Q1

1. Not secure. Because $g^{a+b} \, mod \, p = (g^a \, mod \, p) \times (g^b \, mod \, p) \, mod \, p = A \times B \, mod \, p$. "Man in the middle" can easily get the secret key by eavesdropping.
2. Incorrect. Because it is extremely hard for Alice and Bob to calculate their secret key. Since they cannot know what number (a for Alice, and b for Bob) did the other person chose.
3. It is correct and secured. Both of them know what A and B are, and g^{ab}. And g^{ab} gives them the protection. (Both of them can easily calculate g^{ab} by $A^b \, or \, B^a$, but others without knowing a or b cannot)
4. Alice – Mallory – Bob
   Alice firstly sends $A = g^a \, mod \, p$. Mallory intercepts and change it into $A' = g^m \, mod \, p$
   Bob then sends $B = g^b \, mod \, p$. Mallory intercepts and change it into $B' = g^m \, mod \, p$
   Both Alice and Bob assume that the values the received are sent by another one, but actually, both value they received are sent by Mallory. Mallory can calculate $A^m \, mod \, p$ and $B^m \, mod \, p$ as the keys to send message to Alice and Bob. Each time receive the message from any of them, just simply decrypt, and encrypt with another key and send it out.
   And from Alice and Bob's perspective, nothing unusual happens.

Q2

1. Assume, n=15, d=3, m=2. Then $s' = 2^3 \, mod \, 15 = 8$. But, also note that, $17^3 \, mod \, 15 = 4913 \, mod \, 15 = 8$. Message is not the original one, but verification will still pass.
2. 2^{30}, for each place, Mallory can choose to change or not change.
3. Total number of possible hash is 2^k, number of contract versions Mallory creates is 2^{30}.
   So the probability should be $\frac{2^{30}}{2^k} = \frac{1}{2^{k-30}}$
4. Since Mallory find a collision, she can trick Alice to sign a different contract that seems to be the original one, but with the increased amount to be paid. But Alice will believe she is signing the original one.

Q3

1. They agreed on which ciphersuite to use, and the session key K.
2. Asymmetric is used during handshaking. At this stage, there is no agreement on server and client, so asymmetric encryption is preferred to protect their communication. Symmetric encryption is used after handshaking. Because server and client has established the agreement on ciphersuite and session key (which others does not know), so for less computing purpose, a symmetric encryption is preferred.
3. Certification authority issues digital certificates. When client connects to server through

HTTPS, the server will provide its certificate to the client during the handshake. Then client can use CA's public key to verify the signature on the certificate. If it is valid and trusted, then client can assume communicating with legitimate server.

4. Alice – Mallory – Bob
   a. Alice should generate or modify the server's digital certificates, which claims to be from Bob's website but signed with Mallory's own private key.
   b. Mallory firstly intercepts Alice initial request to Bob's website.
      Mallory generates a fake digital certificate for Bob's website, claiming to be from Bob, but signed with Mallory's own private key.
      Mallory establishes the connection with Alice's browser.
      Mallory establishes another connection with Bob's website using the real certificate.
      Mallory forwards Alice's request by decrypts with the key shared with Alice, and encrypts it with the key shared with Bob, and send it to Bob.
      Mallory forwards Bob's response by decrypts with the key shared with Bob, and encrypts it with the key shared with Alice, and send it to Alice.
      And Mallory can record the bank information during the process.
5. Attacker can monitor the communication between Bob and server. Since the initial connection is through HTTP, attacker can get Bob's bank information directly since it is plain text.
   To prevent this, what Bob can do is directly connects to HTTPS (e.g. using something like HTTP strict transport security, which guarantees the connections are all through https). Or for server, which can redirect the request from HTTP to HTTPS whenever the client want to access HTTP version of the website, the redirection should be executed before the data transmitted.

Q4

1. No, not 3-anonymous. One way of changing value ranges of age is [21-26],[27-32],[33-38]. By doing this, the new table is 2-diverse
2. Jhon is aged in [21-25], and his race is White.
3. Differential Privacy

Q5

1. To not let companies learn from user queries, a trivial solution is to get info of all items. To achieve this, Alice needs to upload $m \times n$ matrix elements.
2. For setting a, total number of matrix elements downloaded is mn, for setting b, total number of matrix elements downloaded is $\frac{mn^2}{2}$. The first setting downloaded a smaller number of matrix elements. This is because for my trivial scheme, user need to download info of all items, even if the user only want to obtain the detail of 1 product. So for setting a, there is only one user, whereas setting b has $\frac{n}{2}$ users.

3. Let's focus on one specific position of q1 and q2.
   There are 4 possible combination, (q1,q2) = (0,0), (0,1), (1,0), (1,1), and the corresponding responses are (s1,s2) = (0,0), (0,1), (1,0), (1,1). Applying XOR, for q, it becomes 0,1,1,0, and for s it becomes 0,1,1,0.
   Now consider q3 = q1 XOR q2 XOR q, with corresponding q1,q2 values, q3 should be 0,0,0,0(if q=1) and 0,1,1,0(if q=0), then, corresponding s3 should be 0,0,0,0(if q=1) and 0,1,1,0(if q=0)
   Now consider s = s1 XOR s2 XOR s3, with corresponding q1,q2, s1, s2, and q3, s3 values, s should becomes 0,0,0,0(if q=1) and (0,1,1,0)(if q=0)