



more: bigdev.de/teaching

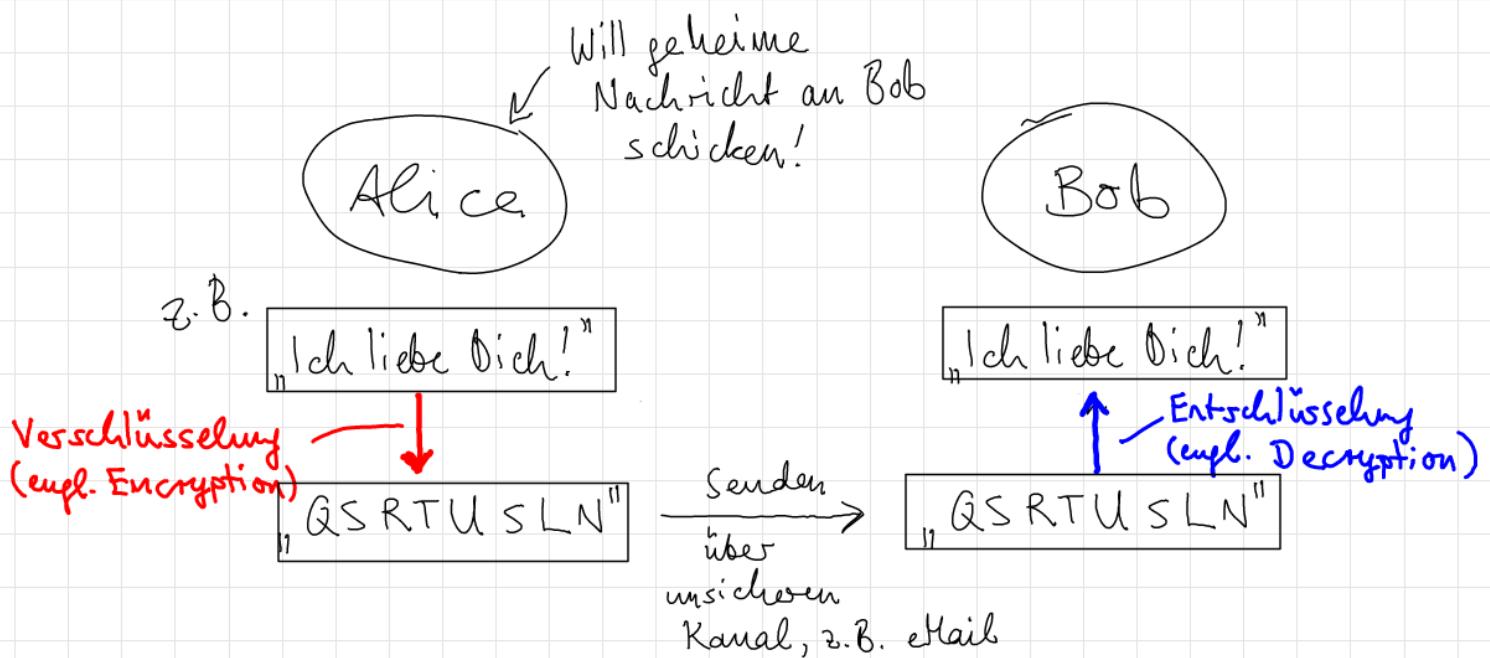
Kryptographie

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

Geheimtext: L F K O L K E E G L F K

Schlüssel/Key
ist $k = 3$

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

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

Ist das sicher? Nein

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 R I N G R I N G

Geheimtext: Z K U R Q . .

Ist das sicher? Nein

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.
- a.) THAOLYVZRZ mit $k = 7$
- b.) M A T H E R O C K S
STIMMTSTIM
ETBTQKGVSÉ

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 $N = p \cdot q$ **RSA-Modul**
3. Bestimme $\varphi(N) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$
4. Wähle eine Zahl e mit $1 < e < \varphi(N)$ mit $\text{ggT}(e, \varphi(N)) = 1$

öffentlicher Schlüssel / public key: $(e; N)$

5. Bestimme ein Zahl d mit $e \cdot d \equiv 1 \pmod{\varphi(N)}$
(letztlich löse $e \cdot d + \varphi(N) \underbrace{x}_{\times} \underbrace{-y}_{\equiv 1}$ mit EEA).

privater Schlüssel / private key: $(d; N)$

Auf was basiert die Sicherheit von RSA?

Ver- und Entschlüsselung mit RSA:

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

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

Verschlüsselung: $G = T^e \bmod N$

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

Entschlüsselung: $T = G^d \bmod N$

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

$$e \cdot d \equiv 1 \bmod \varphi(N)$$

$$e \cdot d = c \cdot \varphi(N) + 1$$

$$\text{ggf}(a; m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \bmod m$$

$$(T^e)^d \equiv T^{e \cdot d} \equiv T^{c \cdot \varphi(N) + 1} \equiv T^{c \cdot \varphi(N)} \cdot T \equiv (T^{\varphi(N)})^c \cdot T \equiv 1^c \cdot T \equiv T \bmod N$$

Ü

Seien $p=7$, $q=11$, $N=p \cdot q = 77$ (RSA-Modul).

Bestimmen Sie geeignete e, d und ver-/entschlüsseln Sie $T = 2$ ($\hat{=} 'B'$).

1.) $p=7$; $q=11$; $N=77$

2.) $\varphi(77) = \varphi(7) \cdot \varphi(11) = (7-1) \cdot (11-1) = 60$

3.) $e=47 \Rightarrow$ public key: $(47; 77)$

4.) $47 \cdot d \equiv 1 \pmod{60} \Rightarrow d=23 \Rightarrow$ private key $(23; 77)$

EEA: $47x + 60y = 1$

$$\begin{array}{rcl} 47 & = & 0 \cdot 60 + 47 \\ 60 & = & 1 \cdot 47 + 13 \\ 47 & = & 3 \cdot 13 + 8 \\ 13 & = & 1 \cdot 8 + 5 \\ 8 & = & 1 \cdot 5 + 3 \\ 5 & = & 1 \cdot 3 + 2 \\ 3 & = & 1 \cdot 2 + 1 \\ 2 & = & 2 \cdot 1 + 0 \end{array} \quad \begin{array}{rcl} (23) & -18 & \\ -18 & 23 & \\ 5 & -18 & \\ -3 & 5 & \\ 2 & -3 & \\ -1 & 2 & \\ 1 & -1 & \\ 0 & 1 & \end{array}$$

$$2^{47} \pmod{77}$$

$$2^{47} \equiv 2^5 \cdot (2^5)^6 \equiv 32 \cdot 51^6 \equiv 32 \cdot (51^2)^3 \equiv 32 \cdot 60^3$$

$$\equiv 32 \cdot (-17)^3 \equiv 32 \cdot (-17) \cdot (-17)^2 \equiv (-5) \cdot 58 \equiv (-5) \cdot (-13)$$

$$\equiv 85 \equiv 18 \pmod{77}$$

$$18^{23} \pmod{77}$$