Q1)

a. ElGamal encryption is a public-key cryptosystem which uses asymmetric key encryption. ElGamal encryption is based off of the Diffie-Hellman key exchange which is a method of securely sharing cryptographic keys over a public channel. This cryptosystem is defined over any cyclic group G and is based on the difficulty of finding the discrete logarithm G (which is difficult even if we knew g^a and g^k)

b. Eve has the ElGamal public key which means she has the Cyclic group F, the prime number q, the element f which was chosen from F, and the value $h = f^a$ but a is of course unknown. Eve has a ciphertext C, and some oracle that can decrypt any ciphertext except C.

   To decrypt a message you calculate some value $s' = f^{ak}$ where a in the receivers private key, and we are given $p = f^k$ ← the oracle would know this value to be able to decrypt the message

   The encrypted message M*s (where $s = f^{ak}$) is decrypted by diving by s' (since s = s')

   Let C = (c1, c2) which is the encryption of the unknown message. We can compute an ElGamal encryption using the value 2 with the public key (since any prime number and 2 will have gcd = 1). Let d = (d1, d2) be the encryption of 2 using the public key that Eve has.

c. Elgamal is semantically secure under the Hash Diffie-Hellman assumption

Q2)

a.

- During a TLS handshake the following happens (only cryptographic info):
  - Decide on which cipher suites to use (cryptographic information)
  - Authenticate the identity of the server via the server's public key and the SSL certificate authority's digital signature (client does this)
  - The client sends the premaster secret which is encrypted with the public key from the SSL certificate and can only be decrypted with he private key of the server
  - Generate session keys to use symmetric encryption
- Basically they decide on the cipher suite which is a set of encryption algorithms that is used to secure communications connection.

b. Asymmetric encryption is used to establish a secure session between client and server, while symmetric encryption is used to exchange data during the secured session that is established by asymmetric encryption. Since symmetric encryption uses one key for both encryption and decryption, while asymmetric uses public for encryption and private for decryption, asymmetric encryption is more secure, thus it is used in the portion of TLS which requires a secure connection. If symmetric encryption was used to encrypt and establish the session, the public key can be easily found and the session is now compromised.
c. A certificate authority (CA) confirms that the site is owned by you and that the organization which you own and that owns the site is legitimate. It creates trust between the customers web browsers. The CA issues digital certificates essentially that certifies the ownership of the public key by the person on the certificate who owns the website.
d. We know: tls is invalid and Mallory can perform a MITM attack to steal Alice's banking information
    a. When Alice sends a request for Bobs servers public key, Mallory receives this message instead and using their own address as the response address, sends to the message to the server
    b. The server replies with its public key which is then taken by Mallory (however the server thinks it's the client) and instead Mallory sends their own public key to Alice and Mallory creates the pre-master secret with the public key from Bobs server
    c. The pre-master secret that the client generates uses Mallory's public key, and is sent to Mallory, who then sends their actual pre-master secret key to the server
    d. Then the server and Mallory compute a master secret for their connection, as does Alice and Mallory, which makes the Alice and Bobs server think they have a secure connection, but Mallory can is able to read everything

- This is everything that Mallory needs to generate and modify to establish a secure connection

Q3)

Thought process: we select the row for Nicky to get her race and position, since salary is repressed we won't see that

Our tracker will be Nicky's race which can be found by pulling his/her row

R = SELECT race FROM Employee WHERE Name = "Nicky"

Tracker: T = SELECT SUM (Salary) FROM Employee WHERE Race = R

QUERY:

A = SELECT SUM (Salary) FROM Employee WHERE Race = R OR Name="Nicky"

B = SELECT SUM (Salary) FROM Employee WHERE Race != R OR Name="Nicky"

C = SELECT SUM (Salary) FROM Employee

Nicky Salary = A + B – C

b) GUESS = what we think Lily has ← again we assume we can get lily's race

A = select count (*) from employee where name="lily" and salary = target or race = R

B = select count (*) from employee where name = "Lily" and Salary = Target or race != R

C = select count(*) from employee where Salary <= 200,000

Count = A + B – C

Q4)

- An IRP includes the processes, procedures, and documentation related to how an organization responds to and recovers from incidents, threats etc.
- 4 things I would consider in the IRP for a data breach is
    - 1. Identification and Scoping
        - That is, a way of detecting security incidents that request the response of Computer Security Response Team.
    - 2. Data Access Security
        - In a data breach there can be multiple levels for types of data, it is important to know which type of data was accessed, its level (in terms of importance/security) and where it was located when they were accessed
    - 3. Damage Control/Eradication
        - In this part of the plan, we should describe how to contain the threat to prevent further damage from incurring and removing the threat
    - 4. Recovery
        - Enabling all systems to be put online and monitored to ensure that it is no longer compromised