# **Komplexe Leistung**

# Darstellung der Funktionsweise von Verschlüsselungsverfahren

# Gliederung

- 1. Einleitung
- 2. Arten der Verschlüsselung
  - 1. Symmetrische Verschlüsselung
  - 2. Asymmetrische Verschlüsselung
  - 3. Hybride Verschlüsselung
- 3. Vorstellung zweier Verfahren
  - 1. Vigenère Chiffre
  - 2. RSA Verschlüsselung
- 4. Präsentation der Eigenleistung
- 5.Quellen

## 1. Einleitung

- Essentielle Errungenschaft der Neuzeit
- Beginn war circa 1900 vor Christus in Ägypten
- Einsatz der ENIGMA im zweiten Weltkrieg
- Einteilung der Verschlüsselung in drei Teile
  - Schlüsselerzeugung
  - Verschlüsselung
  - Entschlüsselung

## 2. Arten der Verschlüsselung

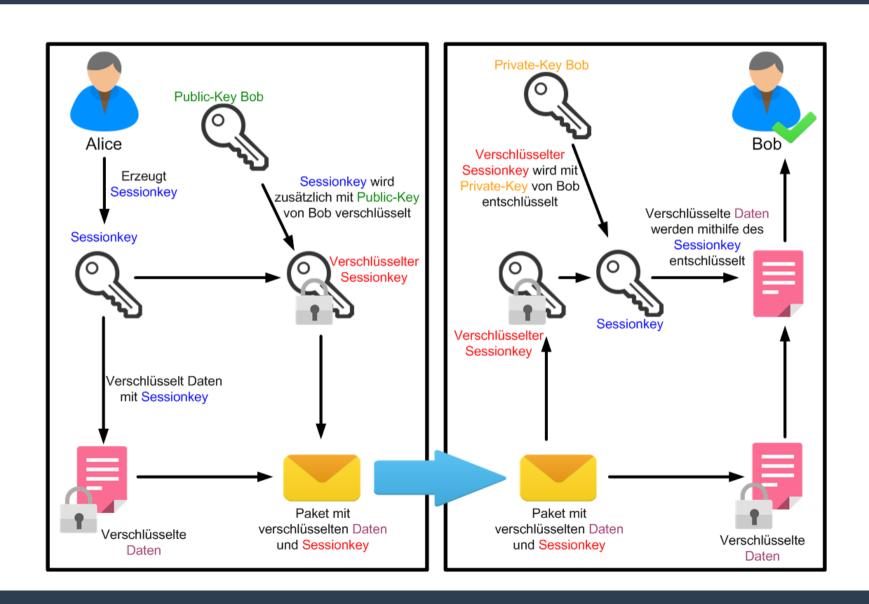
- 2.1. Symmetrische Verschlüsselung
- Beide Teilnehmer haben meistens den selben Schlüssel
- Einteilung in Block- und Stromchiffren
- Nachteil ist der Transport des Schlüssels
  - => Lösung liegt in hybrider Verschlüsselung

## 2. Arten der Verschlüsselung

- 2.2 Asymmetrische Verschlüsselung
- Jeder Teilnehmer hat einen anderen Schlüssel
- Öffentlicher Schlüssel: Klartext → Geheimtext
- Privater Schlüssel: Geheimtext → Klartext
- Mindestens drei Algorithmen
  - Schlüsselerzeugung
  - Verschlüsselung
  - Entschlüsselung

## 2. Arten der Verschlüsselung

- 2.3 Hybride Verschlüsselung
- Kombination aus symmetrischer und asymmetrischer Verschlüsselung
- Klartext wird symmetrisch verschlüsselt
- Schlüssel wird asymmetrisch verschlüsselt



- 3.1 Vigenère Chiffre
- Entstanden im 16. Jahrhundert und bennant nach dem Erfinder Blaise de Vigenère
- Stromchiffre
- Substituierte Geheimzeichen werden durch das Vigenère-Quadrat bestimmt

											i e					_			(A)						_
Α	В	C	D	E	F	G	H	I	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z
В	C	D	Ε	F	G	H	Ι	J	K	L	M	И	0	Ρ	Q	R	S	Т	U	V	W	X	Y	Z	Α
С	D	Е	F	G	Η	Ι	J	K	L	М	И	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В
D	Ε	F	G	H	Ι	J	K	L	Μ	И	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С
E	F	G	Η	Ι	J	K	L	Μ	И	0	Ρ	Q	R	S	Τ	U	V	W	Χ	Y	Z	A	В	С	D
F	G	Η	Ι	J	K	L	Μ	Ν	0	Ρ	Q	R	S	Τ	U	V	W	X	Y	Z	Α	В	C	D	Е
G	Η	Ι	J	K	L	Μ	И	0	Ρ	Q	R	S	Τ	U	V	W	Χ	Y	Z	Α	В	С	D	Ε	F
н	Ι	J	K	L	Μ	И	0	Ρ	Q	R	S	Т	U	V	W	X	Y	Z	A	В	С	D	Ε	F	G
I	J	K	L	М	И	0	Ρ	Q	R	S	Т	U	V	W	X	Y	Z	Α	В	С	D	Ε	F	G	Н
J	K	L	Μ	И	0	P	Q	R	S	Т	U	V	W	Х	Y	Z	A	В	С	D	Е	F	G	Н	Ι
$\mathbf{K}$	L	Μ	Ν	0	Ρ	Q	R	S	Τ	U	V	W	X	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J
L	М	Ν	0	P	Q	R	S	Т	U	V	W	Х	Y	Z	A	В	C	D	Ε	F	G	H	Ι	J	K
M	И	0	P	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L
N	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	C	D	Ε	F	G	Н	Ι	J	K	L	М
О	Ρ	Q	R	S	Τ	U	V	W	X	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	М	И
P	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	М	И	0
Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	K	L	Μ	И	0	Р
R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	М	И	0	Р	Q
S	Т	U	V	W	Х	Y	Z	Α	В	C	D	Е	F	G	Н	Ι	J	K	L	М	И	0	P	Q	R
T	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	K	L	Μ	И	0	Ρ	Q	R	S
U	V	W	X	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	Μ	И	0	Ρ	Q	R	S	Т
v	W	Х	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	М	И	0	Ρ	Q	R	S	Т	U
W	Х	Y	Z	A	В	С	D	Ε	F	G	Н	Ι	J	K	L	М	N	0	Ρ	Q	R	S	Т	U	V
X	Y	Z	A	В	С	D	Ε	F	G	Н	Ι	J	K	L	М	И	0	Ρ	Q	R	S	Т	U	V	W
Y	Z	Α	В	С	D	Е	F	G	Н	Ι	J	K	L	М	И	0	Ρ	Q	R	S	Т	U	V	W	Х
Z	Α	В	С	D	Е	F	G	Н	Ι	J	K	L	Μ	И	0	P	Q	R	S	Т	U	V	W	Х	Y

#### <u>Funktionsweise</u>

- 1. Auswahl eines Schlüssels
- Auswahl der Geheimbuchstaben durch Krezungspunkt des Schlüsselbuchstabens und des Klartextbuchstabens
  - Schlüssel wird solange wiederholt, bis der Klartext zu Ende ist

	0 01	9 05		- 10			500			20			9 9	9		2 10			500						0 20
Α	В	C	D	E	F	G	Н	I	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z
В	С	D	Ε	F	G	Η	Ι	J	K	L	Μ	И	0	Ρ	Q	R	S	Т	U	V	W	Χ	Y	Z	Α
C	D	Ε	F	G	Η	Ι	J	K	L	Μ	И	0	Ρ	Q	R	S	Τ	U	V	W	X	Y	Z	Α	В
D	Ε	F	G	Η	Ι	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	W	Χ	Y	Z	Α	В	С
E	F	G	Η	Ι	J	K	L	Μ	И	0	Ρ	Q	R	S	Т	U	V	W	X	Y	Z	Α	В	C	D
F	G	Η	Ι	J	K	L	Μ	Ν	0	Ρ	Q	R	S	Τ	U	V	W	Х	Y	Z	A	В	C	D	Е
G	Н	Ι	J	K	L	Μ	И	0	Ρ	Q	R	S	Τ	U	V	W	Х	Y	Z	Α	В	С	D	Ε	F
н	Ι	J	K	L	Μ	И	0	Ρ	Q	R	S	Т	Ū	V	W	Х	Y	Z	A	В	U	D	Ε	F	G
Ι	J	K	L	М	И	0	Ρ	Q	R	S	Т	U	V	W	X	Y	Z	Α	В	С	D	Ε	F	G	н
J	K	L	Μ	Ν	0	P	Q	R	S	Т	U	V	W	Х	Y	Z	A	В	С	D	Ε	F	G	Н	Ι
$\mathbf{K}$	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	W	X	Y	Z	A	В	С	D	Ε	F	G	Н	Ι	J
L	М	И	0	Ρ	Q	R	S	Т	υ	V	W	X	Y	Z	A	В	C	D	Ε	F	Ç	Н	Ι	J	K
м	И	0	P		R	S	Τ	U	V	W	Х	Y	Z	Α	В	С	D	Е	F	G	Η	Ι	J	K	L
N	0	Ρ	Q	R	S	Т	U	V	W	X	Y	Z	A	В	C	D	Ε	F	G	Η	Ι	J	K	L	М
О	Р	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	С	D	Ε	F	G	H	Ι	J	K	L	Μ	И
P	Q	R	S	Т	U	V	W	Х	Y	Z	Α	В	C	D	Ε	F	G	Н	Ι	J	K	L	М	И	0
Q	R	S	Т	U	V	W	X	Y	Z	A	В	С	D	Ε	F	G	H	Ι	J	K	L	Μ	И	0	P
R	S	Т	U	V	W	X	Y	Z	Α	В	C	D	Ε	F	G	H	Ι	J	K	L	Μ	И	0	P	Q
S	Т	U	V	W	X	Y	Z	Α	В	C	D	Ε	F	G	Η	Ι	J	K	L	М	И	0	P	Q	R
T	U	V	W	Х	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	Μ	И	0	Ρ	Q	R	S
U	V	W	X	Y	Z	Α	В	С	D	Ε	F	G	Η	Ι	J	K	L	М	И	0	Ρ	Q	R	S	Т
V	W	Χ	Y	Z	A	В	С	D	Е	F	G	Η	Ι	J	K	L	М	И	0	Ρ	Q	R	S	Т	U
W	Χ	Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	М	И	0	Ρ	Q	R	S	Т	U	V
X	Y	Z	A	В	С	D	Ε	F	G	Н	Ι	J	K	L	М	И	0	Ρ	Q	R	S	Т	U	V	W
Y	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	М	И	0	Р	Q	R	S	Т	U	V	W	Х
Z	Α	В	С	D	Е	F	G	Н	Ι	J	K	L	Μ	И	0	Ρ	Q	R	S	Т	U	V	W	Х	Y

#### 3.2. RSA-Verfahren

- Eines der sichersten Verschlüsselungsalgorithmen der Welt
- Das erste veröffentlichte asymmetrische Verschlüsselungsverfahren
- Erfunden von Ronald Rivest, Adi Shamir und Max Adleman => RSA

#### **Funktionsweise**

Komplizierte Algorithmen zur
Schlüsselgenerierung und zur Verschlüsselung

# 4. Präsentation der Eigenleistung

- Entwicklung eines Programms in der Programmiersprache "Java"
- Mit Hilfe des Programms kann man, die drei in der Komplexen Leistung vorgestellten Verfahren testen
- Es wurde das Framework "JavaFX", die IDE "IntelliJ" und das Programm "JavaFX Scene Builder 2.0" verwendet

## 5. Quellen

- https://upload.wikimedia.org/wikipedia/commons /3/3d/Code-1076536.jpg
- https://pixabay.com/p-1294045/?no\_redirect
- https://de.wikipedia.org/wiki/Hybride\_Verschl %C3%BCsselung#/media/File:Hybride\_Verschl %C3%BCsselung.png
- Meine Komplexe Leistung