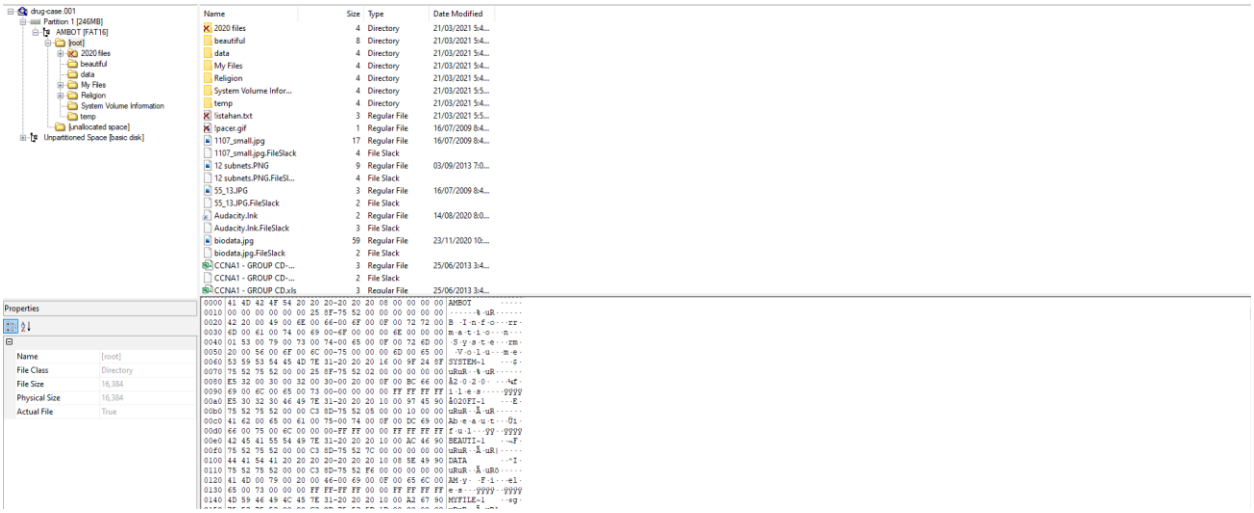
Pedophile Case – James Carl Liboon

Acquired using: ADI3.1.5.0
Case Number: 101024-10
Evidence Number: 101024
Submitted by: Jomar Leaño

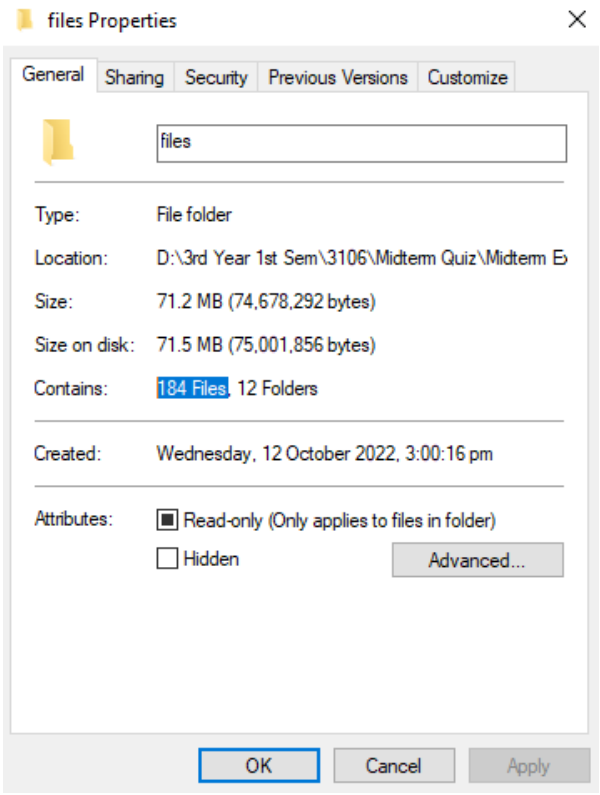


1. Source Drive: **Generic Flash Disk USB Device**
2. The capacity of the source disk in # of bytes: **246 MB**
3. Type of Forensic Tool Used: **AccessData® FTK® Imager 3.1.5.0**
4. Destination Location: **C:\Users\Godwin Monserate\Desktop\2ND Sem 2020-2021\Information Assurance and Security\Digital Forensics\Photo Crime\Pedophile**
5. Target Filename: **Pedophile-Case.001**
6. Estimated time to finish developing the image: **3 minutes, and 58 seconds**
7. Hash Value MD5: **514cad8d821a1404ece56c78ebc62b9d**
8. Hash Value SHA1: **a8f7f7387396ef06a9eb0c73ee5b3ac96067cebb**

Pedophile Case – James Carl Liboon

Acquired using: ADI3.1.5.0
Case Number: 101024-10
Evidence Number: 101024
Submitted by: Jomar Leaño

Disk Analysis



1. Number of Files in the Source Drive: **184 Files**
2. Number of Files in the Target Image: **203 Files**
3. Number of Folders in the Source Drive: **12 Folders**
4. Number of Folders in the Target Image: **12 Folders**
5. Number of Deleted Files: **8 Files**
6. Number of Deleted Folders: **0 Folders**

Data Recovery

1. Extract the Deleted Files in the Root
   Number of Files Extracted? **4 Files**
2. Extract the Deleted Folders
   Number of Folders Extracted? **0 Folders**
   Number of Files Extracted in the Folder (Specify folder and number of files) : **0**

Pedophile Case – James Carl Liboon

Acquired using: ADI3.1.5.0
Case Number: 101024-10
Evidence Number: 101024
Submitted by: Jomar Leaño

Data Analysis

1. Examine the contents of the file if it is an image file or a document file
   Number of JPEG Files: **17 files**
2. Number of Document (.doc) Files: **2 files**
3. After Examining the signature format of the files, Identify the following:
   What is the signature Format of JPEG files? **ÿØÿâ**
   how many jpeg files have been altered?: **None**
   have you recovered the file back to its original format? **Nothing to be recovered**
   What is the signature format of a word document file? **ÐÏ.à¡±.á and PK**
   how many doc files have been altered? **None**
   have you recovered the file back to its original format? **Nothing to be recovered**
4. After recovering the file into its original form.
   Number of JPEG Files: **17 files**
   Number of Document (.doc) Files: **2 files**

5. Use HASH calculator for the image file and the source file, and compare both hash values.

   Source:
   MD5 value: **514cad8d821a1404ece56c78ebc62b9d**
   SHA1 value : **a8f7f7387396ef06a9eb0c73ee5b3ac96067cebb**

   Target:
   MD5 value: **514cad8d821a1404ece56c78ebc62b9d**
   SHA1 value : **a8f7f7387396ef06a9eb0c73ee5b3ac96067cebb**

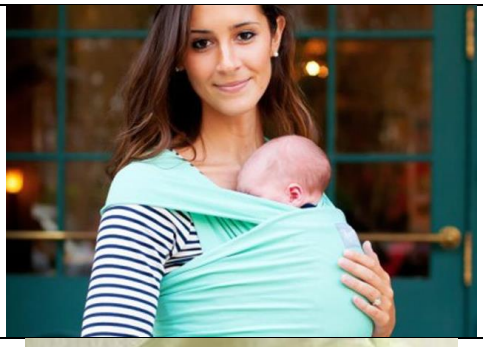
   Does the output between the source and the target image render a similar value? **Yes, it has the same hash value**

Pedophile Case – James Carl Liboon

Acquired using: ADI3.1.5.0
Case Number: 101024-10
Evidence Number: 101024
Submitted by: Jomar Leaño

Report Conclusion

Evidence Table

Fig #	Image Name:	Image	Date Deleted	Date Recovered
1	baby-wearing.jpg		3/21/2021	10/12/2022
2	baby1.jfif		3/20/2021	10/12/2022
3	baby2.jfif		3/21/2021	10/12/2022
4	baby3.jfif		3/21/2021	10/12/2022

Pedophile Case – James Carl Liboon

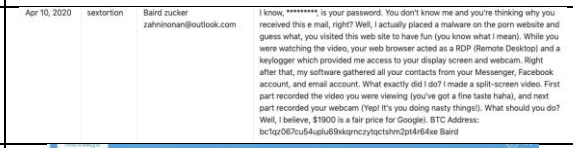
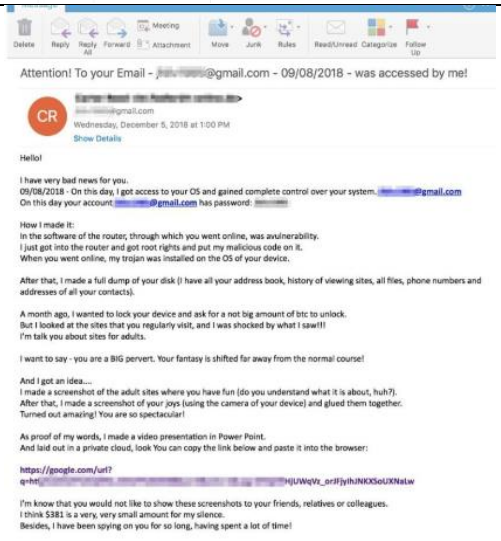
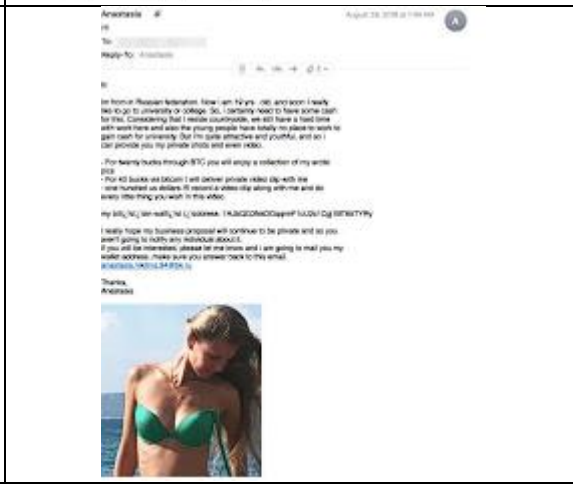
Acquired using: ADI3.1.5.0
Case Number: 101024-10
Evidence Number: 101024
Submitted by: Jomar Leaño

5	daughter janine at school.jfif		3/21/2021	10/12/2022
6	father daughter love.jfif		3/21/2021	10/12/2022
7	i love my little girl.jfif		3/21/2021	10/12/2022
8	me and janine.jfif		3/21/2021	10/12/2022

Pedophile Case – James Carl Liboon

Acquired using: ADI3.1.5.0
Case Number: 101024-10
Evidence Number: 101024
Submitted by: Jomar Leaño

Using FTK Imager and all the available evidence, an image copy of the data was made in order to preserve the evidence. A laptop underwent considerable and thorough analysis using a digital forensic process. A major number of the 8 crucial photographs that were discovered after extensive file searching and the recovery of lost files—including those of James Carl Liboon, his wife, Janine, and their daughter—are displayed here. Other photographs also appear to be youngsters, although these kids have no connection to the people who were detained.

Fig #	Image Name:	Image	Date Deleted	Date Recovered
1	Screenshot-2020-04-20-at-15.59.04.png	 Apr 10, 2020 sextortion Baird zucker zahninonan@outlook.com I know, ********* is your password. You don't know me and you're thinking why you received this e mail, right? Well, I actually placed a malware on the porn website and guess what, you visited this web site to have fun (you know what I mean). While you were watching the video, your web browser acted as a RDP (Remote Desktop) and a keylogger which provided me access to your display screen and webcam. Right after that, my software gathered all your contacts from your Messenger, Facebook account, and email account. What exactly did I do? I made a split-screen video. First part recorded the video you were viewing (you've got a fine taste haha), and next part recorded your webcam (Yep! It's you doing nasty things!). What should you do? Well, I believe, $1900 is a fair price for Google). BTC Address: bc1qz067cu54uplu69xkqmczytqctshm2pt4r64xe Baird	3/21/2021	10/12/2022
2	sei_43779174-e47e.jpg	 Attention! To your Email - [redacted]@gmail.com - 09/08/2018 - was accessed by me! CR [redacted]@gmail.com Wednesday, December 5, 2018 at 1:00 PM Show Details Hello! I have very bad news for you. 09/08/2018 - On this day, I got access to your OS and gained complete control over your system. [redacted]@gmail.com On this day your account [redacted]@gmail.com has password: [redacted] How I made it: In the software of the router, through which you went online, was avulnerability. I just got into the router and got root rights and put my malicious code on it. When you went online, my trojan was installed on the OS of your device. After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts). A month ago, I wanted to lock your device and ask for a not big amount of btc to unlock. But I looked at the sites that you regularly visit, and I was shocked by what I saw!!! I'm talk you about sites for adults. I want to say - you are a BIG pervert. Your fantasy is shifted far away from the normal course! And I got an idea.... I made a screenshot of the adult sites where you have fun (do you understand what it is about, huh?). After that, I made a screenshot of your joys (using the camera of your device) and glued them together. Turned out amazing! You are so spectacular! As proof of my words, I made a video presentation in Power Point. And laid out in a private cloud, look You can copy the link below and paste it into the browser: https://google.com/url?q=ht[redacted]HjUWqVz_or3FjylhJNKXSoUXNsLw I'm know that you would not like to show these screenshots to your friends, relatives or colleagues. I think $381 is a very, very small amount for my silence. Besides, I have been spying on you for so long, having spent a lot of time!	3/21/2021	10/12/2022
3	!mage13.png		3/21/2021	10/12/2022

Pedophile Case – James Carl Liboon

Acquired using: ADI3.1.5.0
Case Number: 101024-10
Evidence Number: 101024
Submitted by: Jomar Leaño

Although deleting pictures of oneself, one's wife, one's daughter, as well as other pictures of kids who aren't your own seems highly suspicious, it doesn't offer sufficient proof for one to be found guilty of pedophilia. Despite this, additional proof that points to sextortion was found in Mr. Liboon's laptop's erased files.

Report Recommendation

Screenshots of emails that the sender is using for sextortion were on his laptop. There is not enough evidence to prove that James Carl Liboon is a pedophile based on the information found on his work laptop. He might simply be a devoted father who has no sexual or evil intentions. He may be devoted to his family, but there is evidence that he has been involved in numerous sextortion cases, indicating that he does not have the same regard for other women. As a result, James Carl Liboon might not be found guilty in this pedophilia case, but his sextortion-related activities need to be looked at more thoroughly.

After analyzing the data, the examiner has acquired sufficient evidence to bring charges against Kushiro Yamamoto from many drug case incidents. A trial is scheduled for the guilty, and we firmly support the harsh penalty of the accused based on the proof of several crimes that has been revealed.

SF Quiz #4

Due No due date **Points** 45 **Questions** 17
Available after Nov 21 at 3pm **Time Limit** 25 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	24 minutes	31.5 out of 45

Correct answers are hidden.

Score for this quiz: **31.5** out of 45
Submitted Nov 21 at 3:25pm
This attempt took 24 minutes.

Question 1

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
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
Verification Process & Certificate Issue	After you have done the

Partial

Question 2

6 / 7 pts

Identify the following prime numbers. choose all that apply.

- [x] 751

- [x] 347
- [x] 491
- [ ] 720
- [ ] 770
- [x] 421
- [x] 491
- [ ] 910
- [ ] 330
- [ ] 6
- [x] 19

Question 3

1 / 1 pts

Process of converting electronic data into another form, called cipher text, which cannot be easily understood by anyone except the authorized parties. This assures data security.

- (•) Encryption
- ( ) Hashing
- ( ) Decryption
- ( ) Digital Certificate

Incorrect

Question 4

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.

asymmetric encryption

Incorrect

Question 5

0 / 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

Incorrect

Question 6

0 / 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 encryption

Question 7

1 / 1 pts

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

- (●) cryptanalysis
- ( ) steganography
- ( ) imaging
- ( ) acquisition

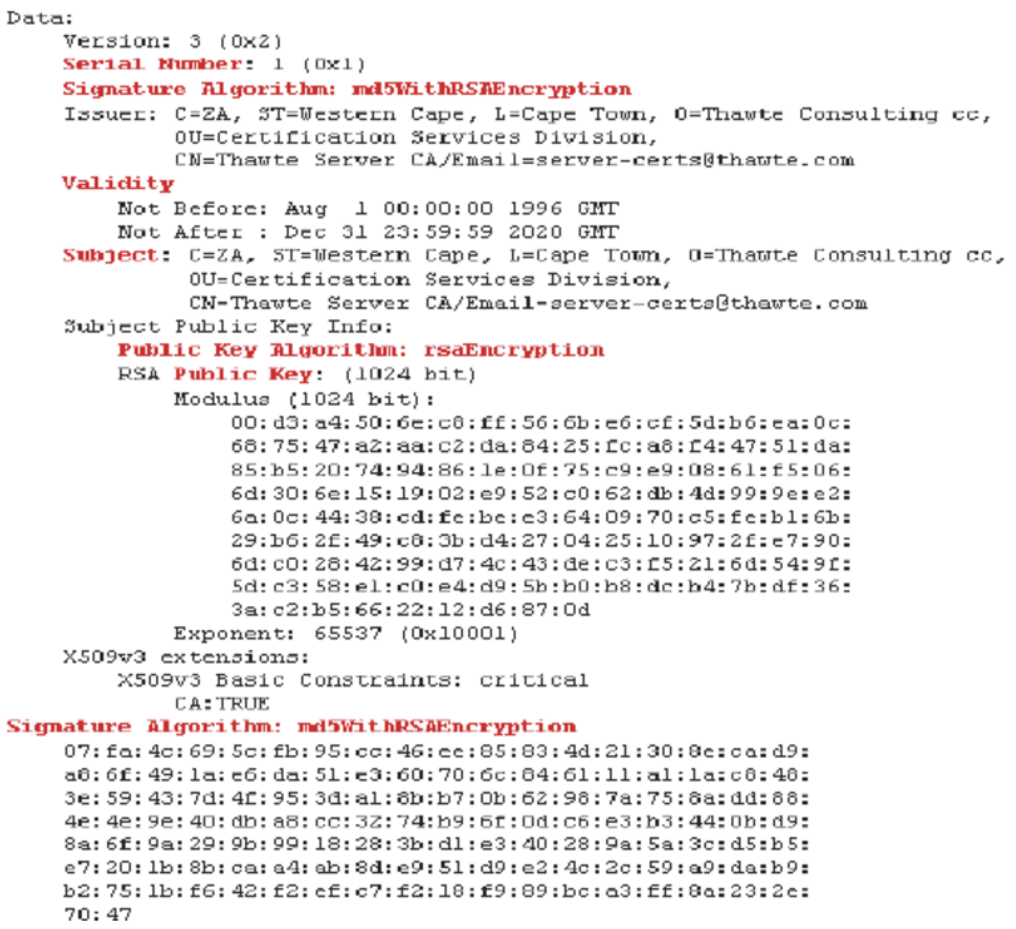
Incorrect

Question 8

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:21:30:8c:ca:d9:
    a0:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:40:
    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:cf:c7:f2:18:f9:89:bc:a3:ff:8a:23:2c:
    70:47
```

rivest-shamir-adleman

Question 9

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.

- asymmetric cipher
- advance encryption standard

- symmetric cipher
- data encryption standard

Question 10

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.

- integrity
- hashing
- non-repudiation
- authenticity

Question 11

1 / 1 pts

It is a 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 within the certificate.

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

x.509

Question 12

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.

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

Partial

Question 13

2.5 / 5 pts

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

Server Certificates	Allows visitors to exchan
Server Certificates	are used by corporate er
Personal Certificates	Prove authorship and re
Personal Certificates	These are perfect for bu
Corporate Certificates	Client Certificates or Dig

Corporate Certificates	These are perfect for bu
Developers Certificates	Prove authorship and re
Developers Certificates	Used to sign software or

Partial

Question 14

3 / 5 pts

Identify the 2 different types of SSL Certificates by Matching Column A with Column.

Basic SSL certificate	It allows you to secure o
Basic SSL certificate	This certificate is quite w
Basic SSL certificate	If you want to also anoth
Wildcard SSL certificate	allows you to secure you
Wildcard SSL certificate	This is best suited for lar

Question 15

2 / 2 pts

Which of the following are the basic SSL Certificates?

Choose all that applies.

- [ ] Wildcard Server
- [ ] SSL 256
- [ ] Positive SSL Wildcard
- [ ] SSL 128
- [x] SSL123
- [x] Positive SSL

Incorrect

Question 16

0 / 2 pts

What are the 2 things does SSL Certificates do?

- [x] Authenticate your website's identity.
- [x] Encrypt the information sent from your website visitor's browser to your website
- [x] encrypting communication between the website and its users.
- [x] used when a website wants to accept sensitive information like passwords, credit card details and other sensitive information.

protects your customer's personal data including passwords, credit cards and identity information.

Incorrect

Question 17

0 / 2 pts

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

advanced encryptic _____

data encryption sta _____

rivest-shamir-alden _____

Answer 1:

advanced encryption standard

Answer 2:

data encryption standard

Answer 3:

rivest-shamir-aldeman

Quiz Score: **31.5** out of 45

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

SF Quiz #5: Test 2

Due No due date **Points** 26 **Questions** 7
Available after Nov 23 at 3:30pm **Time Limit** 30 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	12 minutes	20 out of 26

ⓘ Correct answers are hidden.

Score for this quiz: **20** out of 26
Submitted Nov 23 at 3:53pm
This attempt took 12 minutes.

Incorrect

Question 1

0 / 2 pts

Write the formula of the euler's function:

totient = ?

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

phi(n)

Question 2

2 / 2 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 3

8 / 10 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 4

1 / 3 pts

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

if p = 2; q = 13

- [ ] 19
- [x] 11
- [x] 5
- [x] 7
- [ ] 13
- [ ] 9
- [ ] 15

- [ ] 3

Question 5

2 / 2 pts

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

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

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

Question 6

2 / 2 pts

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

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

12

Question 7

5 / 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
- [ ] 3
- [ ] 18
- [ ] 7
- [x] 10
- [x] 17
- [ ] 6
- [x] 20
- [x] 13
- [x] 19
- [ ] 15
- [ ] 9

Quiz Score: **20** out of 26