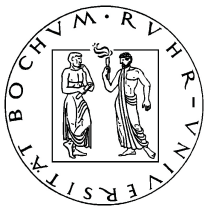
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Thomas Dullien



Präsenzübungen zur Vorlesung

Kryptographie I

WS 2009

Blatt 1 / 19.Oktober 2009

AUFGABE 1:

1. Der folgende Chiffretext ist mit einer monoalphabetischen Verschiebe-Chiffre verschlüsselt und in der deutschen Sprache verfasst. Bestimmen Sie den verwendeten Schlüssel.

   ```
   LMZ DWZABIVLADWZAQBHMVLM LMZ LMCBAKPMV JIVS PIB LQM TIOM
   IV LMV NQVIVHUIMZSBMV ITA EMQBMZPQV NZIOQT JMHMQKPVMB.
   IVOMAQKPBA LMZ LZIUIBQS LMZ DMZOIVOMVMV HEWMTN UWVIBM
   PIMBBM EWPT SICU MQVMZ MZEIZBMB, UQB EMTKPMZ OMAKPEQVLQOSMQB
   ```

2. Betrachten Sie die polyalphabetische Verschiebe-Chiffre. Nehmen Sie an, t sei Ihnen bekannt. Geben Sie einen Algorithmus an, der Ihnen im CPA-Modell den Schlüssel liefert.

AUFGABE 2:

Betrachten Sie die Vernam-Chiffre mit dem Schlüssel $k = 0^\ell$. Da unter diesem Schlüssel $\mathsf{Enc}_k(m) = m$ ist, geht die Nachricht im Grunde unverschlüsselt über die Leitung. Dies ist vermutlich nicht gewollt.
Man könnte jetzt vorschlagen, den Schlüssel $k = 0^\ell$ auszuschliessen. Ist das resultierende Schema immer noch perfekt sicher ? Beweisen Sie.

AUFGABE 3:

Beweisen oder widerlegen Sie: Für ein perfekt sicheres Verschlüsselungsschema gilt, dass für jede Verteilung auf dem Nachrichtenraum $\mathcal{M}$, jedes $m, m' \in \mathcal{M}$ und jedes $c \in \mathcal{C}$:

$$\mathsf{Ws}[M = m | C = c] = \mathsf{Ws}[M = m' | C = c]$$