

Security

Sommersemester 2022

(LV 4120 und 7240)

9. Aufgabenblatt

Ziel des folgenden Aufgabenblatts ist es, eine Hillchiffre zu implementieren und den zugrundeliegenden Algorithmus zu analysieren.

Aufgabe 9.1

- a) Entwickeln und implementieren Sie in der Programmiersprache C eine Applikation für eine (3x3)-Matrix Hill-Chiffre in Form einer multiplikativen Tauschchiffre $E : \{0, 1\}^{64} \times \{0, 1\}^{64} \rightarrow \{0, 1\}^{72}$ mit $\mathbf{C} = (\mathbf{K} \cdot \mathbf{P}) \bmod n$ gemäß dem in Vorlesung betrachteten Verfahren. Realisieren Sie sowohl die Verschlüsselungs- als auch die Entschlüsselungsfunktion `hillverH33()` bzw. `hillentH33()`. Für die Invertierbarkeit der Chiffre wird die Bedingung $\text{ggT}(\det \mathbf{K}, n) = 1$ vorausgesetzt. Die Matrizen \mathbf{C} , \mathbf{K} und \mathbf{P} betrachten wir jeweils als 3x3-Matrix mit jeweils 9 Elementen. Jedes Element hat eine Länge von einem Byte.

$$\mathbf{X} = \begin{pmatrix} X_{1,1} & X_{1,2} & X_{1,3} \\ X_{2,1} & X_{2,2} & X_{2,3} \\ X_{3,1} & X_{3,2} & X_{3,3} \end{pmatrix}$$

Matrix-Form \mathbf{X} für \mathbf{C} , \mathbf{K} , \mathbf{P}

Das Feldelement $x_{2,2}$ wählen wir sowohl bei der Schlüsseltextmatrix \mathbf{K} als auch bei der Klartextmatrix \mathbf{P} als Prüffeld (Addition mod n) zur Absicherung der übrigen Elemente der Matrix gegenüber eventuellen Übertragungs- oder Berechnungsfehler, so dass sich mit diesem Verfahren eine Blocklänge von 8×8 Bit = 64 Bit erzielen lässt. Für die Berechnung des Feldelements $x_{2,2}$ biete sich an:

$$x_{2,2} = (x_{1,1} \oplus x_{1,2} \oplus x_{1,3} \oplus x_{2,1} \oplus x_{2,3} \oplus x_{3,1} \oplus x_{3,2} \oplus x_{3,3}) \bmod n;$$

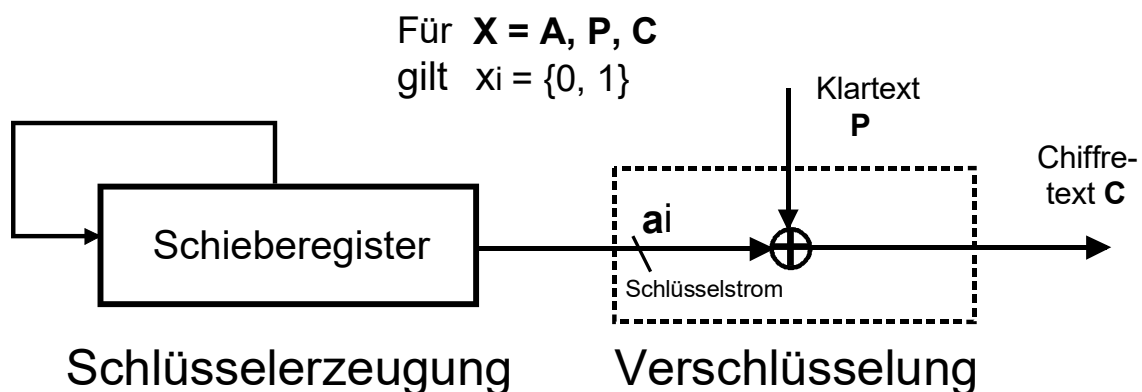
Der verwendete Zeichensatz sei $\{a..z, |, !, :, -, ?\}$ und alle Berechnungen seien im Restklassenring \mathbb{Z}_{31} auszuführen.

- b) Ermitteln Sie unter Verwendung Ihres Programms für das 24 Zeichen lange Klartextpasswort `lestershlestersh:pass-rm` und den 8 Zeichen langen Schlüsseltext `hillkey!` den entsprechenden 24 Zeichen langen Ciphertext.

- c) Wie lautet die entsprechende Dechiffrierfunktion und welche Matrizen müssen zum Entschlüsseln verwendet werden?
- d) Ist durch die Wahl des Schlüsseltextes die Umkehrbarkeit der Chiffre gewährleistet? Begründen Sie Ihre Antwort.

Aufgabe 9.2

Bei einer binären Strom-Chiffre werden Klartext und Schlüssel modulo 2 addiert, um den Chiffretext zu erhalten. Umgekehrt werden zur Entschlüsselung Chiffretext und Schlüssel modulo 2 addiert. Eine besonders einfache Realisierung dieses Verfahrens (der "heiße Draht" zwischen Washington und Moskau soll auf diesem Prinzip basieren) mit Schieberegisterschaltungen und XOR-Schaltkreisen zeigt das folgende Prinzipschaltbild:



Bei der weiteren Betrachtung nehmen wir an, dass es sich um ein 4stufiges lineares Schieberegister handelt.

- a) Welcher Schlüsselstrom ist erforderlich, um die Klartextfolge $\{1, 0, 1, 1, 0, 1, 1, 1\}$ in die Chiffrefolge $\{1, 0, 1, 0, 0, 1, 0, 0\}$ abzubilden?
- b) Wie lautet der Startvektor des verwendeten Schieberegisters?
- c) Ermitteln Sie die zugrundeliegende Rückkopplungsstruktur des Schieberegisters.
- d) Skizzieren Sie die vollständige Schaltung des Verschlüsslers sowie des entsprechenden Entschlüssers.
- e) Was gilt es in bezug auf Synchronisation zu beachten?

Aufgabe 9.3

Gegeben sei eine Hash-Funktion H , die 10^8 unterschiedliche Hash-Werte erzeugen kann, z. B. Zahlen aus dem Intervall von 0 bis 99 999 999.

- a) Weiterhin sei eine Nachricht M mit Hash-Wert $H(M)$ gegeben. Wie viele Nachrichten müssen Sie erzeugen, um mit einer Wahrscheinlichkeit größer als $1/2$ eine Nachricht mit demselben Hash-Wert $H(M)$ zu erhalten?
- b) Was ist eine Kollision bei Hash-Werten und wieso gibt es überhaupt Kollisionen?

Aufgabe 9.4

- a) Entwickeln und implementieren Sie eine C-Funktion `hash(m)`, die zu einer einzulesenden Textdatei bzw. einer beliebig langen Nachricht `m` einen Fingerabdruck in Form eines Hashwertes `h(m)` erzeugt, der eine feste Länge von 56 Bit ausweist. Bei der Konstruktion des Hashalgorithmus werden jeweils 8 Zeichen der eingelesenen Nachricht `m` zu einem Block `mi` ($i = 0, 1, \dots, M$) mit der Länge von 8 Byte zusammengefasst und gemäß folgendem Algorithmus verarbeitet:

Wiederhole für alle Eingabetextblöcke `i` mit $0 \leq i < M$

`mi := block(z0 z1 z2 ... z7);`

`mM := block(z0 z1 z2 ... z5 '\0' '\0');`

`c0 = (m0)k mod n ;`

Wiederhole für alle Eingabetextblöcke `i` mit $0 < i \leq M$

`ci = (mi ⊕ ci-1)k mod n ;`

Output `h(m) = cM ;`

Dabei wird der zuletzt berechnete Block `cM` als Hashwert der Nachricht `m` aufgefasst. Die beiden Sonderzeichen der Textdatei LF (`\n`) und EOF werden mit dem Wert 10 für `\n` bzw. 127 für EOF in die Berechnung des Hashwertes miteinbezogen. Falls ein Auffüllen (Pad) des letzten Blockes `mM` erforderlich ist, um auf eine Blocklänge von 8 Zeichen zu kommen, erfolgt dies mit dem Zeichen '0' bzw. ASCII-Wert 48 von rechts (LSB) nach links (MSB). Die Parameter dieses Hash-Algorithmus sind `n` und `k`. Sie sind für die Kollisionsresistenz von entscheidender Bedeutung.

Wir interpretieren die Zeichen der Textdatei als 7-Bit-ASCII im Wertebereich von 0 bis 127 (dezimal) bzw. 0 bis 7F (hexadezimal) und wenden folgende Zahleninterpretation für den Wert eines Blockes an.

$$\text{Wert}(m_i) = z_0 \cdot 2^{49} + z_1 \cdot 2^{42} + \dots + z_6 \cdot 2^7 + z_7$$

bzw. für $0 \leq i < M$

$$\text{Wert}(m_i) = z_0 \lll 49 + z_1 \lll 42 + \dots + z_6 \lll 7 + z_7$$

und für den letzten Block `mM`:

$$\text{Wert}(m_M) = z_0 \cdot 2^{49} + z_1 \cdot 2^{42} + \dots + \backslash n \cdot 2^{21} + \text{EOF} \cdot 2^{14} + '\0' \cdot 2^7 + '\0'$$

Zwischenräume (Leerzeichen) werden mit dem Wert 32 berücksichtigt.

- b) Ermitteln Sie für den Wert der folgenden Eingabetexte im UTF-8-Format den 56 Bit Hashwert als Dezimal- und Hexadezimalwert (einschließlich der beiden Steuerzeichen LF und EOL). Parameter sind `k = 17` und `n = 72.057.594.037.927.935`.

Eingabetext	56 Bit Hashwert (dezimal und hexadezimal)	AZ
12345678		
123456789		
01234567		

AZ: Anzahl Zeichen (einschließlich `\n` und `EoF`)