Doubt Session 1

1 Q1

$$M = \{0,1\}^n = K, C = \{0,1\}^{n+1}$$
$$enc(m,k) = (m \oplus k, < m, k > \mod 2)$$

Show that this encryption scheme violates the 3^{rd} definition.

Solution: Take $D = U$, $m = 0^n$, $c = 0^n 1$. Now, the RHS is 0 but the conditional has non zero probability. Hence, proved.

2 Q2

Show equivalence between 3^{rd} and 4^{th} definition.

Solution:

($\implies$) Assume by contradiction that definition 4 does not hold for some $m_0 = a$, $m_1 = b$ and $c = c_0$. We now show a distribution D, message x and cipher text c such that the definition 3 fails.

($\Longleftarrow$) Start with RHS of definition 3 and arrive at LHS of the definition. We use the fact that all $P[enc(m_i, k)]$ are equal to complete the result.

3 Q3

Show equivalence between Security Game and 4^{th} definition

Solution:

($\implies$) Can formally write game as

$$\underset{k \in K, b \in \{0,1\}}{P}[A \text{ wins game}] = \frac{1}{2}$$

$$\implies \underset{k \in K, b \in \{0,1\}}{P}[A(enc(m_b, k)) = b] = \frac{1}{2}$$

Since b is uniformly and independently sampled, we get,

$$\implies \underset{k\in K}{P}[A(enc(m_0,k))=0]\times P[b=0]+\underset{k\in K}{P}[A(enc(m_1,k))=1]\times P[b=1]=\frac{1}{2}$$

$$\implies \underset{k\in K}{P}[A(enc(m_0,k))=0]+\underset{k\in K}{P}[A(enc(m_1,k))=1]=1$$

Similarly, since probability of losing is 1/2, we get,

$$\underset{k\in K}{P}[A(enc(m_0,k))=1]+\underset{k\in K}{P}[A(enc(m_1,k))=0]=1$$

We also know the following,

$$\underset{k\in K}{P}[A(enc(m_0,k))=0]+\underset{k\in K}{P}[A(enc(m_0,k))=1]=1$$

$$\underset{k\in K}{P}[A(enc(m_1,k))=0]+\underset{k\in K}{P}[A(enc(m_1,k))=1]=1$$

Subtracting appropriate equations,

$$\underset{k\in K}{P}[A(enc(m_0,k))=0]=\underset{k\in K}{P}[A(enc(m_1,k))=0]$$

$$\underset{k\in K}{P}[A(enc(m_0,k))=1]=\underset{k\in K}{P}[A(enc(m_1,k))=1]$$

4 Q4

$$M=\{0,1\}^l, K=\{0,1\}^n, l>n$$

$$enc(m,k)=m\oplus G(k), G:\{0,1\}^n\to\{0,1\}^l$$

Show that this scheme is not perfectly secure/indistinguishable.

Solution:

Can be done by taking m_0, m_1, c appropriately such that G reveals some information about exactly one of the two thus changing probabilities.