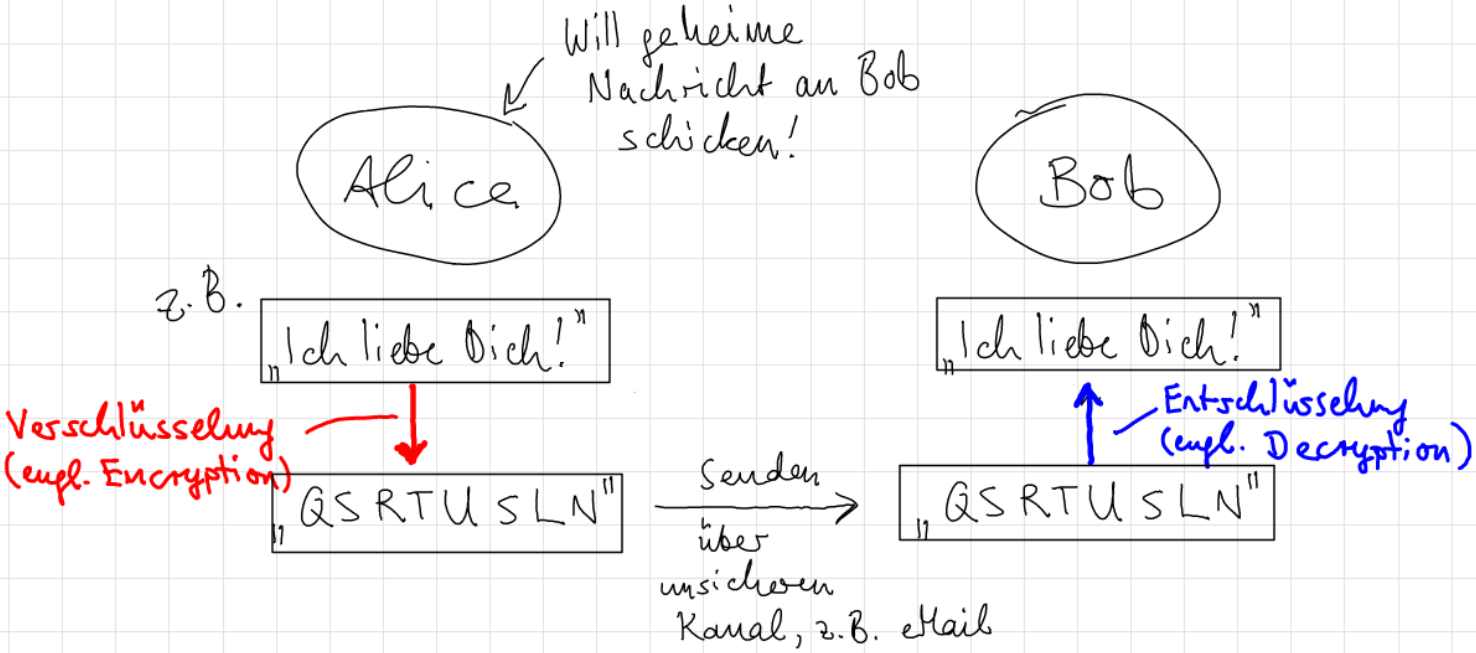
Kryptographie

Kryptographie – Cäsar-Verschlüsselung

Warum Zahlentheorie? ☐ Promotion

☐ Verschlüsselung / Kryptographie

Die Grundidee der Verschlüsselung:



Ein einfaches Verfahren, das Cäsar benutzt haben soll:

Klartext: I C H L I E B E D I C H

Schlüssel/Key ist $k = 3$

Geheimtext:

Verschlüsselung: $E_k : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}$, $E_k(x) = x + k \mod 26$

Entschlüsselung: $D_k : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}$, $D_k(x) = x - k \mod 26$

Ist das sicher?

Kryptographie – Vigenère-Verschlüsselung

Eine verbesserte Variante davon ist Folgendes:

Klartext: I C H L I E B E D I C H

Schlüssel: R I N G

Geheimtext:

Ist das sicher?

Ü Verschlüsseln Sie M A T H E R O C K S mit:

a) Cäsar-Verschlüsselung mit $k = 7$.

b) Vigenère mit dem Schlüsselwort STIMMT.

Kryptographie – RSA

Problem: Wie kommt Bob an den Schlüssel?

Lösung: privater & öffentlicher Schlüssel

→ **RSA-Verfahren**

1. Nehme große Primzahlen p, q und berechne die
2. „riesige" Zahl $\boxed{N = p \cdot q}$ **RSA-Modul**
3. Bestimme $\varphi(N) =$
4. Wähle eine Zahl e mit

   öffentlicher Schlüssel / public key:
5. Bestimme ein Zahl d mit $\boxed{}$

   (letztlich löse $e \cdot \underbrace{d}_{x} + \varphi(N) \underbrace{(-q)}_{y} = 1$ mit EEA).

   privater Schlüssel / private key:

Auf was basiert die Sicherheit von RSA?

Ver- und Entschlüsselung mit RSA:

Gegeben ein Klartext T, z.B. $T = \text{'A'} \hat{=} 0$

Wie berechnet man den Geheimtext G mit dem öffentlichen Schlüssel (N, e):

Verschlüsselung: $T \mod N$

Man bekommt dann den Klartext T mittels des privaten Schlüssels (N, d):

Entschlüsselung: $G \mod N$

Warum gilt $(\underbrace{T^e}_{G})^d \equiv T \mod N$?

ü

Seien $p = 7$, $q = 11$, $N = p \cdot q = 77$ (RSA-Modul).
Bestimmen Sie geeignete e, d und ver-/entschlüsseln Sie $T = 2$ ($\hat{=}$ 'B').