LU05f - XOR-Verschlüsselung

Internal reference: lu/05-6.md

XOR Operation

Da wir mit Bits (und nicht mit Buchstaben) arbeiten, müssen wir nach anderen Möglichkeiten zur Verschlüsselung suchen. Alphabetverschiebungen wie bei Caesar und Substitutionen sind unsichere Verschlüsselungsverfahren.
Nebst den bekannten Operationen, Addition, Subtraktion, Multiplikation und Division, kann ein Computer auch noch weitere Operationen auf zwei Binärzahlen anwenden. Eine solche Operation ist das XOR (Exklusives Oder, Exclusive OR):

Verschlüsselung

XOR kann auch zur Verschlüsselung verwendet werden. Dabei wird jeweils 1 Bit des Klartextes mit einem Bit des Schlüssels verrechnet. Das Ergebnis ist 1 Bit des Geheimtextes.

Verschlüsselung

p	k	c=p XOR k
0	0	0
0	1	1
1	0	1
1	1	0

Entschlüsselung

c	k	p=c XOR k
0	0	0
1	1	0
1	0	1
0	1	1

wobei p : plain text (Klartext) k : key (Schlüssel) c : cipher (Verschlüsselt)

Die Verschlüsselung ist identisch mit der Entschlüsselung, da Folgendes gilt:

```
c XOR k=(p XOR k) XOR k=p
```

—

Quelle: https://ofi.gbsl.website/26P/Kryptologie/Symmetrisch/xor