1.

1.1) They agree on a session key, K, which is based on the client shared key and server shared key. This is then used to encrypt and decrypt information sent by the client and server.

1.2) Symmetric encryption: Used in TLS as the session key. This is preferred becouse it allows users to communicate both ways while protecting the information (messages)

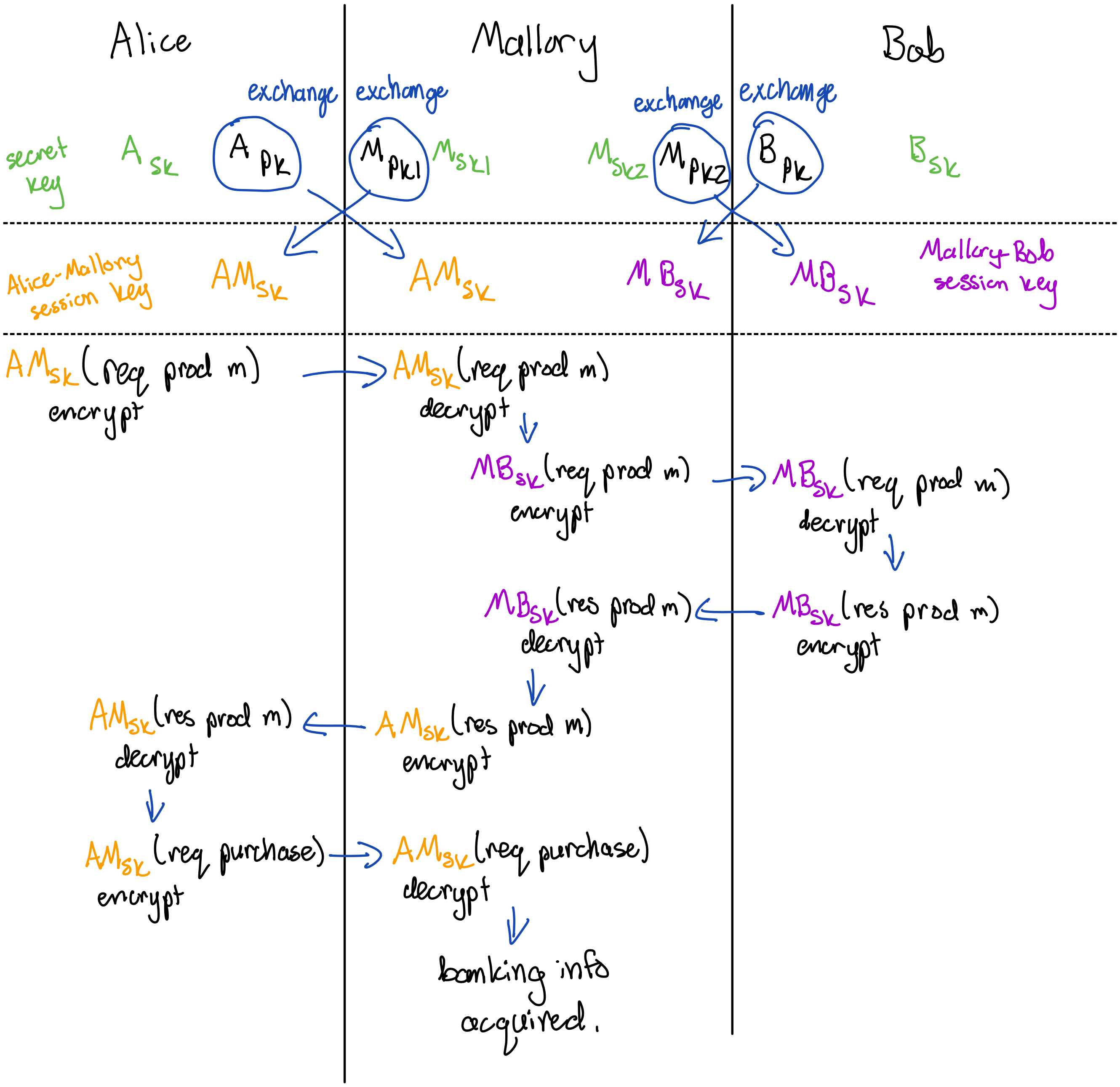
Asymmetric encryption: Used in TLS to share public client key and public server key to derive the session key. This is preferred because it is more secure when when sharing keys to transfer information. With symmetric encryption it is more dangerous to share the key because it

can decrypt and encrypt messages. But with asymmetric encryption the private key is kept safe (on client and server side) so it is safer to use assymetric encruption here to establish the shared key.

1.3) CA issue digital certificates that help the entity verify their authenticity online. So a client can check the digital certificate to verify that the entity can be trusted. In which they can then establish a secure connection.

4. a) Mallory needs to generate her own key pair, e_k, d_k, to establish a connection with Alice. Once Mallory receives Alice's shared client public key Mallory needs to generate the session key to communicate with Alice. Mallory also needs to share their public sever key so that Alice can generate the session key as well.

4. b)


Alice
Mallory
Bob
exchange
exchange
exchange
exchange
secret key
A_{sk}
A_{pk}
M_{pk1}
M_{sk1}
M_{sk2}
M_{pk2}
B_{pk}
B_{sk}
Alice-Mallory session key
AM_{sk}
AM_{sk}
MB_{sk}
MB_{sk}
Mallory-Bob session key
AM_{sk}(req prod m)
encrypt
AM_{sk}(req prod m)
decrypt
MB_{sk}(req prod m)
encrypt
MB_{sk}(req prod m)
decrypt
MB_{sk}(res prod m)
decrypt
MB_{sk}(res prod m)
encrypt
AM_{sk}(res prod m)
decrypt
AM_{sk}(res prod m)
encrypt
AM_{sk}(req purchase)
encrypt
AM_{sk}(req purchase)
decrypt
banking info acquired.

2. a) yes it is possible to recover the ids and names:

Bob:	1
Cathy:	2
Alice:	4
Robert:	5
Dave:	6

b) known

E : $x = 24$ $y = 23$

M : $x = 56$ $y = 31$

calculate slope from known x_1, y_1, x_2, y_2

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{31 - 23}{56 - 24} = \frac{8}{32} = \frac{1}{4}$$

calculate b with slope, m, and x_1, y_1 values (Eve)

$$b = y - mx = 23 - 24\left(\tfrac{1}{4}\right) = 17$$

final values

$$m = \frac{1}{4}, \quad b = 17, \quad y = \frac{1}{4}x + 17$$

emails per id

9:56	12:32	15:24
10:76	13:80	16:16
11:28	14:40	

c)

4-anonymous, for each quasi-identfier there are 3 other records with the same quasi-identifier

d) 3-diverse, there are 3 unique quasi-identifiers

e) Tim knows Matt has Heart Disease

f) Biggest range is when 7 employees have 0 emails and 1 employee has 400 in D_1 and in D_2 all employees have 0 emails.

D_1 = 7 employees : 0 , 1 employee : 400

D_2 = 8 employees : 0

$\frac{400}{8} - \frac{0}{8} = 50$ is the sensitivity.

3. a) Use an identity matrix of size nxn so when you do $q \cdot A$ you get A. Once you have A, you can simply get the row you wanted.

Frieda will need to upload an nxn matrix.

b) Using the trivial solution:

1. You will need to upload an (n/2)(n/2) identity matrix to get n/2 items from ACME. Then you will download (n/2)(m) items from ACME.

2. With all n/2 users, they will each upload nxn identity matrices, so we have (n/2)(n×n) uploads. Then each user will receive the nxm matrix, A, which means (n/2)(nxm) total dowloads.

Solution 1 involves downloading fewer matrix elements because $(n/2)m < (n/2)(n \times m)$.

d) no they do not. Assuming the servers do not contact eachother, each server is dealing with randomly generated matrices. q_1 and q_2 will be random and q_3 has many scenarios where the ACME server can't know c. For instance, take:

$$q_1 = [0], \quad q_2 = [1], \quad q = [1]$$

then $q_3 = [0]$ and ACME servers have to assume the row was not picked even though it was.

e) uploaded: $3 \cdot n$ downloaded: $3 \cdot m$

f) $3n + 3m < n^2 + nm \Rightarrow 3n + 45 < n^2 + 15n$

$$n^2 + 12n - 45 > 0 \Rightarrow (n-3)(n+15) > 0$$

so when $n > 3$, the trivial solution will upload and download more matrix elements.