1.

(a):In this case,Mallory will be able to get Alice login information.Root CA are mostly pre-install into the browser as a core of the Chain of turst.If the root CAis changed to a fake one,then we can no longer detect if the public key is trustable by TLS.Hence mallory will attack successfully.

(b):Attack will be success.Since Mallory use a valid certificate from the actual company website for her phishing website, TLS will dentify it as the real company website.

(c):Attack will be success.After Mallory runs DNS cache poisoning attack on Alice's browser successfully,the browser will jump to the phishing website when Alice try to visit the real company website.

(d):

2:

(d):The fingerprints is insert into the key,in order to check if the key is real.Without checking the fingerprints,we might import a fake or modified public key,then our message will be decrypt by other people.It would be best if users can share the fingerprints face to face,or by phone,sns.

3:

(a):

Tracker: select sum(Grade) from Student where Gender=M

Since females and males are roughly the same number in the database,the result of T will be about N/2.And K=N/8,then records of T=4k, 2k< 4k <(8k-2k),clearly q(c) matches between 2k and N-2k records,then it can be a tracker.

let q() represent the sum of query.

q(name=Blair) = q(name=Blair or Gender=M) +q(name=Blair or Gender=F)-q(All the records)

(b):From the showing part of the table,it's not a 3-anonymous.A 3-anonymous require users released at lesat another 2 records even through I have some of the information of the target.In this example,If I know someone's birthdate is 0930,then I can easliy find her in this talbe by the 093* because there is only one record match his birthdate.Then I will know this person's Postcal code is N8M5Q1.

my table:

Name	Birthdate	Gender	Postal Code
*	0***	M	N8M 5Q1
	0***	M	N8M 5Q1
	0***	M	N8M 5Q1
	0***	F	V3B 9C7
	0***	F	V3B 9C7
	0***	F	K0L 6B3
	0***	F	K0L 6B3
	1***	M	N8M 5Q1
	1***	M	V3B 9C7

1***	M	V3B 9C7

It is a 1-diverse.If I know a person's birthday is 0*** and Gender is M,then I will know his postal code is N8M5Q1.