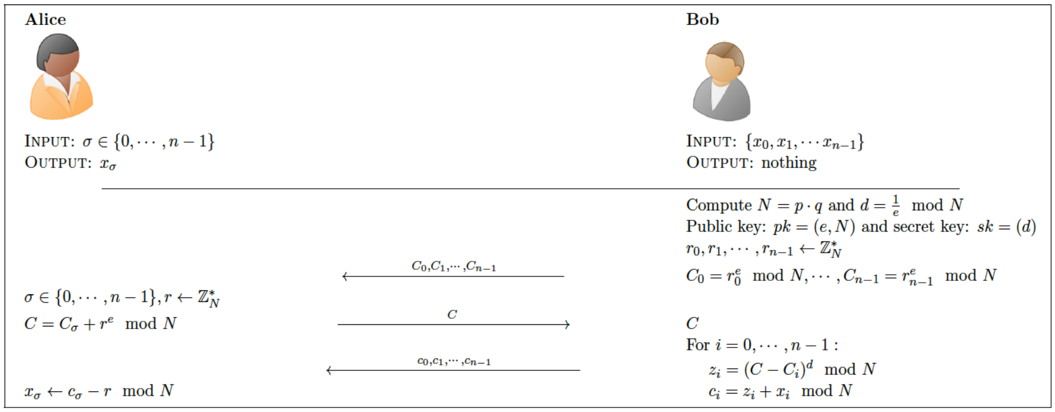
A2. [**50**] Suppose Bob has a set of n numbers $X = \{x_0, x_1, \cdots, x_{n-1}\}$ that are private, and Alice has a private index $\sigma \in \{0, \cdots, n-1\}$. Both Alice and Bob are concerned about their input privacy. Alice wants to obtain the number x_σ for the index σ. The following figure describes a RSA based 1-out-of-n OT protocol that Alice and Bob can use to accomplish the above task. Please implement the 1-out-of-n OT protocol protocol in a single code and submit the source code of your implementation. Please see the last page for the RSA modulus parameters (primes p, q). The RSA encryption scheme is defined as $c = E(pk, m) = m^e \mod N$ and the decryption scheme is defined as $m = D(sk, c) = c^d \mod N$ where $pk = (N, e)$ is the public key and $sk = (p, q, d)$ is the private key.



Alice

INPUT: $\sigma \in \{0, \cdots, n-1\}$
OUTPUT: x_σ

Bob

INPUT: $\{x_0, x_1, \cdots x_{n-1}\}$
OUTPUT: nothing

Compute $N = p \cdot q$ and $d = \frac{1}{e} \mod N$
Public key: $pk = (e, N)$ and secret key: $sk = (d)$
$r_0, r_1, \cdots, r_{n-1} \leftarrow \mathbb{Z}_N^*$
$C_0 = r_0^e \mod N, \cdots, C_{n-1} = r_{n-1}^e \mod N$

$\xleftarrow{C_0, C_1, \cdots, C_{n-1}}$

$\sigma \in \{0, \cdots, n-1\}, r \leftarrow \mathbb{Z}_N^*$
$C = C_\sigma + r^e \mod N$

$\xrightarrow{C}$

C
For $i = 0, \cdots, n-1$:
$z_i = (C - C_i)^d \mod N$
$c_i = z_i + x_i \mod N$

$\xleftarrow{c_0, c_1, \cdots, c_{n-1}}$

$x_\sigma \leftarrow c_\sigma - r \mod N$

Sample I/O:

Please enter n (≥ 2): ______

Print the values in X: ______

Print σ: ______

Print $C_0, C_1, \cdots, C_{n-1}$: ______

Print C: ______

Print $c_0, c_1, \cdots, c_{n-1}$: ______

Print x_σ: ______
