Lösungen für Sicherheit Übungsblatt 2

Aufgabe 1

Fall 1: Der Initialisierungsvektor wird fest gewählt

Anmerkung: Die Nachrichten sind prinzipiell beliebig.
Wir konstruieren einen erfolgreichen Angreifer auf ein beliebiges Blockchiffre im CBC-Modus mit festem IV. Unser Angreifer läuft folgendermaßen ab:

1. Wir wählen als Nachrichten M_0, das nur aus Nullen besteht, sowie M_1, das nur aus Einsen besteht.
2. Nutze das Orakel, um Enc(K, M_0) sowie Enc(K, M_1) zu berechnen.
3. Verschlüssele eine zufällige der beiden Nachrichten mit dem Verschlüsselungsalgorithmus.
4. Nach Konstruktion muss das Chiffrat, das der Angreifer erhält, genau eines der zwei sein, die er vorher berechnet hat. Gebe den dazu gehörigen Klartext aus.

Dieser Angreifer gewinnt das IND-CPA-Spiel immer.

Fall 2: IV wird fest gewählt und bei jeder Verschlüsselung um 1 hochgezählt.

Anmerkung: ˜(W) bezeichne das bitweise Komplement eines Bitstrings W
Wir konstruieren einen Angreifer auf ein beliebiges Blockchiffre im CBC-Modus mit konstanter IV-Wahl, der bei jedem Verschlüsselungsvorgang um 1 erhöht wird.

1.
2.

Aufgabe 2

Aufgabe 3

Aufgabe 4

1. WPA 2 (benutzt AES):

- Blockchiffre
- Counter Mode with CBC-MAC (CTR)
- IV im Klartext in der Nachricht: IV = Priorität (immer 0, noch), Padding, MAC-Source-Address, Package Number
- Schlüssel: Pre-shared key, den jede Station von vornherein kennen muss. Daraus werden temporäre Schlüssel berechnet die dann zur Verschlüsselung benutzt werden.