**CS458 A3**

**Yu Gan**

**20563500**

Written part



Public key value that Bob gives to Alice is

The resulting secret key that is generated as a result of DH protocol is

1. Eve knows . Thus, she knows that . Eve can recover a and b from these information. Since p is smaller than 512 bits, Eve can still calculate a and b. If p is larger than 512 bits as well as g, then it is really hard for Eve to calculate a and b.
2. Mallory can counterfeit a key , where m is a large random key chosen by Mallory. Then, she intersects A and B and send M to both Alice and Bob. This way. Alice would think that Bob receives her private key and sends back his private key, and Bob would think that Alice receives his private key and sends back her private key. Therefore, Mallory could obtain all of the plaintext communications between Alice and Bob. This problem can be prevented if Alice and Bob exchange their private key without using public network. Instead, they can exchange their private key face to face.
3. Fingerprints help us to verify if we got the right key. If someone claim that he can be trusted and he sends us a key with a fingerprint, we can check if the fingerprint of the received key is the same as the fingerprint he gives us. If the two fingerprints are the same, then we got the correct key. If you have a fingerprint of a key and want to find its corresponding key on the internet, and you found two same keys, you need verify that the fingerprints of the two keys matches the fingerprint. Otherwise, you could use a faked key and an attacker could launch an imperson attack.
4. Let the query c denote Name = Leonardo.

Let the tracker T denote Occupation = not staff.

Let be the result of a query.

Let s be the set of all records.

Since matches fewer than records,

Thus, we can infer Leonardo’s salary by

SELECT SUM(Salaray) FROM Employee WHERE (Name = Leonardo) OR (Occupation != Staff)

+ SELECT SUM(Salary) FROM Employee WHERE (Name = Leonardo) OR (Occupation = Staff)

* SELECT SUM(Salary) FROM Employee

1. This is not a correct 3-anonymous table because for each released record, there are not enough other released records from which record cannot be distinguished.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Birthday | Occupation | Allegiance |
| \* | 7\*\* | Specialist | Quendor |
| \* | 7\*\* | Specialist | Quendor |
| \* | 7\*\* | Specialist | Antharia |
| \* | 8\*\* | Specialist | Antharia |
| \* | 8\*\* | Specialist | Antharia |
| \* | 8\*\* | Specialist | Quendor |
| \* | 7\*\* | Staff | Kovalli |
| \* | 7\*\* | Staff | Kovalli |
| \* | 7\*\* | Staff | Quendor |
| \* | 7\*\* | Staff | Antharia |

For any quasi-identifier, there should be at least 2 “well-represent” values of the sensitive fields.

Programming part

* 1. I will modify line 5 (b) and line 6 to account for the different padding scheme used by the web server. I want to change line 5 (b) to “if then stop and output ”. And, I want to change line 6 to “output ”
  2. I will modify line 1 and line 5. I want to change line 1 to “take ”. And, I want to change line 5 to “output ”

1. On average we need padding oracle calls to perform the modified last oracle attack. The worst case of padding oracle calls required is . On average we need padding oracle calls to perform the modified block decryption oracle attack. The worst case of padding oracle calls required is ..
2. We can use MAC to fix this problem. MAC provides integrity and can prevent leakage of information required to perform an oracle attack.