Aufgabe 4

KPA-Sicherheit, Vigenère Chiffre

$$W\left[KPA_{\Pi}^{Priv}(A) \Rightarrow 1\right]$$

$$= W\left[KPA_{\Pi}^{Priv}(A) \Rightarrow \text{[illegible]} \wedge b=0\right] + W\left[KPA^{Priv}(A) \Rightarrow 1 \wedge b=1\right]$$

$$= W\left[KPA_{\Pi}^{Priv}(A) \Rightarrow 1 \mid b=1\right] \cdot \underbrace{W[b=1]}_{\frac{1}{2}} + W\left[KPA_{\Pi}^{Priv}(A) \Rightarrow 0 \mid b=0\right] \cdot \underbrace{W[b=0]}_{\frac{1}{2}}$$

$$= \frac{1}{2}\left(W\left[KPA_{\Pi}^{Priv}(A) \Rightarrow 1 \mid b=1\right] + W\left[KPA_{\Pi}^{Priv}(A) \Rightarrow 1 \mid b=0\right]\right)$$

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

Wenn obige WSK signifikant größer ist als $\frac{1}{2}$, dann ist das Verfahren nicht KPA-sicher

→

Angreifer Modell für das KPA-Spiel

geg.: Vigenère = (Gen, Enc, Dec)

$l, t \in \mathbb{N}$ sei $K = \mathbb{Z}_{26}^t$, $M = C = \mathbb{Z}_{26}^l$

für (Gen, Enc, Dec) siehe Vorlesung 1

$\boxed{t = 5}$ Schlüssellänge, Nachrichtlänge > 5

Angreifer $\mathcal{A}$:

1) $m_0 := ADDDDA\ldots$

2) $m_1 := ABCDEF\ldots$

3) Schick (m_0, m_1) an KPA-Spiel

4) erhalte c

5) if (in c 1. und 6. Buchstabe gleich)

return 0

else

return 1

Erklärung: Da der Schlüssel nur 5 lang ist und die Nachricht ≥ 6, ist für den Angreifer klar, dass z.B.: 1. und 6. Ziffer um den gleichen Wert verschoben wird.

→

Fall $b = 0$:

A erhält $c = Enc_k(ADDDDDA)$

Dann gibt A $\underline{0}$ aus, weil 1. und 6. im Ciphertext gleich

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

Fall $b = 1$:

A erhält $c = Enc_k(ABCDEF)$

Dann gibt A $\underline{1}$ aus, weil 1. und 6. nicht gleich (in c)

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

Daraus folgt: $W[KPA^{Priv}_{Vigenère}(A) = 1]$

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

$$= \frac{1}{2}(1+1) = \underline{1}$$

1 ist signifikant größer als $\frac{1}{2}$. Daher ist die Vigenère Chiffre nicht KPA-sicher.