XOR-Verschlüsselung

Bestandteil vieler moderner Blockchiffreverfahren ist die sogenannte XOR-Verschlüsselung. Dazu wird ein Klartext zunächst binär codiert. Anschließend wird jedes Bit des Klartextes mit dem zugehörigen Bit des Schlüssels mittels XOR verknüpft. XOR bedeutet „Entweder-Oder“, d.h. es ergeben sich die folgenden Kombinationen:

Klartextbit	Schlüsselbit	Geheimtextbit
0	0	0
0	1	1
1	0	1
1	1	0

Beispiel

Der Klartext HALLO soll mittels XOR-Blockchiffre verschlüsselt werden. Wir treffen für unser Verschlüsselungsverfahren folgende (willkürliche) Entscheidungen:

Blocklänge: 16 Bit

Schlüsselwort: 0101 1011 0001 0011

Binärcodierung: Jeder Buchstabe wird gemäß der ASCII-Tabelle binär codiert. D.h. A entspricht 0100 0001, B entspricht 0100 0010, C entspricht 0100 0011 usw.

Damit ergibt sich folgende Verschlüsselung des Wortes HALLO:

Klartext	**H**	**A**	**L**	**L**	**O**
ASCII-Code	0100 1000	0100 0001	0100 1100	0100 1100	0100 1111
Schlüssel	0101 1011	0001 0011	0101 1011	0001 0011	0101 1011
Geheimtext	0001 0011	0101 0010	0001 0111	0101 1111	0001 0100

Aufgaben

1) Verschlüsseln Sie zu den Festlegungen im Beispiel (Schlüsselwort 0101 1011 0001 0011) den Klartext BLUME. Entschlüsseln Sie außerdem den Geheimtext
0001 1101 0101 0110 0000 1001 0101 1010 0001 1110 0101 1101

2) Begründen Sie, warum man bei der XOR-Verschlüsselung den Geheimtext entschlüsseln kann, indem man ihn erneut mit dem Schlüssel verschlüsselt.

3) Entscheiden Sie, ob es sich bei dem Verfahren um ein Substitutions- oder Transpositionsverfahren handelt.

CC BY NC SA

4) Für die Verschlüsselung benötigt man möglichst zufällige Schlüsselwörter. Implementieren Sie in einer im Unterricht verwendeten Programmiersprache eine Operation `schluesselgenerieren`. Diese gibt zu einer als Parameter übergebenen Länge einen zufällig erzeugten Binärcode zurück.

5) In Abbildung 1 ist das Struktogramm einer Operation `dezimalZudual` dargestellt. Geben Sie die Rückgabewerte von `dezimalZudual(65)` und `dezimalZudual(122)` an. Beschreiben Sie die Funktionalität der Operation `dezimalZudual`.

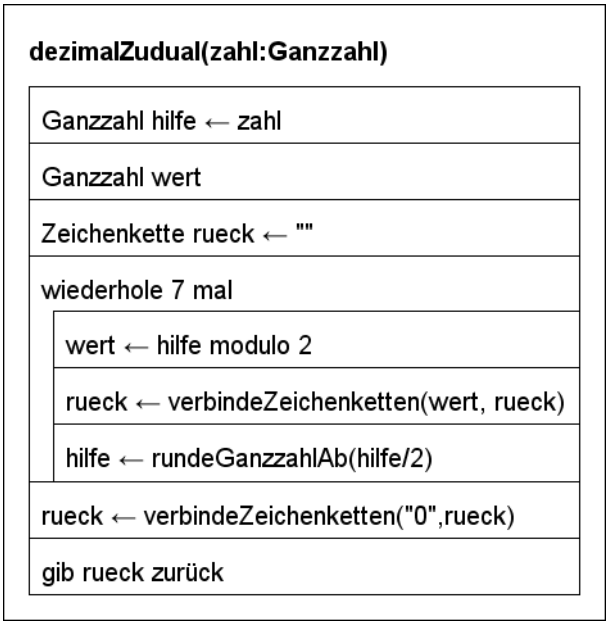

Abbildung 1: Struktogramm

6) Implementieren Sie in einer im Unterricht verwendeten Programmiersprache eine Operation `AsciiCodeGenerieren`. Der Operation wird als Parameter ein Klartext übergeben, Rückgabewert ist der zugehörige binäre ASCII-Code.

7) Implementieren Sie in einer im Unterricht verwendeten Programmiersprache eine Operation `verschluesseln(asciifolge,schluessel:Zeichenkette):Zeichenkette`. Als Parameter werden zwei Binärcodes `asciifolge` und `schluessel` übergeben. Als Rückgabewert berechnet die Operation daraus dann den nach dem XOR-Verfahren erzeugten Geheimtext.

8) Entscheiden Sie, ob das Verfahren der XOR-Verschlüsselung für Diffusion sorgt.

9) Informieren Sie sich über Kerckhoffs' Prinzip. Jemand schlägt vor, den ASCII-Code eines Textes als Verschlüsselung zu verwenden. Nehmen Sie Stellung zu diesem Vorschlag. Gehen Sie dabei auch auf Kerckhoffs' Prinzip ein.

Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz. Sie erlaubt Bearbeitungen und Weiterverteilung des Werks unter Nennung meines Namens und unter gleichen Bedingungen, jedoch keinerlei kommerzielle Nutzung.