Kryptografie und -analyse, Übung 8

Henry Haustein

Betriebsarten

(a) Die Blöcke c_1 bis c_{i-1} können ohne Probleme entschlüsselt werden. Der Block c_i kann nicht entschlüsselt werden, er wurde ja gelöscht. Für den Block c_{i+1} muss folgendes berechnet werden: $m_{i+1} = \text{dec}(k, c_{i+1}) \oplus c_i$, was nicht geht. Ab Block c_{i+2} kann wieder alles entschlüsselt werden, $c_{i+2} = \text{dec}(k, c_{i+2}) \oplus c_{i+1}$.

(b) Ja, man kann unterschiedliche IVs auf Sender- und Empfängerseite verwenden. Auf Senderseite wird verschlüsselt:

- $c_1 = \text{enc}(k, m_1 \oplus IV_S)$
- $c_2 = \text{enc}(k, m_2 \oplus c_1)$

Auf Empfängerseite wird entschlüsselt:

- $m_1 = \text{dec}(k, c_1) \oplus IV_E \Rightarrow$ klappt nicht
- $m_2 = \text{dec}(k, c_2) \oplus c_1 \Rightarrow$ funktioniert

Bei CFB ist die Beeinflussung länger, nämlich $\lceil \frac{l}{r} \rceil$, bei OFB geht das gar nicht, weil nur der IV immer wieder verschlüsselt wird. Ist der IV anders, so werden eine völlig andere Pseudo-Schlüssel generiert mit denen die Nachricht $\oplus$ wird.

(c) $m = 128$ Bit, Blocklänge 64 Bit, $r = 8$ Bit. Bei CBC wird die Verschlüsselungfunktion zwei mal aufgerufen, weil es 2 Blöcke gibt. Bei CFB kommt es auf r an, hier wird die Verschlüsselungfunktion $\frac{128}{8} = 16$ mal ausgeführt.

(d) Es gilt:

	Direktzugriff	**Parallelisierbarkeit**	**Vorausberechnung**
ECB	ja	ja	nein
CBC	enc: nein, dec: ja	enc: nein, dec: ja	nein
CFB	ähnlich CBC	ähnlich CBC	nein (nur 1 Block)
OFB	wenn Schlüsselblöcke nicht gespeichert werden: nein	wenn Schlüsselblöcke nicht gespeichert werden: nein	ja
CTR	ja	ja	ja

(e) Direktzugriff: ob eine Abhängigkeit von vorherigen Cipherblöcken/Klartextblöcken vorliegt.
Parallelisierbarkeit: wenn Direktzugriff vorliegt
Vorausberechnung: ob Verschlüsselung auf Klartextblöcke oder Schlüsselblöcke angewendet wird

Grundlagen

(a) $\mathbb{Z}_{77}^* = \{a \in \mathbb{Z}_{77} \mid \text{ggT}(a, 77) = 1\}$. Offensichtlich $\text{ggT}(20, 77) = 1$ und $\text{ggT}(14, 77) = 7$ und $20^{-1} = 27$ mit WolframAlpha (`20^ -1 mod 77`)

(b) Satz von Lagrange: Wenn H Untergruppe von G, dann $\text{ord}(H) \mid \text{ord}(G)$, damit haben die Untergruppen von $\mathbb{Z}_{13}^*$ die Ordnungen 1, 2, 3, 4, 6 und 12 (die Ordnung von $\mathbb{Z}_{13}^*$ ist $\Phi(13) = 12$).

(c) Primfaktorzerlegung von Gruppenordnung: $12 = 2^2 \cdot 3$. Für $a_1 = 5$:

- $b = a_1^{\frac{n}{p_1}} = 5^{\frac{12}{2}} = 5^6 \equiv 12 \mod 13$
- $b = a_1^{\frac{n}{p_2}} = 5^{\frac{12}{3}} = 5^4 \equiv 1 \mod 13$

Für $a_2 = 6$:

- $b = a_2^{\frac{n}{p_1}} = 6^{\frac{12}{2}} = 6^6 \equiv 12 \mod 13$
- $b = a_2^{\frac{n}{p_2}} = 6^{\frac{12}{3}} = 6^4 \equiv 9 \mod 13$

$\Rightarrow a_1 = 5$ ist kein Generator, $a_2 = 6$ ist ein Generator.

(d)