Übung 2, Aufgabe 2)

CPA-Unsicherheit deterministischer Verfahren

geg. Π symmetrisch mit (Gen, Enc, Dec) deterministisch

---

aus der Vorlesung Definition für deterministische Verfahren:

Für alle $k \in K$ und $m \in M$ gilt: $Dec_k(Enc_k(m)) = m$

gleicher Schlüssel, gleiche Nachricht $\Rightarrow$ gleiche Verschlüsselung

aus der Vorlesung WSK für Angreifer:

$$W[CPA_{\Pi}^{Priv}(A) \Rightarrow 1] = \frac{1}{2}\left(W[0 \leftarrow A(Enc_k(m_0))] + W[1 \leftarrow A(Enc_k(m_1))]\right)$$

aus der Vorlesung Definition CPA-Sicherheit:

$$W[CPA_{\Pi}^{Priv}(A) \Rightarrow 1] - \frac{1}{2} \leq 0$$

CPA-Spiel Angreifer Modell

Angreifer mit Orakel-Zugriff

Angreifer $\mathcal{A}$:

1) Generiere $m_0, m_1 \in \mathcal{M}$, wobei $m_0 \neq m_1$ und $|m_0| = |m_1|$

2) Schick m_0, m_1 an CPA-Spiel

3) erhalte c

4) Verschlüssle m_0 mit $Enc_k()$ (durch Orakelzugriff möglich)

$$c_{A_0} := Enc_k(m_0)$$

5) if $(c_{A_0} == c)$
   return 0
   else
   return 1

Erklärung: Angreifer verschlüsselt durch Orakel-Zugriff m_0 mit gleichem k wie im Spiel.
Weil deterministische Verfahren mit gleichem Schlüssel die gleiche Verschlüsselung ausgeben, gelingt dem Angreifer durch Vergleichen, das Spiel zu gewinnen.

Fall $b=0$:

A erhält $c = Enc_k(m_0)$

$c_{A0} = Enc_k(m_0)$

Angreifer gibt $\underline{0}$ aus, weil $c == c_{A0}$

Also $W[0 \leftarrow A(Enc_k(m_0))] = \underline{1}$

Fall $b=1$

A erhält $c = Enc_k(m_1)$

$c_{A0} = Enc_k(m_0)$

Angreifer gibt $\underline{1}$ aus, weil $c \neq c_{A0}$

Also $W[A \leftarrow A(Enc_k(m_1))] = 1$

Daraus folgt:

$$W[CPA_{\Pi}^{Priv}(A) = 1] = \underline{1}$$

$1 > \frac{1}{2} \Rightarrow$ CPA-unsicher

Die WSK vom Angreifer richtig zu raten ist signifikant größer als $\frac{1}{2}$. Heißt: CPA unsicher.