CS 458 A3

Jia Yi Yan

Written Response Questions

1. I used a strategy called crib dragging when trying to decipher the original plaintexts. I created a program that performs the xor of text from command line input with the xor of the two plaintexts in every possible position. Using the program, I started with the word " the ", and found a couple of English words that matched in various places. Then I started prepending or appending letters to the words to see if I get an output that's English. This took a lot of trial and error. Once I had a couple of consecutive words, I searched on Wikipedia and was able to get the page I was looking for.

2. (a) Try all three combinations of m_1, m_2, m_2 to the power of e mod n and see if it matches c

   (b) Brute force through all 1000 possibilities of the integer concatenation between m and r for each m_1, m_2 or m_3. We use the same method as part a) of checking the concatenation to the power of e mod n and see if it matches c'

   (c) m_3 was encrypted to yield c'. I used the same method as part b) written in a python script with a for loop. I calculated the modular exponentiation in each iteration and I found it when r is 641 on m_3

   (d) Mallory should create the challenge by first selecting a random integer $x \in Z_n$. She computes $\overline{c} = cx^e \bmod n$. Mallory then sends this $\overline{c}$ to Bob, and Bob sends back $\overline{r} = \overline{c}^d \bmod n$. Note that $\overline{r} \equiv \overline{c}^d \equiv c^d(x^e)^d \equiv rx \bmod n$. Then Mallory can compute $r = \frac{\overline{r}}{x} \bmod n$ and thus learn the value of r

3. (a) Assumption: The birthdays of the people in the bidding platform are somewhat evenly distributed (ie. amount of people with birthdays in the first half of the year and the second half are similar)

   Tracker: People with birthdays from July onwards

   Query:

   SELECT SUM(Bid) FROM Bids WHERE Birthday >= "07/01" OR Name = "MIGUEL"

   SELECT SUM(Bid) FROM Bids WHERE Birthday < "07/01" OR Name = "MIGUEL"

   SELECT SUM(Bid) FROM Bids

   (b) The table is not 3-anonymous. The corret solution is:

Name	Gender	Age	Medical Item
*	Male	[30-49]	insulin pump
*	Female	[40-59]	thermometer
*	Male	[30-49]	blood pressure monitor
*	Male	[50-69]	blood pressure monitor
*	Female	[40-59]	thermometer
*	Male	[50-69]	insulin pump
*	Female	[40-59]	insulin pump
*	Male	[30-49]	thermometer
*	Male	[50-69]	insulin pump

   The value of l for which the table is l-diverse is 2

4. (a) Query every possible row and only use the result of the row that we want

   (b) For a particular r_j in $\vec{r}$, it can be written as:
   $r_j = Enc_K(q_1) * M_{1j} + Enc_K(q_2) * M_{2j} + ... + Enc_K(q_m) * M_{mj}$

   Using equation 4, we obtain
   $r_j = Enc_K(M_{1j} * q_1) + Enc_K(M_{2j} * q_2) + ... + Enc_K(M_{mj} * q_m)$

   By equation 1, we get
   $r_j = Enc_K(M_{1j} * q_1 + M_{2j} * q_2 + ... + M_{mj} * q_m)$

   If we decrypt r_j, we get
   $Dec_{\hat{K}}(r_j) = M_{1j} * q_1 + M_{2j} * q_2 + ... + M_{mj} * q_m$

Since $q_i = 0$ for $i \neq c$ and $q_c = 1$,
$Dec_{\hat{K}}(r_j) = M_{cj} * q_c = M_{cj}$

Thus we obtain $[Dec_{\hat{K}}(r_j)]_{1\times m} = [M_{c1}, M_{c2}, ..., M_{cn}]$ which gives us the row of M as required

5. (a) It is difficult to achieve secrecy of the symmetric decryption keys for each of the citizens because the government will always have access to it. The secret key will not only be encrypted with the citizen's public key but also with the government's public key. The government can then easily decrypt your symmetric decryption key with their secret key. Thus both the police force and the government will have access to the symmetric keys for each of the citizens.

   (b) There are certain scenarios where being able to hide communication content from the government is beneficial, particularly if the citizen's life is at threat. One example is if the citizen is a human rights activist, and may not want the government to know what they are doing or else they may get in trouble. The threat to the society is that everyone will get slightly paranoid about what they communicate over the internet, so effectively the freedom of the citizens will be limited.