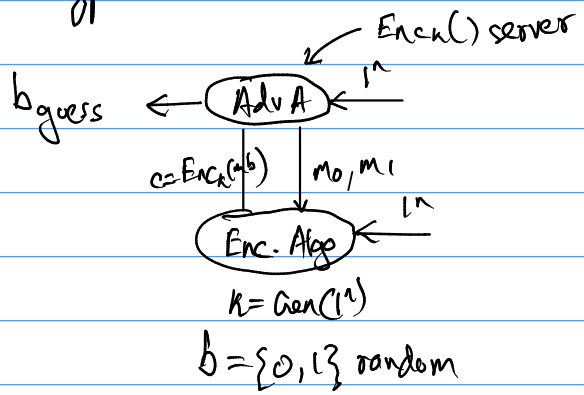
CPA-secure Encryption

In CPA, the adversary has access to the encryption server. As a result, they can try to gain information about the sent message by using the encryption server.



The adversary can distinguish b/w m_0 & m_1 as they can check $Enc(m_0)$ & $Enc(m_1)$ with ciphertext.

We have to use probabilistic encryption algorithms to make CPA-secure systems.

Hence, to construct CPA-secure scheme we use the following method.

- Gen : on input 1^n, $k \leftarrow \{0,1\}^n$ uniformly at random and output as key.
- Enc : on input key k & message m we choose, $r \leftarrow \{0,1\}^n$ at random & output
  $c = \langle r, f_k(r) \oplus m \rangle$ as ciphertext.
- Dec : On input key k & ciphertext $c = \langle r, s \rangle$ we output
  $m = f_k(r) \oplus s$ as message.