1)

a) Length(Herschelle) % 2 = 10 % 2 = 0 = 2-anonymous

ID	Name	Place	City	Country	No.of Items	Price
C0001*	*	*	*	*	2-3	6000
C0000*	*	New York	New York	USA	1-2	3000
C0002*	*	New York	New York	USA	2-3	5000
C0002*	*	*	*	India	1-2	5000
C0000*	*	*	*	*	1-2	10000
C0000*	*	New York	New York	USA	2-3	5000
C0001*	*	Brisban	Brisban	Australia	2-3	7000
C0002*	*	Brisban	Brisban	Australia	1-2	7000
C0001*	*	Chennai	Chennai	India	1-2	8000
C0000*	*	Mumbai	Mumbai	India	1-2	7000
C0000*	*	Chennai	Chennai	India	1-2	7000
C0002*	*	Mumbai	Mumbai	India	2-3	7000

b)

Email	Year	Smoke or not
*63@iiitd.ac.in	*	No
*45@iiitd.ac.in	*	Yes
*92@iiitd.ac.in	2nd	No
*78@iiitd.ac.in	3rd	No
*03@iiitd.ac.in	3rd	Yes
*63@iiitd.ac.in	2nd	No

Randomisation: Added noise without changing data's aggregate distribution to make it harder to figure out why exactly data is being collected.

Suppression: Removed some entries to not let anyone distinguish between 1st and 4th year.

2-anonymity: At least 2 rows are similar again to prevent distinguishing.

2)

- Clearly defining the privacy policy and making users aware of it.
- Give options to users as to how any personal information collected from them may be used. Two traditional types of choice/consent
  i) Opt-in requires affirmative steps by the consumers to allow the collection and/or use of information
  ii) Opt-out requires affirmative steps to disallow the collection and/or use of such information.
- Users should be able to review, update, delete some personal information on a particular website.
  Access must encompass
  i) timely and inexpensive access to data
  ii) means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.

- Websites must use both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.
- Mechanisms to enforce all above privacy principles.
  i) Self-Regulation: Mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties.
  ii) Private Remedies: A statutory scheme could create private rights of action for consumers harmed by an entity's unfair information practices.
  iii) Government Enforcement: Civil or criminal penalties enforced by governments.

3)

a) No, Bob will not be able to decrypt the message, since he does not have 'private_alice' to decrypt the message. The message is encrypted with 'public_alice' and can only be decrypted with 'private_alice'.

b) Yes, bob will be able to decrypt the message, since he has 'private_bob' to decrypt the message. Confidentiality: Yes, the message is kept confidential as the key to decrypt the message belongs to Bob only. The message is encrypted with 'public_bob' and can only be decrypted with 'private_bob'. Non-Repudiability: No, it is ensured, since the hash is not signed. For Bob, there is no way of knowing that the message is from alice. He can only use the hash to validate the message.

Steps to decrypt the message:

Decrypt the ciphertext - encrypt(concat(m, hash(m)), public_bob) using 'private_bob' key to get concat(m, hash(m))

Use the function to split concat(m, hash(m)) to get m and hash(m)

c) Yes, bob will be able to decrypt the message m. Confidentiality: Yes, the message is kept confidential as the key to decrypt the message belongs to Bob only. The message is encrypted with 'public_bob' and can only be decrypted with 'private_bob'. Non-Repudiability: Yes, it is ensured as the hash is signed using 'private_alice' and Bob can verify the signature using 'public_alice' to check that the message is from her.

After that the following steps to check the integrity of m.

Decrypt the ciphertext - sign(hash(m), private_alice) using key 'public_alice' to get hash(m)

Use hash(m) to verify if m is the same as the message sent to them

Steps to decrypt the message:

Decrypt the ciphertext - encrypt(m, public_bob) using 'private_bob' key to get m

d) Yes, Bob will be able to decrypt the message m. Confidentiality: Yes, the message is kept confidential as the key to decrypt the message belongs to Bob only. The message is encrypted with 'public_bob' and can only be decrypted with 'private_bob'. Non-Repudiability: No, it is ensured, since the hash is not signed. For Bob, there is no way of knowing that the message is from Alice, since it is signed using 'private_bob' and doesn't have Alice's signature . He can only use the hash to validate the message.

Steps to decrypt the message:

Decrypt the ciphertext - encrypt(m, public_bob) using 'private_bob' key to get m

e) Yes, bob will be able to decrypt the message m. Confidentiality: Yes, the message is kept confidential as the key required to decrypt the message belongs to Bob(private_bob) and Alice(private_alice), only. Non-Repudiability: It is not ensured, as the integrity of the message can not be verified since the signed hash is not sent along with the message.

Steps to decrypt the message:

Decrypt the Ciphertext - encrypt(sym, public_bob) using 'private_bob' key to get 'sym'

Use 'sym' to decrypt the ciphertext - encrypt(m,sym) to get 'm'

f) Yes, bob will be able to decrypt the message m. Confidentiality: No, the message is not kept confidential as the keys sym_1 and sym_2 are accessible to everyone using sign(sym_1, private_alice) , and sign(sym_2, private_alice) and public_alice. Thus, the keys sym_1 and sym_2 are public and can be used to decrypt encrypt(encrypt(m, sym_2), sym_1) to get m. Non-Repudiability: It is not ensured, as the integrity of the message can not be verified since the signed hash is not sent along with the message.

Steps to decrypt the message:

Decrypt the Ciphertext - encrypt(sym_1, public_bob) using 'private_bob' key to get 'sym_1'

Decrypt the Ciphertext - encrypt(sym_2, public_bob) using 'private_bob' key to get 'sym_2'

Use 'sym1' to decrypt the ciphertext - encrypt(encrypt(m, sym_2), sym_1) to get encrypt(m, sym_2)

Use 'sym2' to decrypt encrypt(m, sym_2) to get 'm

4)

System:

- Google classroom of FCS with access to people having IIITD account.
- It consists of Professor, TAs and students enrolled in the course.
- TAs and Professors can post assignments, grade them and view the submission of all the students
- A student can only view his own submission only and cannot modify it after turning in.
- The account data can be seen by IIITD administration and google itself.

Next Steps:

- Submissions of google classroom need to be protected.
- Adversaries: TAs, Professor, thiefs.
- Vulnerability: Local copy of submissions on the system of TAs and Professor.
- Threats: Tampering of data, theft.
- Risk to the future of the students.

5)

a)

1. Brute Force Attack: This is the simplest but inefficient way of attack. All possible alphabet and integer combinations are tried to guess the password of the targeted person.
2. Dictionary Attack: Combinations of all possible words in the dictionary along with integers are tried to guess the password. This is an efficient version of brute force attack.

3. Password Resetting: The hacker manipulates a website into generating reset password link and compromises the user's password. He then tries to get the reset token or sends the user to his own server creating identical website.
4. Phishing: In this attack the user is tricked into revealing sensitive information to the attacker or to deploy malicious software on his device. This is done through various mediums like emails, SMS voice, page hijacking etc.
5. Rainbow Table: Large table bases are available on the internet which contain hashes and their underlying plain text of various algorithms like MD5. In this attack the hacker observes the hash from leaked database of a company and tried to obtain the plain text from the table base.

b)

1. Password scheme is secure only if the secret key of the server is NOT leaked or stolen.
2. The ID should be dynamic for each login to avoid leaking partial information about the user's login message to the adversary.
3. The passwords or verification tables are not stored in the system.
4. The passwords can be set and updated easily without restrictions by the users.
5. The passwords cannot be revealed by anyone.
6. The passwords are hashed before transmission.
7. The length of a password must be appropriate.
8. The password scheme must be efficient and practical.
9. Unauthorized login should be detected quickly when a user inputs wrong password.
10. A session key is established during password authentication process to provide confidentiality of communication.

c)

i) Total permutations = 127^n, where n is length of the password

Formula = 127^n * 0.1 / 10000 seconds

For length 1: < 1 seconds

For length 2: <1 seconds

For length 3: 21 seconds

For length 4: 2602 seconds

For length 5: 330384 seconds = ~ 92 hrs

For length 6: 41958730 seconds = ~ 485 days

For length 7: 5328758602 seconds = ~ 171years

For length 8: 676752342411 seconds = ~ 21757years

ii)

Total permutations = (26 + 26 + 10)^n, where n is length of the password

Formula = 62^n * 0.1 / 10000 seconds

For length 1: <1 seconds

For length 2: <1 seconds

For length 3: 3 seconds

For length 4: 148 seconds

For length 5: 9162 seconds = ~ 153 mins

For length 6: 568003 seconds = ~ 158 hrs

For length 7: 35216147 seconds = ~ 408 days

For length 8: 2183401056 seconds = ~ 71 years

iii)

Total permutations = 10^n, where n is length of the password

Formula = 10^n * 0.1 / 10000 seconds

For length 1: <1 seconds

For length 2: <1 seconds

For length 3: <1 seconds

For length 4: <1 seconds

For length 5: 1 seconds

For length 6: 10 seconds

For length 7: 100 seconds

For length 8: 1000 seconds

d)

i)

When the authentication module is directly connected to the server, it provides the most secure way. To attack this adversary can spoof the authentication server and replace it with something else. If data servers are located somewhere else, so the users need to communicate through a network, then adversary can try to tamper with the network.

ii)

Attacker can intercept the communication, then it can send a “Yes” and perform a fake authentication. There is no need to find the biometrics of a valid user. Or he can perform the same function from a malicious program installed on the pc of user.

6)

a)

The access control lists are used to represent access control matrices in following way: -
- The access control list represents the access matrix in a way that is column wise in which there is a different Access Control List for different objects.
- They both associate to each other via objects with the help of access rights.

The environment in which they are mostly used are: -
- They are mostly used in Windows and Linux.
- In Linux there is flexibility to perform any modification so it is mostly used here.
- Also, in Windows there is a stable platform which is even better than linux.

Advantages: -
1. It helps in controlling the traffic flow.
2. It monitors the traffic to always ensure that the system is not flooded.
3. It also provides security for the Network access.
4. It improves the performance by restricting the number of users that can access the system.
5. It also saves the money of the organisation.

Disadvantages: -
1. In some cases the ACL unintentionally can open the security holes of the system that can lead to many attacks.
2. Since user get a very limited time of access using this there can be many cases in which the user is not able to complete the work that it intends to do thus demotivating them.

b)

1) Paul cannot read or write to the document.
2) Anna can read and write to the document.
3) Jesse can read but cannot write to the document.
4) Sammi can read the document but cannot write.
5) Robin cannot read but can write to the document.

c)

i)

- According to the policy, Group 1 is allowed to read.
- So, if the first policy is applied then, Group 1 i.e., group having Alice will only have access to read and not to write the files. So, Alice will not be able to perform the write operation.

ii)

- The first policy on the list is not giving access to Alice to write.
- The second policy on the list is giving access to Alice for the write operation.
- Since Alice is both in Group 1 and Group 2 and Group 2 gives access to write to Alice, so Alice will be allowed to write.

7)

a)

When every computer is linked to all others, we have a complete graph. This implies n(n-1)/2 edges.

b)

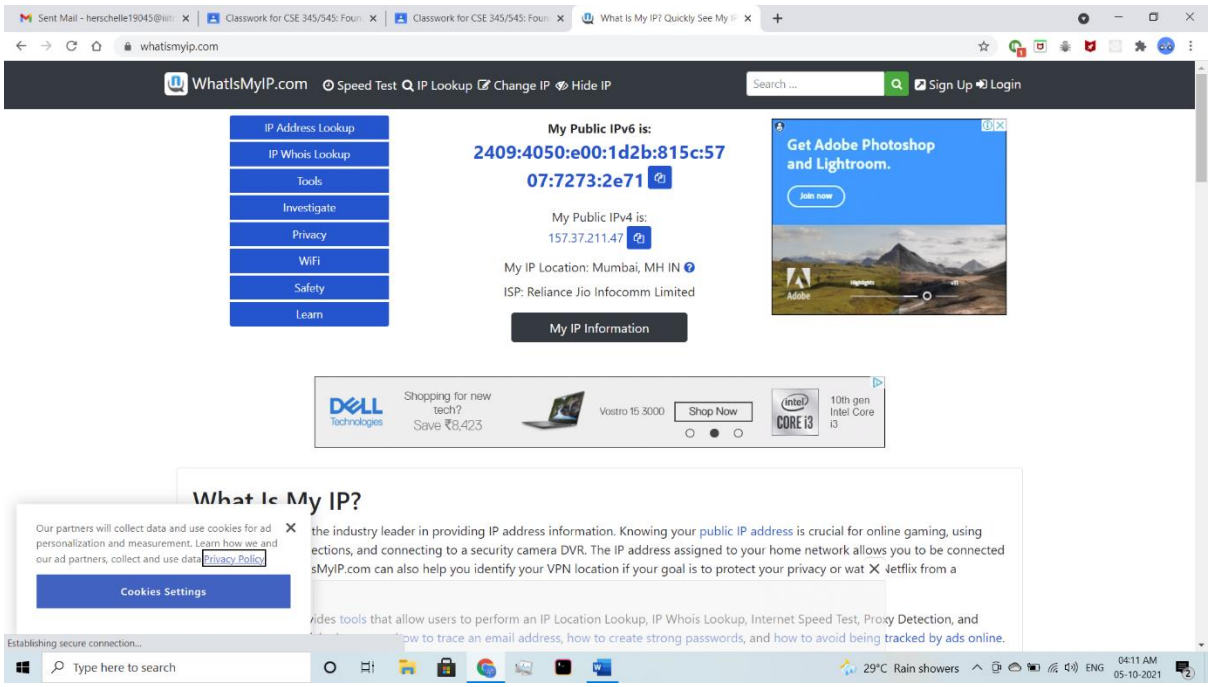
This field is present to show the extension forecast of the X.509 certificate. A CA can use extensions to issue a certificate only for a specific purpose (e.g., only for signing digital object). Each extension can be critical or non-critical. If an extension is critical and the system processing the certificate does not recognize the extension or cannot process it, the system MUST reject the entire certificate. A non-critical extension, on the other hand, can be ignored while the system processes the rest of the certificate.

c)

Yes, certificate authorities are trustworthy as they are trusted organization and work deliberately to make internet a safe and secured place to work and interact with.

They act as organization that provide a authorized certificate to the websites after verifying the details just like a passport authority verifies document of citizens to provide them passports.

d)



I see both IPv4 and IPv6.

IPv4 Advantages or IPv6 Disadvantages:

1. Existing infrastructure – Most websites use IPv4, even those that also support IPv6. This makes version four a more seamless experience. That is, until most of the Internet switches to version six.
2. Simplicity – IPv4's 32-bit dotted decimal is much smaller and simpler than IPv6's hexadecimal numbers. This simplicity is easier for humans to read.
3. Support – Because most traffic is still using IPv4, Network operators find IPv4 familiar. They may wait until more traffic is IPv6 before they make any decisions about their own infrastructure—especially if they have enough IPv4 addresses for the near future.

IPv4 Disadvantages or IPv6 Advantages:

1. Exhaustion of IPv4 – The world is short on IPv4 addresses. This means there's a cost to buy IPv4 addresses, where IPv6 addresses can be for the cost of registration with a regional registry (RIR).
2. IPv6 Speed – Sites load 5% faster in median and 15% faster for the 95% percentile on IPv6 compared to IPv4.
3. Network Address Translation for IPv4 – NAT allows a group of devices that share a single public IP with IPv4. This requires complex configurations like forwarding and firewall alterations. Because IPv6 has so many addresses, IPv6 devices don't require additional configuration.

8) n-1, where n is number of lectures after 1st one.