Anleitung zur Herstellung eines

One-Time-Pad-Schlüssels

Anforderungen:

Ein One-Time-Pad-Schlüssel ist eine Folge von natürlichen Zahlen.

- Die Länge dieser Folge muss mindestens so lang sein wie die Anzahl der Buchstaben der zu verschlüsselnden Nachricht. Jeder Buchstabe (bzw. Symbol) bekommt genau eine Zahl zum Verschlüsseln.

- Die Zahlen der Folge müssen *echt* zufällig generiert werden.

- Die Zahlen müssen in einem Wertebereich liegen, der größer gleich der Anzahl der verfügbaren Symbole ist.

Aufbau :

Um *echte* Zufallszahlen zu generieren, die das ganze Alphabet (26 Symbole) verschlüsseln können, benutzen wir zwei spezielle Würfel:

- 10er-Würfel für die Einerstelle (0-9, wobei 10=0 meint)
- 3er-Würfel für die Zehnerstelle (0-2)

Damit kann man alle Zahlen zwischen 00 (erste Null mit dem 3er Würfel, zweite Null ist eine 10 mit dem 10er Würfel) und 29 (die Zwei mit dem 3er Würfel und die 9 mit dem 10er Würfel) darstellen. Würfelt man eine Zahl, die größer gleich 26 ist, würfelt man einfach nochmal.

Anleitung :

1. Schnappe dir zwei leere Hilfszettel (je 5 Blöcke zu 3 Zeilen).

2. Würfle genügend Zufallszahlen zwischen 0 und 25, um alle ersten Zeilen eines jedes Blocks auszufüllen. (Schau dir auch nochmal das Beispiel an)

3. Schreibe nun die eben gewürfelten Zufallszahlen in identischer Reihenfolge auch auf den zweiten Hilfszettel.

4. Gib den zweiten Hilfszettel demjenigen geheim, der die Nachricht bekommen soll.

5. Denke dir nun eine Nachricht aus und trage diese auf deinen Hilfszettel in die Zeile „Klartext“ ein.

6. Verschiebe nun jeden Buchstaben mit der zugehörigen Zufallszahl. (Caesar-Verschlüsselung mit jedem einzelnen Buchstaben)

7. Schreibe die verschobenen Buchstaben in die Zeile „Geheimtext“.

8. **FERTIG !** Nun kannst du die Nachricht unknackbar – 100% sicher - öffentlich versenden. Selbst die NSA kann nun deine Nachricht nicht mehr lesen. ;D

9. Dein_e Partner_in aus Schritt 4 kann nun die übermittelte Geheimtext-Nachricht (z.B. via Whatsapp) versuchen wieder zu entschlüsseln, indem er/sie den Geheimtext auf seinem/ihrem Hilfszettel einträgt und die Verschiebung rückgängig macht.