Kombination zweier Verfahren

Moderne symmetrische Blockchiffreverfahren basieren auf mehreren Verschlüsselungsrunden, in denen verschiedene Verschlüsselungsverfahren kombiniert werden. Wir wollen im Folgenden beispielhaft zunächst eine willkürliche Kombination der beiden vorher beschriebenen Verfahren untersuchen. Als Klartext soll das Wort TOLL verschlüsselt werden. Wir treffen für unser Beispiel folgende (willkürliche) Entscheidungen:

Reihenfolge: erst XOR-Verfahren, dann Permutation

Blocklänge: 16 Bit

Schlüsselwort: 1110 0101 1111 0111

Binärcodierung: ASCII-Code

Schlüsselwort Permutation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 13 & 7 & 15 & 10 & 3 & 6 & 8 & 12 & 1 & 5 & 14 & 2 & 16 & 4 & 11 & 9 \end{pmatrix}$$

XOR-Verschlüsselung:

Klartext	**T**	**O**	**L**	**L**
ASCII-Code	0101 0100	0100 1111	0100 1100	0100 1100
Schlüssel	1110 0101	1111 0111	1110 0101	1111 0111
Geheimtext				

Permutationen:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 13 & 7 & 15 & 10 & 3 & 6 & 8 & 12 & 1 & 5 & 14 & 2 & 16 & 4 & 11 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 13 & 7 & 15 & 10 & 3 & 6 & 8 & 12 & 1 & 5 & 14 & 2 & 16 & 4 & 11 & 9 \end{pmatrix}$$

Aufgabe:

1) Führen Sie das Verfahren (erst XOR, dann Permutation) einmal durch.

Durch die Kombination beider Verfahren wird eine Konfusion zum Teil erreicht. Allerdings sorgt auch die Kombination nicht für eine Diffusion: ändert man ein Bit des Klartextes, so ändert sich auch nur ein Bit des Geheimtextes. Auch bleiben Änderungen immer nur innerhalb eines Abschnittes, d.h. Bits des Abschnittes TO bleiben in diesem Abschnitt und Bits des Abschnittes LL im zweiten Abschnitt. Gesucht ist eine Möglichkeit, bei Änderung eines Bits eines Abschnitts Änderungen in mehreren Abschnitten des Geheimtextes zu erreichen. Denken Sie zunächst selbst über mögliche Lösungen hierzu nach, bevor Sie weiterlesen.

Feistel-Netzwerke

Feistel-Netzwerke bilden die Grundlage vieler moderner symmetrischer Blockchiffreverfahren. Sie wurden von Horst Feistel Anfang der 70er Jahre entwickelt. Das Grundprinzip von Feistel-Netzwerken ist:

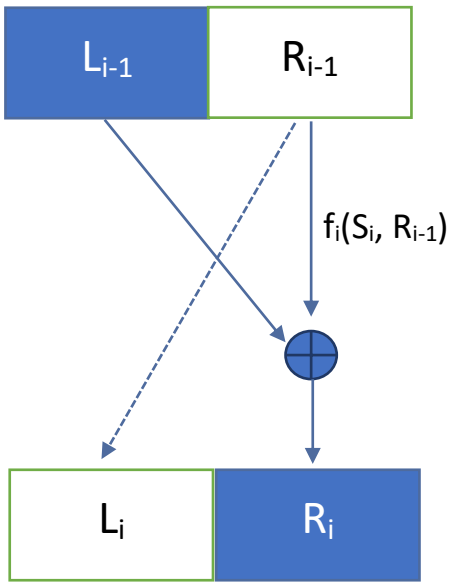
- Die Verschlüsselung erfolgt blockweise. Je länger die Blöcke, desto sicherer ist das Verfahren.
- Die Verschlüsselung erfolgt in mehreren aufeinander folgenden Runden. In jeder Runde wird ein anderer Schlüssel verwendet, diese Rundenschlüssel lassen sich aus einem Anfangsschlüssel ableiten.
- Zur Verschlüsselung werden Substitutions- und Transpositionsverfahren kombiniert. Diese Verfahren sind häufig „hardwarenah" realisierbar (XOR-Verfahren, Verschiebungen etc.).
- Durch die geschickte Kombination verschiedener Verfahren und die Durchführung mehrerer Runden wird für eine möglichst große Diffusion und Konfusion gesorgt.

Die Verschlüsselung durch mehrere Runden oder die Kombination verschiedener Verfahren führen nicht zwangsläufig zu mehr Sicherheit bzw. großer Diffusion und Konfusion. Ein Gegenbeispiel haben Sie bereits bei der Hintereinanderausführung einer XOR-Verschlüsselung mit einer Permutation kennengelernt.

Aufgabe

2) Untersuchen Sie, ob und wenn ja wie sich die Sicherheit verändert, wenn man einen Text mehrfach hintereinander mithilfe des Vigenère-Verfahrens verschlüsselt.

In Feistel-Netzwerken wird für eine Erhöhung der Diffusion gesorgt, indem in jeder Runde Teile des Blocks so miteinander kombiniert werden, dass manche Eingangsbits mehrere Ergebnisbits beeinflussen. Das grundlegende Schema der i-ten Runde ist wie folgt:

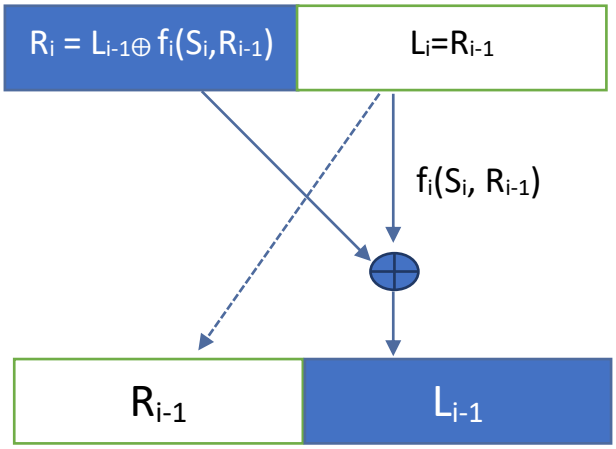
Jeder Block wird in zwei (gleich große) Hälften geteilt. Zu Beginn der Runde bezeichnen wir die linke Hälfte mit L_{i-1}, die rechte mit R_{i-1}.	
Der rechte Block wird mittels des Rundenschlüssels S_i und der gewählten Rundenfunktion f_i verschlüsselt. Anschließend wird das Ergebnis z.B. mittels XOR mit dem linken Block verknüpft. Auf diese Weise sorgt man für Konfusion. Das Ergebnis bildet den neuen rechten Block R_i.	
Der neue linke Block L_i ist der ursprüngliche rechte Block R_{i-1}. Auf diese Weise beeinflusst jedes Bit des alten Blocks R_{i-1} mindestens zwei Bits des neuen Gesamtblocks L_iR_i und man sorgt für Diffusion.	

Aufgaben

3) Begründen Sie, warum eine Erhöhung der Rundenanzahl zu einer Erhöhung der Diffusion und Konfusion führt.
4) Der neue Block R_i entsteht durch eine Verknüpfung von $f_i(S_i,R_{i-1})$ mit dem linken Block L_{i-1}. Untersuchen Sie, ob auf die Verschlüsselung mittels einer Rundenfunktion f_i verzichtet werden kann und anstatt dessen nur die XOR-Verknüpfung beider Blöcke ausreicht.

Entschlüsselung in Feistel-Netzwerken

Zur Entschlüsselung müssen zunächst L_i und R_i getauscht und der Rundenzähler um 1 reduziert werden. Im Anschluss können rundenweise die gleichen Operationen durchgeführt werden, lediglich der Rundenzähler muss um 1 reduziert werden. Anschließend müssen die beiden Blöcke erneut getauscht werden:



Zur Entschlüsselung muss die Rundenfunktion f nicht umkehrbar sein, stattdessen wird das Verfahren im Prinzip pro Runde erneut durchgeführt.

5) Begründen Sie kurz, warum man so vorgehen kann.

Ausblick: AES

Ein aktuelles symmetrisches Blockchiffreverfahren ist das sogenannte AES-Verfahren (Advanced Encryption Standard). Darin werden inzwischen Schlüssellängen von 128, 192 oder 256 Bit verwendet. Es besteht wie Feistel-Netzwerke auch aus mehreren Runden, deren Kombination für möglichst hohe Konfusion und Diffusion sorgen. Unter https://www.cryptool.org/de/cto/aes-step-by-step (Link vom 22.04.2021) kann das AES-Verfahren schrittweise untersucht und die Abhängigkeit eines Ergebnisbits von verschiedenen Eingangsbits veranschaulicht werden.