CS458 A3 Writing Part
Hanzhang Chen
20574275
h343chen

[1a]
(i):

P1 XOR P2 = P1 XOR P2 XOR 0
= P1 XOR P2 XOR (K XOR K)
= (P1 XOR K) XOR (P2 XOR K)
= C1 XOR C2

Since A XOR A = 0, (1 XOR 1 = 0; 0 XOR 0 = 0), A XOR 0 = A, (1 XOR 0 = 1, 0 XOR 0 = 0), also according to associativity law and commutativity law, the equation above is correct.

(ii):
"Crib-dragging": Since they are only English ASCII text and space, so A-Z, a-z and space in bits are represented by 01000001-01011010, 01100001-01111010 and 00100000 separately. Also, given P1 XOR P2, we can get P1 = P1 XOR P2 XOR P2, let A = P1 XOR P2, P1 = A XOR P2. For the first 3 bits, they are easy to distinguish, since upper case and lower case are different. Then we can try one by one with common words on P1 = A XOR P2 given A.

(iii):
Yes, we can. If those plaintext are recovered accurately, we can get K from the following equation.

Since C = P XOR K,
C XOR P = P XOR K XOR P
=> K = C XOR P
C1 XOR P1 and C2 XOR P2 should return the same bit list.

[1b]
(i):

No, countermeasure is to add a tag or a component number.

(ii):

Yes. For those short text, brute force is a way to keep trying to obtain the plaintext without knowing the private key. To avoid this, longer text or text with paddings can solve this.

(iii):

When one is sending messages, add timestamps or nonces in order that the server can ensure this is a one-time, independent and non-repeated message.

[2d]

It is used to verify the user, using fingerprint instead of checking the long public key, which simplifies certain key management tasks. It is also unique. There will not be two same fingerprints for two public keys. It avoids that attackers use same public key to try to access files.

[3a]:

tracker: SELECT SUM(Salary) FROM Employee WHERE TYPE = ‘Nurse’

Q1: SELECT SUM(Salary) FROM Employee WHERE TYPE = ’Nurse’ AND ID != ‘jdoe’

Q2: SELECT SUM(Salary) FROM Employee WHERE TYPE != ‘Nurse’

Q3: SELECT SUM(Salary) FROM Employee WHERE TYPE != ‘Nurse’ AND ID != ‘jdoe’

Salary of jdoe = Q1 + Q2 -Q3 - tracker

[3b]

Age	Gender	Description
79	F	Flu
79	F	Heart disease
79	F	Cancer
79	F	Cancer
65	M	Flu
65	M	Heart disease
65	M	Heart disease
65	M	Cancer
78	M	Heart disease
78	M	Heart disease
78	M	Alzheimer’s

2-diversity

4.1

Average: NbW

Worst case: O(NbW)

Where N=>number of blocks

B=>block length

W=>number of possible words

4.2:

Encrypt-then-MAC construction is used to fix this. The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content. If the MAC fails, you don't even need to look at the padding. If the MAC is correct, it is cryptographically unlikely that the padding has been tampered with.

4.3:

According to the requirements above, the first byte of the padding has the value 0x01, and

all other padding bytes have the value 0x00. Thus:

For 3.1,

line 5 should be: if O(r|y)==0 then stop and return (r[b-n+1] XOR 1)(r[b-n+2] XOR 0)…(r[b] XOR 0)

For 3.2,

Line 1 should be: take (r[k] = a[k] XOR 0) for k=j,…,b

Line 5 should be: output r[j-1] XOR i XOR 1