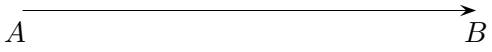
Kryptologie

kryptos, griech. geheim
logos, das Wort, der Sinn

chiffrieren, verschlüsseln
dechiffrieren, entschlüsseln



A möchte B eine Zahl T verschlüsselt zusenden.
Denkbar wäre $100 - T$.

Dechiffriere
WRQRE XNAA QVR IREFPUYHRFFRYHAT IBA PNRFNE RVASNPU XANPXRA.

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

Vigenère, französischer Diplomat, 16. Jahrhundert

Die bekannteste Public-Key-Chiffrierung geht auf die Mathematiker Rivest, Shamir und Adleman vom Massachusetts Institute of Technology (MIT) zurück und wird seit 1978 nach deren Anfangsbuchstaben als RSA-Verfahren bezeichnet.

Beim Verschlüsseln wird ein öffentlicher Schlüssel und beim Entschlüsseln ein privater Schlüssel verwendet. Mit dem öffentlichen Schlüssel kann jeder Nachrichten verschlüsseln, aber nicht entschlüsseln. Zum Entschlüsseln benötigt man den privaten Schlüssel, und den kennt nur der Empfänger.

In den USA und in Frankreich ist die Verschlüsselung von Nachrichten nur erlaubt, wenn der Staat einen „Nachschlüssel“ besitzt.

```
# 1. Versuch

k=3
Geheimtext=""

def verschluesseln():
   Klartext=input("Klartext: ")

   global Geheimtext
   for n in range(len(Klartext)):
      Geheimtext=Geheimtext + chr(ord(Klartext[n])+k )
   print(Geheimtext)



def entschluesseln():
   Klartext=""
   for n in range(len(Geheimtext)):
      Klartext=Klartext + chr(ord(Geheimtext[n])-k)
   print(Klartext)

verschluesseln()
entschluesseln()
```

ord(“A“) = 65		ASCII-Codierung
ord(“B“) = 66		American Standard Code for Information Interchange
ord(“Z“) = 90		
chr(65) = “A“		
chr(97) = “a“		

```
# 2. Versuch

k=3
Geheimtext=""

def verschluesseln():
   Klartext=input("Klartext: ")

   global Geheimtext
   for n in range(len(Klartext)):
      Geheimtext=Geheimtext + chr((ord(Klartext[n])+k-65) % 26 + 65)

   print(Geheimtext)



def entschluesseln():
   Klartext=""
   for n in range(len(Geheimtext)):
      Klartext=Klartext + chr((ord(Geheimtext[n])-k-65) % 26 + 65)
   print(Klartext)

verschluesseln()
entschluesseln()
```

$\text{ord}(\text{“A“}) = 65$ ASCII-Codierung

$\text{ord}(\text{“B“}) = 66$ American Standard Code for Information Interchange

$\text{ord}(\text{“Z“}) = 90$

$\text{chr}(65) = \text{“A“}$

$\text{chr}(97) = \text{“a“}$

```
s = "Das ist ein Text."
s = s.upper()
print(s)                    # DAS IST EIN TEXT.
```

Chiffrieren durch Maskieren

$$
\begin{array}{cccccccccccccc}
1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & \ldots \\
0 & 1 & 1 & 0 & 1 & 1 & 1 & & & & & & & \\
\hline
1 & 1 & 1 & 1 & 0 & 1 & 0 & & & & & & &
\end{array}
$$

Beschreibe das Verfahren.