MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

One-Time-Pad mit Fehlern

Autor: Bernhard Esslinger

November 2010 (Update Januar 2012)

One-Time-Pad

Die „Drei Fragezeichen“ haben gehört, dass man wirklich unknackbare Geheimtexte erzeugen kann, wenn man die Zeichen einer richtigen Zufallsfolge nimmt und dann den Klartext damit verknüpft (One-Time-Pad).
Die Verknüpfungsoperation kann z.B. byteweise per Vigenère-Verfahren (Addition der entsprechenden Zahlenwerte modulo 26) oder per XOR-Verfahren (exklusives Oder der Einzelbits) erfolgen.

Seitdem verschlüsseln die „Drei Fragezeichen“ ihre Nachrichten untereinander und nutzen das Vigenère-Verfahren zur Verknüpfung der einzelnen Zeichen. Ihre Klartexte bestehen nur aus den 26 Großbuchstaben. Als Zufallszahlen benutzen sie eine zufällige Zahlenfolge.

One-Time-Pad

Der Geheimtext errechnet sich dann auf folgende Weise:
Zuordnung Buchstabe - Zahlenwert

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

Beispiel-Klartext: T E X T = 19 4 23 19
Beispiel einer Zufallszahlenfolge = Schlüsselstrom:
16, 8, 17, 23, 0, 3, ...
Beispiel-Geheimtext: (19+16) mod 26 = 35 mod 26 = 9 = J
(4+8) mod 26 = 12 mod 26 = 12 = M
(23+17) mod 26 = 40 mod 26 = 14 = O
(19+23) mod 26 = 42 mod 26 = 16 = Q

Aufgabe

Das ist eine einfach anzuwendende Methode, die man auch mit Papier & Bleistift durchführen kann. Andererseits ist es sehr schwer, wirklich zufällige Schlüsselstrom-Folgen zu generieren (egal ob mit oder ohne Computer).

Deshalb dachten sich die „Drei Fragezeichen“ eine Zahl aus und nahmen diese als Startwert für eine endlose, zufällige Zahlenfolge. Sender und Empfänger sollten sich diese Zahlenfolge jederzeit leicht erzeugen oder besorgen können.
Statt eines Buches wählten sie die mathematische Konstante PI = 3,14159265358979323846264338327950288419716939937510582097494459230781640 62...

Aufgabe

Als Schlüssel vereinbarten sie das Offset im Schlüsselstrom (z.B. ist Offset 7 die Ziffer „6“) und ab da nahmen sie aus dem folgenden Schlüsselstrom immer 2 Ziffern große Blöcke als eine Zahl für die Zufallszahlenfolge: Mit einem Offset von 7 wäre der Beginn des Schlüsselstromes beispielsweise: 53, 58, 97, 93, 23, ...

Um den Aufwand zu begrenzen wollten die „Drei Fragezeichen“ ihre Nachrichten kurz halten und ihre Offsets nie größer als 100 wählen. Dafür einigten sie sich aber darauf, regelmäßig ihre Schlüssel zu wechseln.

Aufgabe

Sie kennen nun das Verfahren, aber nicht den Schlüssel. Haben Sie trotzdem eine Chance, eine abgefangene verschlüsselte Nachricht (siehe die Datei *mtc3-esslinger-06-onetimepad-cipher.txt*) zu entschlüsseln?

Die Lösung besteht aus dem gesamten Klartext (er enthält ein Zitat), dem Nachnamen des eigentlichen Autors des Zitates und dem benutzten Offset. Bitte alles direkt hintereinander schreiben – Buchstaben immer in Großbuchstaben.