

# Algorithmen und Datenstrukturen in C/C++

Prof. Dr. rer. nat. Peter Gerwinski

28. Mai 2018

# Algorithmen und Datenstrukturen in C/C++

<https://gitlab.cvh-server.de/pgerwinski/ad.git>

## 1 Einführung

## 2 Einführung in C++

## 3 Datenorganisation

## 4 Datenkodierung

### 4.0 Parität

4.  $(x^2 - 1)$  Der Herr der Ringe: Manchmal ist  $1 + 1 = 0$ .

### 4.1 Fehlererkennung durch CRC

### 4.2 Ausfall- und Fehlerkorrektur durch Reed-Solomon-Code

### 4.3 Verschlüsselung

## 5 Hardwarenahe Algorithmen

## 6 Optimierung

## 7 Numerik



Änderungen  
vorbehalten

# 4 Datenkodierung

## 4.3 Verschlüsselung

### 4.3.0 OpenPGP in der Praxis

E-Mail

Malware, geschrieben in HTML

- abgefangene E-Mail, verschlüsselt  
→ entschlüsseln
- an berechtigten Empfänger senden,  
damit er sie unbemerkt entschlüsselt

sende: 

Hausaufgabe

Verschlüsselte E-Mail an PG,  
die auch verschlüsselt beantwortet wird

- Software installieren:  
GnuPG, Kleopatra, GPG4Win,  
Enigmail, GPA, mutt
- Schlüsselpaar erzeugen
- Schlüsselaustausch
- benutzen

Schlüssel von PG: Fingerprint

2CFD EA6C 31E6 12A0 BFFF

2457 D955 0227 6224 E7F5

## 4.3 Verschlüsselung

### 4.3.1 Verschlüsselungsverfahren

#### *Symmetrische Verschlüsselung:*

Derselbe Schlüssel zum Ver- und Entschlüsseln

- Cäsar-Chiffre: monoalphabetische Substitution
- Vigenère-Chiffre: polyalphabetische Substitution
- Kryptanalyse: Kasiski-Test, Friedman-Test
- One-Time-Pad
- Pseudozufall

## 4.3 Verschlüsselung

### 4.3.1 Verschlüsselungsverfahren

#### *Symmetrische Verschlüsselung:*

Derselbe Schlüssel zum Ver- und Entschlüsseln

- Cäsar-Chiffre: monoalphabetische Substitution
- Vigenère-Chiffre: polyalphabetische Substitution
- Kryptanalyse: Kasiski-Test, Friedman-Test
- One-Time-Pad
- Pseudozufall
- spezieller Pseudozufall:  
Enigma, RC4, DES, 3DES, IDEA, Rijndael, Blowfish, Twofish, CAST5, ...

## 4.3 Verschlüsselung

### 4.3.1 Verschlüsselungsverfahren

#### *Symmetrische Verschlüsselung:*

Derselbe Schlüssel zum Ver- und Entschlüsseln

- Cäsar-Chiffre: monoalphabetische Substitution
- Vigenère-Chiffre: polyalphabetische Substitution
- Kryptanalyse: Kasiski-Test, Friedman-Test
- One-Time-Pad
- Pseudozufall
- spezieller Pseudozufall:  
Enigma, RC4, DES, 3DES, IDEA, Rijndael, Blowfish, Twofish, CAST5, ...  
                                  unsicher  
Rijndael = AES, RC4 = CipherSaber

## 4.3 Verschlüsselung

### 4.3.1 Verschlüsselungsverfahren

#### *Symmetrische Verschlüsselung:*

Derselbe Schlüssel zum Ver- und Entschlüsseln

- Cäsar-Chiffre: monoalphabetische Substitution
- Vigenère-Chiffre: polyalphabetische Substitution
- Kryptanalyse: Kasiski-Test, Friedman-Test
- One-Time-Pad
- Pseudozufall
- spezieller Pseudozufall:  
Enigma, RC4, DES, 3DES, IDEA, Rijndael, Blowfish, Twofish, CAST5, ...  
unsicher  
Rijndael = AES, RC4 = CipherSaber

Problem: geheimer Kanal für Schlüsselaustausch erforderlich

Lösung: *asymmetrische Verschlüsselung*

## 4.3 Verschlüsselung

### 4.3.1 Verschlüsselungsverfahren

#### *Asymmetrische Verschlüsselung:*

Verschiedene Schlüssel zum Ver- und Entschlüsseln

- mathematische Operation „schwierig“ umkehrbar
- Messung von „schwierig“: Landau-Symbol
- Beispiele:
  - Primfaktorzerlegung schwieriger als Multiplikation von Primzahlen
  - Logarithmus schwieriger als Potenz
- Verfahren:
  - RSA, DSA, ElGamal, ECRSA, ...



## 4.3 Verschlüsselung

### 4.3.1 Verschlüsselungsverfahren

#### *Asymmetrische Verschlüsselung:*

Verschiedene Schlüssel zum Ver- und Entschlüsseln

- mathematische Operation „schwierig“ umkehrbar
- Messung von „schwierig“: Landau-Symbol
- Beispiele:
  - Primfaktorzerlegung schwieriger als Multiplikation von Primzahlen
  - Logarithmus schwieriger als Potenz
- Verfahren:
  - RSA, DSA, ElGamal, ECRSA, ...

Problem: Verfahren sind langsam

Lösung: *hybride Verschlüsselung*:

asymmetrisches Verfahren verschlüsselt symmetrischen *Sitzungsschlüssel*

## 4.3 Verschlüsselung

### 4.3.1 Verschlüsselungsverfahren

#### *Asymmetrische Verschlüsselung:*

Verschiedene Schlüssel zum Ver- und Entschlüsseln

- mathematische Operation „schwierig“ umkehrbar
- Messung von „schwierig“: Landau-Symbol
- Beispiele:
  - Primfaktorzerlegung schwieriger als Multiplikation von Primzahlen
  - Logarithmus schwieriger als Potenz
- Verfahren:
  - RSA, DSA, ElGamal, ECRSA, ...

Problem: Verfahren sind langsam

Lösung: *hybride Verschlüsselung*:

asymmetrisches Verfahren verschlüsselt symmetrischen *Sitzungsschlüssel*

Problem: nicht-manipulierbarer Kanal für Schlüsselaustausch erforderlich

Lösung: *Zertifizierung*

## 4.3 Verschlüsselung

### 4.3.2 Zertifizierung von Schlüsseln

- S/MIME: hierarchische Baumstruktur
- OpenPGP: Web of Trust

## 4.3 Verschlüsselung

### 4.3.2 Zertifizierung von Schlüsseln

- S/MIME: hierarchische Baumstruktur
- OpenPGP: Web of Trust – kann auch hierarchische Baumstruktur sein

OpenPGP: E-Mail, spezielle Anwendungen, . . .

- Vertrauen in den Schlüssel: mathematisch berechenbar
- Vertrauen in die Person: persönliche Entscheidung

## 4.3 Verschlüsselung

### 4.3.2 Zertifizierung von Schlüsseln

- S/MIME: hierarchische Baumstruktur
- OpenPGP: Web of Trust – kann auch hierarchische Baumstruktur sein

OpenPGP: E-Mail, spezielle Anwendungen, . . .

- Vertrauen in den Schlüssel: mathematisch berechenbar
- Vertrauen in die Person: persönliche Entscheidung

S/MIME: Webseiten, E-Mail, spezielle Anwendungen, . . .

- Vertrauen in den Schlüssel: mathematisch berechenbar
- Vertrauen in die Person: wird vom Anbieter vorgegeben

# Algorithmen und Datenstrukturen in C/C++

<https://gitlab.cvh-server.de/pgerwinski/ad.git>

## 1 Einführung

## 2 Einführung in C++

## 3 Datenorganisation

## 4 Datenkodierung

### 4.0 Parität

4.  $(x^2 - 1)$  Der Herr der Ringe: Manchmal ist  $1 + 1 = 0$ .

### 4.1 Fehlererkennung durch CRC

### 4.2 Ausfall- und Fehlerkorrektur durch Reed-Solomon-Code

### 4.3 Verschlüsselung

## 5 Hardwarenahe Algorithmen

## 6 Optimierung

## 7 Numerik



Änderungen  
vorbehalten