CS 458 A3
Name: Xiling Wu
Student #: 20561976
userId: x242wu

Written Response Questions:

1. **Two-time Pad**
    a. xor file generated using python script.
    b. I used crib dragging to determine the original plaintexts.
    I found a website which could take a guessed crib and perform XOR over all segments of the XOR of two encrypted files. Then I manually check all results and see if any result is part of a readable text and guess the complete word and use the word as input and try the previous steps again. I started with " the " and then guessed the word " Austrian ", then " the United States " and so on.
    Website link: https://lzutao.github.io/cribdrag/

2. **RSA**
    a. First convert m1, m2, m3 into decimal number same way as the question c mentioned. Then Eve could calculate (m^e) mod n for each of the three possible m. Then compare the result with the c. If any result match the c value, the m value is the correct message content.
    b. For each of m1, m2, m3(decimal value), multiply 1000. And for value "r" in range 0 ~ 999, add r to the value (e.g. Let m_updated = m1(or m2 or m3) * 1000 + r). Then calculate the result of (m_updated^e) mod n. Compare the result with the "c" value she observed. If any result matches the "c" value, the original m value is the correct message content.
    c. M3 was encrypted to yield c'.
    I created a python script using same approach mentioned in question b). And when r = 641, the result match c'.
    I did noticed that use pow (m_updated, e, n) to calculate "c" is much faster than split the calculation into two steps (power first and modulo next).
    d.
    Step 1: Random choose a value s.
    Step 2: encrypt the value s using Bob's public key, name the ciphertext c2
    Step 3: Create a new ciphertext c3 = c * c2
    Step 4: Send the c3 to Bob and get the plaintext r3
    Step 5: Solve equation: r3 = (r * s) mod n to know r
    Proof:

$$c2 = s^e \bmod n$$

$$r3 = c3^d \bmod n = (c * c2)^d \bmod n = c^d * c2^d \bmod n$$

$$= \left((c^d \bmod n) * (c2^d \bmod n)\right) \bmod n = (r * s) \bmod n$$

3. **Inference Attacks:**
    a.

    Assumption: there exists people born before or at July 2nd and people born after July 2nd(assume July 2nd is the middle of the year).

    Tracker:
    T = SELECT SUM(Bid) FROM Bids WHERE Birthday <= 07/02

    Query:
    q(C or T): SELECT SUM(Bid) FROM Bids WHERE Name = “Miguel” OR Birthday <= 07/02

    q(C or not T): SELECT SUM(Bid) FROM Bids WHERE Name = “Miguel” OR Birthday > 07/02

    q(S): SELECT SUM(Bid) FROM Bids

    q(C) = q(C or T) + q(C or not T) – q(S)

    b. No.

Name	Gender	Age	Medical Item
*	Male	[39-48]	insulin pump
*	Female	[49-58]	thermometer
*	Male	[39-48]	blood pressure monitor
*	Male	[59-68]	blood pressure monitor
*	Female	[49-58]	thermometer
*	Male	[59-68]	insulin pump
*	Female	[49-58]	insulin pump
*	Male	[39-48]	thermometer
*	Male	[59-68]	insulin pump

    The table is 2 diverse. For each quasi-identifier there are two values exists.

4. **Private Information Retrieval:**
    a. Every time striker sends any request (or striker always sends request to acquire every row), the DON.MAC will not process the request content and return the whole inventory matrix back to striker. Then striker could perform the matrix product action locally without letting DON.MAC learn about q.

b.

for any j in $[1..n]$

$Dec_{\hat{k}}(r_j) = Dec_{\hat{k}}(M_{1j} \times Enc_K(q_1) + M_{2j} \times Enc_K(q_2) \cdots)$

According to equation. (4)

$M_{1j} \times Enc_K(q_1) = Enc_K(M_{1j} \times q_1)$

So $Dec_{\hat{k}}(r_j) = Dec_{\hat{k}}(Enc_k(M_{1j} \times q_1) + Enc_K(M_{2j} \times q_2) \cdots)$

According to equation (1)

$Enc_K(M_{1j} \times q_1) + Enc_K(M_{2j} \times q_2) + \cdots Enc_K(M_{mj} \times q_m)$

$= Enc_K(M_{1j} \times q_1 + M_{2j} \times q_2 + \cdots M_{mj} \times q_m)$

So

$Dec_{\hat{k}}(r_j) = Dec_{\hat{k}}(Enc_K(M_{1j} \times q_1 + M_{2j} \times q_2 \cdots M_{mj} \times q_m))$

$= M_{1j} \times q_1 + M_{2j} \times q_2 + \cdots M_{mj} \times q_m$

Since only $q_c = 1$

$Dec_{\hat{k}}(r_j) = M_{cj}$

$Dec_{\hat{k}}(\vec{r}) = [M_{C1}, M_{C2}, \cdots M_{Cn}]$

which is the row the striker wanted to acquire.

5. Government surveillance:

a. Since every citizen will use symmetric key, it means each of the citizen will have decryption key of many other citizens. And due to the character of symmetric decryption, once receiver leaks the key or the key is leaked during the key transportation, all communications send from sender side will be at risk since anyone could get the decryption key and decrypt the message.

b. Citizen should be allowed to hold different positions and ideas from the government. And it should be allowed to discuss the opinion with others privately, otherwise people may be afraid of being punished by government and do not express their opinions even if government did something wrong.