06.04.2021

Dr. Felix Heuer
fheuer.lba@fh-salzburg.ac.at

Kryptographie und Mediensicherheit

Sommersemester 2021

Übungszettel 3

Abgabe: 20.04.2021 vor der Vorlesung

1 Aufgabe (10 Punkte)

a) Geben Sie für den CBC-Mode eine Entschlüsselungsfunktion an und zeigen Sie, dass der CBC-Mode mit ihrer Entschlüsselungsfunktion korrekt ist.

b) Geben Sie für den OFB-Mode eine Entschlüsselungsfunktion an und zeigen Sie, dass der OFB-Mode mit ihrer Entschlüsselungsfunktion korrekt ist.

c) Geben Sie für den CTR-Mode die korrekte Entschlüsselungsfunktion an.

2 Aufgabe (10 Punkte)

Erstellen Sie eine komplette tabellarische Übersicht über die Modes of Operation

- CBC-Mode
- OFB-Mode
- CTR-Mode

zu den Eigenschaften

- Benötigt Invertierbarkeit von F für die Korrektheit, d.h. F muss PRF. bzw. PRP sein?
- Größe der Ciphertextexpansion?
- Sind Vorberechnungen vor Kennen der Nachricht möglich? Falls ja, welche?
- Sind Teile der Ver-/Entschlüsselung parallelisierbar? Falls ja, welche?

Welcher Modus ist Ihrer Meinung nach die beste Wahl? Warum?

3 Aufgabe (10 Punkte)

In dieser Aufgabe wird das Geburtstagsparadoxon behandelt. Der Name stammt daher, dass man erstaunlich wenig Personen in einer Gruppe haben muss, damit wenigstens zwei Personen dieser Gruppe mit hoher Wahrscheinlichkeit am gleichen Tag Geburtstag haben. (Ab 23 Personen bereits über 50% Wahrscheinlichkeit.)

Allgemeiner formuliert trifft das Geburtstagsparadoxon eine Aussage darüber, mit welcher Wahrscheinlichkeit Ausgaben einer sich zufällig verhaltenden Funktion kollidieren, man also für unterschiedliche Eingaben, die gleiche Ausgabe erhält.
Das Geburtstagsparadoxon besagt, dass bei einer Funktion mit zufällig, gleichverteilten Ausgaben im Intervall $[1, N]$ mit hoher Wahrscheinlichkeit eine Kollision der Ausgabewerte auftritt, wenn die Funktion circa $\sqrt{2N}$ mal ausgewertet wurde. Im eingehenden Beispiel wäre etwa $N = 365$ und die Funktion die Abbildung „Person“→ „Geburtstag von Person“.

Kollisionen sind eine Gefahr für die Sicherheit und müssen vermieden werden!

Beispiel: Angenommen es gibt bei Verwendung des CBC-Mode bei gleichem Schlüssel eine Kollision der Ausgaben: $c_i = c_j$ für zwei Ciphertextblöcke. Dann gilt

$$\begin{aligned} & c_i = c_j \\ \Leftrightarrow \quad & \mathsf{F}_k(c_{i-1} \oplus m_i) = \mathsf{F}_k(c_{j-1} \oplus m_j), \text{ Definition CBC-Mode} \\ \Leftrightarrow \quad & c_{i-1} \oplus m_i = c_{j-1} \oplus m_j, \text{ da } \mathsf{F} \text{ Permutation ist} \\ \Leftrightarrow \quad & m_i \oplus m_j = c_{i-1} \oplus c_{j-1} \end{aligned}$$

D.h. die Kollision verrät unmittelbar das xor der Nachrichtenblöcke m_i und m_j!

a) Wählen Sie $N = 10.000, 20.000, \ldots, 990.000, 1.000.000$. Für jede Wahl von N mitteln Sie über 20 Durchläufe, wie viele Werte Sie gleichverteilt aus $[1, N]$ ziehen mussten, um die erste Kollision zu erhalten. Plotten Sie die benötigten Werte in Abhängigkeit von N.

b) Passen Ihre experimentellen Daten zur Aussage, dass man nach ungefähr $\sqrt{2N}$ Werten mit einer Kollision rechnen muss?

c) Es soll untersucht werden, wie viele Daten verarbeitet werden können, bis die Gefahr einer Kollision und damit für die verschlüsselten Nachrichten besteht. Nehmen Sie an, dass die Ausgaben von AES gleichverteilt sind. Wie viel Daten können Sie mit AES im CBC-Mode unter gleichem Schlüssel verschlüsseln, bevor eine Kollision der Ausgabeblöcke befürchtet werden muss? (Angabe bitte nicht in Bit, sondern in GB/TB/..., je nach Größe)

4 Aufgabe (10 Punkte)

Diese Aufgabe zeigt, dass kleine Modifikationen an sicheren Konstruktionen sehr gefährlich sein können und diese komplett unsicher machen können. Dazu betrachten wir die folgende Variante des CTR-Modus:

Sei F eine PRP mit $\mathsf{F}\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. Dann definieren wir das symmetrische Verschlüsselungsverfahren Π_{nope} als:

Gen: $k \leftarrow \{0,1\}^n$. Gib k aus.

Enc: Für $m = m_0 \ldots m_{\ell-1}$ mit $m_i \in \{0,1\}^n$ ziehe zunächst $IV \leftarrow \{0,1\}^n$. Berechne dann $c_i = \mathsf{F}_k(m_i \oplus (IV + i))$ für $i = 0, \ldots, \ell - 1$. Gib $(IV, c_0, c_1, \ldots, c_{\ell-1})$ aus.

D.h. wie beim CTR-Modus wird der IV hochgezählt, aber hier wird die Nachricht nicht auf IV gexort *nachdem* dieser durch F_k ausgewertet wurde, sondern *davor*.

a) Zeichnen Sie sich diesen Mode of Operation auf, wie es in der Vorlesung für die anderen Modi gemacht wurde.

b) Geben Sie eine Entschlüsselungsfunktion Dec an und zeigen Sie die Korrekheit von Π_{nope}.

c) Zeigen Sie, dass Π_{nope} nicht mal KPA-sicher ist.

Hinweis zur Notation: Die Nachrichten im KPA-Spiel sollten sie vielleicht m^0, m^1 nennen, da diese in diesem Fall selbst aus Nachrichtenblöcken der Länge n bestehen. Diese könnten sie z.B. als $m^0 = m^0_0, \ldots, m^0_{\ell-1}$ bezeichnen.