2.1 Bitblockchiffren – Einleitung

Beschreibung

Bitblock-Chiffren arbeiten über dem Alphabet $\Sigma = \mathbb{F}_2 = \{0, 1\}$ und verschlüsseln zunächst Blöcke fester Länge längentreu; sie sind also auf dem Vektorraum $\mathbb{F}_2^n$ definiert mit Schlüsselraum $\mathbb{F}_2^l$. Die Fortsetzung auf Bitketten beliebiger Länge ist Thema des Abschnitts „Betriebsarten“ und kümmert uns vorläufig nicht, ebensowenig wie die Frage, wie man zu kurze Blöcke auffüllt („Padding“).

Achtung: Der Buchstabe n bezeichnet jetzt bis auf weiteres nicht mehr die Größe des Alphabets, sondern die Länge der Bitblöcke.

Man kann eine Bitblock-Chiffre auch als monoalphabetisch über dem Alphabet $\Sigma' = \mathbb{F}_2^n$ ansehen. Zur Konstruktion und Beschreibung wird meist die algebraische Struktur als n-dimensionaler Vektorraum über dem Körper $\mathbb{F}_2$ verwendet, gelegentlich die als Körper $\mathbb{F}_{2^n}$, nur selten die als zyklische Gruppe der Ordnung 2^n.

Eine solche Chiffre wird also beschrieben durch eine Abbildung

$$F\colon \mathbb{F}_2^n \times \mathbb{F}_2^l \longrightarrow \mathbb{F}_2^n$$

bzw. als Familie $(F_k)_{k\in K}$ von Abbildungen

$$F_k\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n \quad \text{für alle } k \in K = \mathbb{F}_2^l.$$

Wahl der Blocklänge

Die Blocklänge soll groß genug sein, um die Verfahren zum Brechen monoalphabetischer Substitutionen, insbesondere Muster- und Häufigkeitsanalysen, unmöglich zu machen; besser ist es, jede Art von Informationspreisgabe über den Klartext, z. B. jede Wiederholung im Geheimtext, zu vermeiden.

Bei einer **Codebuch-Attacke** würde der Angreifer bekannte Klartext-Geheimtextpaare bei festem Schlüssel sammeln, sich also sozusagen sein eigenes Codebuch anlegen. Ein vollständiges Codebuch führt, selbst wenn der Schlüssel sich daraus nicht bestimmen lässt, zu einer vollständigen Entschlüsselung. Konsequenzen:

- $\#\Sigma' = 2^n$ sollte größer als die Zahl der im ungünstigsten Fall verfügbaren Speicherplätze sein.
- Der Schlüssel sollte oft genug gewechselt werden.

Wegen des Geburtstagsphänomens sind allerdings strengere Kriterien sinnvoll: Falls der Gegner ca. $\sqrt{\#\Sigma'} = 2^{n/2}$ Klartext-Geheimtextpaare in

seinem Codebuch gesammelt hat, ist die Wahrscheinlichkeit einer Kollision schon etwa $\frac{1}{2}$. Daher sollte diese Zahl, also $2^{n/2}$ bei einer Bitblock-Chiffre, schon die Zahl der verfügbaren Speicherplätze überschreiten; und auch Schlüssel sollten oft genug gewechselt werden – deutlich vor dieser Anzahl verschlüsselter Blöcke.

Die bisher meist verwendete Blocklänge 64 ist so gesehen also schon bedenklich; sie ist allenfalls noch bei häufigem Schlüsselwechsel zu rechtfertigen. Besser ist eine Blocklänge von 128 Bit, wie sie auch im neuen Standard AES vorgesehen ist.

Diese Überlegung ist ein typische Beispiel für die Sicherheitsabwägungen in der modernen Kryptographie: Es wird mit breiten Sicherheitsabständen gearbeitet; erkennbare Schwächen werden vermieden, selbst wenn sie noch weit von einer praktischen Auswertbarkeit für den Gegner entfernt sind. Da es effiziente Verfahren gibt, die diese Sicherheitsabstände einhalten, besteht überhaupt keine Notwendigkeit, weniger strenge Verfahren einzusetzen.