POIS ASSIGNMENT 1

TASK 5

USE THE CPA SECURITY AND SECURE MAC TO DESIGN A PROVABLY CCA-SECURE ENCRYPTION SCHEME

THEORY

MAC :

A message authentication code (MAC) consists of two algorithms (S, V) defined over (K,M, T) where K is the key space, M is the message space, and T is the tag space.
Then, S(k, m) = t ∈ T and V (k, m, t) outputs “yes” or “no.”

A MAC must satisfy the consistency requirement:
∀ k, m : V (k, m, S(k, m)) = ”yes”.

CCA :

A chosen-ciphertext attack (CCA) is an attack model for cryptanalysis where the cryptanalyst can gather information by obtaining the decryptions of chosen ciphertexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption.

Suppose an adversary has a certain ciphertext c that he wants to decrypt. In real life, it is often possible for an adversary to fool the recipient/server into decrypting certain ciphertexts, though not necessarily c. For instance, in the TCP/IP Protocol, the adversary can send a TCP/IP packet and the server will response with an ACK if a certain checksum is correct. By sending such repeated queries, the adversary can learn some information about the plaintext. Thus, we consider a notion of chosen ciphertext security. In particular, the adversary now have the power to obtain the encryption of any message of his choice (CPA) and decrypt any ciphertext of his choice that is not the challenge (CCA). The adversary’s goal is again to break semantic security.

We formalize the chosen ciphertext security model.
Take a cipher E = (E, D) defined over (K,M, C).
For b = {0, 1},

define Exp(b) as follows:

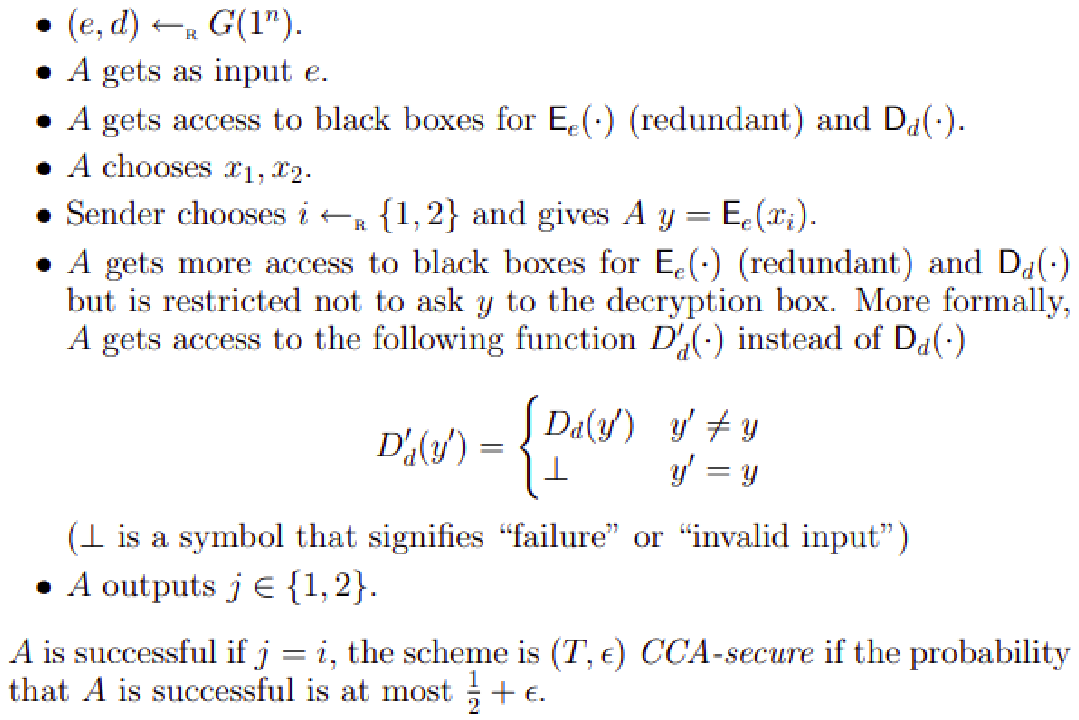
(1) The challenger chooses a k← K

(2) For i = 1, . . . , q, the adversary can submit either a CPA query or a CCA query:

- CPA query: The adversary sends (mi,0, mi,1) ∈ M such that |mi,0| = |mi,1| and receives ci ← E(k, mi,b)
- CCA query: The adversary submits ci ∈ C where ci ∈ { / c1, . . . , ci−1} and receives mi ← D(k, ci)

(3) The adversary then outputs b ′ = {0, 1}.

An encryption (Gen, E, D) is said to be (T,)-CCA secure if it's valid (for every (e, d) = Gen(1n), Dd(Ee(x)) = x) and for every T-time A if we consider the following game:



- $(e, d) \leftarrow_{R} G(1^n)$.
- A gets as input e.
- A gets access to black boxes for $\mathsf{E}_e(\cdot)$ (redundant) and $\mathsf{D}_d(\cdot)$.
- A chooses x_1, x_2.
- Sender chooses $i \leftarrow_{R} \{1, 2\}$ and gives A $y = \mathsf{E}_e(x_i)$.
- A gets more access to black boxes for $\mathsf{E}_e(\cdot)$ (redundant) and $\mathsf{D}_d(\cdot)$ but is restricted not to ask y to the decryption box. More formally, A gets access to the following function $D'_d(\cdot)$ instead of $\mathsf{D}_d(\cdot)$

$$D'_d(y') = \begin{cases} D_d(y') & y' \neq y \\ \perp & y' = y \end{cases}$$

  ($\perp$ is a symbol that signifies "failure" or "invalid input")
- A outputs $j \in \{1, 2\}$.

A is successful if $j = i$, the scheme is (T, ϵ) *CCA-secure* if the probability that A is successful is at most $\frac{1}{2} + \epsilon$.