Aufgabenblatt 5
Sicherheit digitaler Systeme

Institut: Berliner Hochschule für Technik
Dozent: Prof. Dr. Christian Forler
Url: `https://lms.bht-berlin.de/`
Email: `cforler(at)bht-berlin.de`
Wintersemester 23/24

Aufgabe 1 EC-Karten

a) Die PIN-Nummer einer heutigen EC-Karte besteht aus 4 Dezimalziffern. Jede Ziffer wird gleichverteilt und unabhängig von den anderen aus der Menge $\{0, \ldots, 9\}$ gezogen. Wie groß ist die Entropie einer solchen PIN-Nummer?

b) Früher wurden PIN-Nummern von EC-Karten aus vier gleichverteilten und unabhängigen Hexadezimalziffern $h_i \in \{0, \ldots, F\}$ abgeleitet. Die i-te Stelle s_i der PIN-Nummer wurde aus der i-ten Hexadezimalziffer h_i berechnet nach der Regel

$$s_i = h_i \bmod 10.$$

Wie groß war die Entropie dieser alten PIN-Nummer?

c) Beschreibe für die Schlüssel aus a) und b) jeweils einen möglichst effizienten Algorithmus zur Schlüsselsuche.

d) Gehen Sie nun davon aus, dass die Banken entschieden haben, eine führende '0' durch eine '1' zu ersetzen, da einige Kunden denken, dass ein PIN '0123' als '123' zu interpretieren ist. Berechnen Sie für diesen Fall die Entropie.

Aufgabe 2 Aufgabe

Laden Sie aus dem Moodle die Datei `battlefield-hashes.md5` herunter. Inhalt sind ungesalzene MD5-Hashes der Passwörtern von Battelfield-Spielern. Rekonstruieren Sie mindestens 20% der Passwörter.
(Hinweis: Hilfsmittel wie nicht selbst geschriebene Software sind erlaubt.)

Aufgabe 3 Passwortentropie

Berechnen Sie die Min-Entropie von Alice Passwörtern.

a) Alice wählt vier zufällige Kleinbuchstaben unabhängig voneinander aus und reiht diese fünfmal aneinander, um ein Passwort mit 20 Buchstaben zu erhalten.

b) Alice wählt 20 zufällige Kleinbuchstaben unabhängig voneinander.

Aufgabe 4 Passwortgenerierungsverfahren
Sei `[a-z]` die Menge der 26 Kleinbuchstaben, `[A-Z]` die Menge der 26 Großbuchstaben, `[0-9]` die Menge der 10 Ziffern, `[a-zA-Z0-9+=]` eine Menge aus 64 Zeichen, mit Klein- und Großbuchstaben, Ziffern, '+' und '='.

Alice generiert ihre Passwörter immer nach einem von vier verschiedenen Verfahren. In jedem Fall besteht Alice' Passwort am Ende aus 16 Zeichen. Ihre Vorgehensweisen sind:

a) Wähle 16 Zeichen zufällige Zeichen aus `[a-zA-Z0-9+=]`.

b) Nehmen wir an, Alice' Tastatur hätte 32 Zeichen auf der linken und 32 Zeichen auf der rechten Seite. Dann ist Alice' 2. Verfahren: Wähle ein Zeichen von der linken Seite der Tastatur, dann eins von der rechten Seite, dann wieder eins von der linken Seite usw. bis man 16 Zeichen hat.

c) Wähle 16 zufällige Ziffern aus `[0-9]`.

d) Wähle vier zufällige Großbuchstaben aus `[A-Z]`, danach vier zufällige Kleinbuchstaben aus `[a-z]` und danach acht zufällige Ziffern aus `[0-9]`.

Für alle Verfahren ist jedes gewählte Zeichen unabhängig von den anderen und kann mehrfach auftreten. Berechnen Sie die Min-Entropie der einzelnen Passworterzeugungsverfahren.

Aufgabe 5 Programmieraufgabe

Implementieren Sie ein Programm, dass

1. den Pfad zu einer Textdatei als Parameter entgegen nimmt,
2. den Inhalt der Textdatei lädt und den Text in einzelne Worte trennt,
3. die Anfangsbuchstaben der Wörter zählt
4. die Verteilung der Anfangsbuchstaben und die Entropie sowie die Min-Entropie berechnet.

Es ist völlig ausreichend wenn ihr Programm lediglich ein einzelnes Leerzeichen als Trennzeichen zwischen je zwei Worten interpretiert und nur Klein- und Großbuchstaben am Wortanfang berücksichtigt.

Beispielaufruf:
(für "Moby Dick; Or, The Whale" von Herman Melville)
`https://www.gutenberg.org/files/2701/2701-0.txt`

```
$ ./textentropy 2701-0.txt
...
X 5
...
z 16
--------------------------------
Shannon Entropy: 4.4 bit/char
Min Entropy:     2.6 bit/char
--------------------------------
```