LU05f - One time pad

Übersicht

- Kryptographie
- Symmetrische Verschlüsselung
- Substitutionsverfahren

Beim Einmalschlüssel (One-Time-Pad) handelt es sich um eine Abfolge zufälliger Buchstaben. Um einen Text zu verschlüsseln, kombiniert man die einzelnen Buchstaben der Nachricht mit den jeweiligen Buchstaben des Einmalschlüssels. Eine Umsetzungstabelle zeigt, welche Buchstabenkombination von Klartext und Schlüssel zu welchem verschlüsselten Buchstaben führen.

Der Empfänger verfügt über den gleichen Einmalschlüssel. Durch Umkehren des Verfahrens kann er den verschlüsselten Text wieder in den Klartext umwandeln.

Um die Sicherheit des Verfahrens zu gewährleisten:

- muss der Schlüssel mindestens so lang wie die Nachricht sein.
- darf der Schlüssel nur einmal (one time) verwendet werden.

Die Verschlüsselung mit einem One-Time-Pad ist *theoretisch* nicht knackbar. Dazu muss der Schlüssel ...

- ... wirklich komplett zufällig sein.
- ... nur 1x verwendet werden.
- ... auf einem sicheren Weg an den Empfänger übermittelt werden.

Selbst mit Hilfe von Computer kann lediglich jeder denkbare Text ermittelt werden, der die gleiche Länge wie der Chiffretext hat. Welcher dieser gleichlangen Texte der ursprünglichen Nachricht entspricht, kann man nur raten.

Manuelle Anwendung

Grundlagen

Um die Sicherheit zu erhöhen, besteht unser Klartext nur aus Grossbuchstaben und enthält keine Umlaute, Leerzeichen oder Satzzeichen. Jedem Buchstaben wird ein Zahlenwert zugeordnet:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Zur Verschlüsselung verwenden wir eine einfache Addition der Buchstaben im Klartext und Schlüssel. Betrachten wir die Verschlüsselung an einem einzelnen Buchstaben:

- Der Buchstabe im Klartext: „G“
- Der Buchstabe im Schlüssel: „S“

Wir addieren den Zahlenwert der beiden Buchstaben:

- **G** und **S** ergibt **Z**

```
   7 (G)
+ 19 (S)
---------
  26 (Z)
```

Falls die Summe grösser als 26 ist, so subtrahieren wir 26.

- **T** + **O** = **I**

```
  20 (T)
+ 15 (O)
--------
  35 [Das Resultat ist grösser als 26]
- 26
--------
   9 (I)
```

Verschlüsselung

Zur besseren Übersicht unterteilen wir Klartext und Schlüssel in Gruppen zu vier Buchstaben.

Nachricht	Hütet euch am Morgarten
Klartext	HUET ETEU CHAM MORG ARTE N
Schlüssel	DZJY OHQQ YMFN ICXA EPBG U
Chiffre	LVOS TBVL …

Entschlüsselung

Zum Entschlüsseln wird der Prozess umgekehrt; Wir subtrahieren den Schlüssel von der Chiffre. **X** minus **S** ergibt **G** (24 - 17 = 7).

Chiffre	LVOS TBVL …
Schlüssel	DZJY OHQQ YMFN ICXA EPBG U
Klartext	HUET ETEU CHAM MORG ARTE N

Übung

- Bilden Sie 2er oder 3er Gruppen.
- Definieren Sie einen gemeinsamen Schlüssel aus zufälligen Buchstaben.

- Verschlüsseln Sie eine kurze Nachricht.
- Tauschen Sie die Chiffre aus.
- Entschlüsseln Sie die Nachricht.

Computerbasierte Anwendung

Mit einem Computer lassen sich solche Verschlüsselungen wesentlich schneller und mit weniger Fehlern erledigen. Als Zahlenbasis bietet sich der ASCII-Code an, der jedem Buchstaben einen entsprechenden Zahlenwert zuordnet. Die Grossbuchstaben haben einen ASCII-Code von 65_{10} (A) bis 90_{10} (Z).

Die Formel für die Verschlüsselung lautet:

```
chiffre = [ (klartext + schlüssel) modulo 26 ] + 65

  Klartext:  G   ASCII 71
+ Schlüssel: J   ASCII 74
= Chiffre  : P   ASCII 80

1. 71 + 74        = 145
2. 145 modulo 26  =   5  Rest 15
3. 15 + 65        =  80
```

Die Formel für die Entschlüsselung lautet:

```
klartext = (chiffre + 65) - schlüssel
```

Einmalschlüssel mit XOR

XOR ist eine logische Operation die auf zwei Bits angewandt wird. Sie entspricht dem umgangssprachlichen „Entweder … oder“. Das Resultat ist '1' wenn genau eines der Bits '1' ist:

- 0 XOR 0 = 0
- 1 XOR 0 = 1
- 0 XOR 1 = 1
- 1 XOR 1 = 0

Bisher haben wir die Verschlüsselung auf Buchstaben beschränkt. Um beliebige Informationen zu Verschlüsseln, betrachten wir die Klartext-Daten und den Schlüssel als binären Code. Mit dem logischen Operator X0R wird die Chiffre gebildet.

Klartext	0101 0001 0001 0101 0011 1000 0011 0100 1101 1011 1010 0101 1001 0011 0001 1001
Schlüssel	0010 1000 1000 1010 1001 1100 0001 1010 0110 1010 1110 0010 1111 1010 0100 0011
Chiffre	0111 1001 1001 1111 1010 0100 0010 1110 1011 0001 0100 0111 0110 1001 0101 1010

Beim Entschlüsseln wird der X0R-Operator auf die Chiffre und den Schlüssel angewandt.

Schlüssel	0010 1000 1000 1010 1001 1100 0001 1010 0110 1010 1110 0010 1111 1010 0100 0011
Chiffre	0111 1001 1001 1111 1010 0100 0010 1110 1011 0001 0100 0111 0110 1001 0101 1010
Klartext	0101 0001 0001 0101 0011 1000 0011 0100 1101 1011 1010 0101 1001 0011 0001 1001

Durch dieses Verfahren können jegliche Art von Daten mit beliebigen Schlüsseln verschlüsselt werden.

Beispiel

Sie möchten eine geheime Excel-Datei an einen Kollegen im Ausland verschicken. Der Versand per eMail ist nicht möglich, weil Sie befürchten, dass der eMail-Verkehr überwacht wird.

- Als Schlüssel verwenden Sie ein Urlaubsfoto das auf Ihrer Facebook-Seite öffentlich zugänglich ist.
- Sie verschlüsseln die Excel-Datei und stellen diese Datei auf einen öffentlichen Server für Kochrezepte.
- Ihr Kollege lädt sich das Bild und die verschlüsselte Datei herunter.

Damit haben Sie sowohl Kryptographie (Verschlüsselung) als auch Steganographie (Verheimlichung) angewandt.

---

m114-A0G