Cordelia Tan
c63tan
21112180

Q1 p1

C1 = P1 XOR K
C2 = P2 XOR K

C1 XOR C2 = (P1 XOR K) XOR (P2 XOR K)
K XOR K = 0
Thus using properties of associativity,
(P1 XOR K) XOR (P2 XOR K) = P1 XOR P2

Q1 p2

Since the XOR of P1 and P2 is known, we could potentially use frequency analysis to try to figure out some of the words. We can guess parts of the plaintext and then check if it forms meaningful words. It would also be useful to look for common characters such as space, as XORing with space would cause other letters to change case. This can be used to evaluate the text.

Q2a

The attacker can intercept your traffic (while potentially still forwarding your traffic such that you are unaware that it has been intercepted). Since they will have access to both source and destination, you no longer have anonymity.

Q2b

Periodic changes would increase the user's privacy (allow for unlinkable anonymity). Since the relays are now always changing, the malicious entity would be less able to track any activity from the user of its relay, since it would likely change frequently.

Changing relays also just decreases the chances where one would end up using compromised relays for prolonged periods.

Q2c

Almost all connections to the email account can be linked to the user. Especially since the adversary would be able to see each time that someone is logging in to the same account.

Q2d

Advantage: The speed and stability of the circuits would likely be faster and more stable. Since there is no switching of relays, the user would likely be able to experience a faster connection as time is not lost constantly switching and connecting to new relays.
Disadvantage: If a user is using a malicious relay, the owner of the relay could potentially track the users activity and the user would now have linkable anonymity if they are doing things like logging in to certain accounts or websites.

Q2e

Entry guards help reduce the probability that the attacker can control both entry and exit relays to compromise your data. Also reduces the chance of selecting a malicious guard relay.

Q2f

We could perform traffic analysis on the packets. By monitoring things like packet timing and size at both the guard and exit nodes we could potentially match up the packets to correlate them.

Q2g

They would route traffic through a series of relays (usually with different owners) with layers of encryption like an onion. This would make it extremely hard to trace back to its origin. Things like OnionShare also work together with Tor to prevent companies from being able to access files that are being shared as long as you are sending the unguessable web address securely.

Q3a
Tracker: SELECT SUM(Grade) FROM Student WHERE Gender = ‘M’ AND Postal Code = ‘G3R 4S2’

q(C or not T)
Q1: SELECT SUM(Grade) FROM Student WHERE Name = ‘Charlie’ OR NOT (Gender = ‘M’ AND Postal Code = ‘G3R 4S2’)

q(C or T)
Q2: SELECT SUM(Grade) FROM Student WHERE Gender = ‘M’ and Postal Code = ‘G3R 4S2’ or Name = ‘Charlie’

q(S)
Q3: SELECT SUM(Grade) FROM Student

To derive Charlie’s grade, we could do q(C) = Q1 + Q2 - Q3

Q3b
Q1: SELECT COUNT(*) FROM Student WHERE Gender = ‘F’ AND Name != ‘Natalie’

Q2: SELECT COUNT(*) FROM Student WHERE Gender = ‘F’ AND Grade > 70

Q3: SELECT COUNT(*) FROM Student WHERE Gender = ‘F’ AND Grade > 70 OR Name = ‘Natalie’

If the answers for Q2 and Q3 are the same, we can infer that Natalie is also included in the group of students that have grade > 70. In the case where Natalie scored < 70, the result for Q3 would be 1 larger than Q2. Using Q2 and Q3 we can vary the grade to get closer to Natalie’s score.

Q3c
The university is incorrect. This is because even after they have hidden the last digit of the birthdates, many birth dates still remain unique, with only one entry.

Name	Birthdate	Gender	Postal Code
*	103*	M	H4A 5A6
*	123*	M	H4A 5A6
*	052*	M	Y1R 4J4
*	121*	M	Y1R 4J4
*	071*	F	G9Q 3X2
*	112*	F	H4A 5A6
*	072*	M	H4A 5A6

Name	Birthdate	Gender	Postal Code	
*	09**	F	G9Q 3X2	
*	11**	F	G9Q 3X2	
*	04**	M	H4A 5A6	
*	09**	F	Y1R 4J4	
*	05**	F	H4A 5A6	
*	10**	F	H4A 5A6	
*	10**	M	H4A 5A6	
*	12**	M	H4A 5A6	
*	05**	M	Y1R 4J4	
*	12**	M	Y1R 4J4	
*	07**	F	G9Q 3X2	
*	11**	F	H4A 5A6	
*	07**	M	H4A 5A6	

I value is likely to be at least 2, considering that this is only part of the table.

Q4.1
The petition was filed to allow the use of non official filament. Currently many 3 d printers do not allow external/alternative feedstock/filament and this petition is meant to provide more freedom and creativity to 3d printer owners regarding the materials they are using

Q4.2
The opposition’s argument is that jailbreaking these voice assistants is probably meant for pirating content. They argue that it would also increase the downloading of counterfeit apps and unauthorized software. Companies selling such devices would likely be stricter and more focused on reducing jailbreaking (by removing warranties, etc) as users could now more easily use counterfeit software instead of the company’s official software

Q4.3
No. It may still violate other laws such as the Computer Fraud and Abuse Act.
Other restrictions also ensure that scientists cannot randomly hack into others’ computers. Such as needing to be carried out in a controlled environment to avoid any harm to individuals or the public.