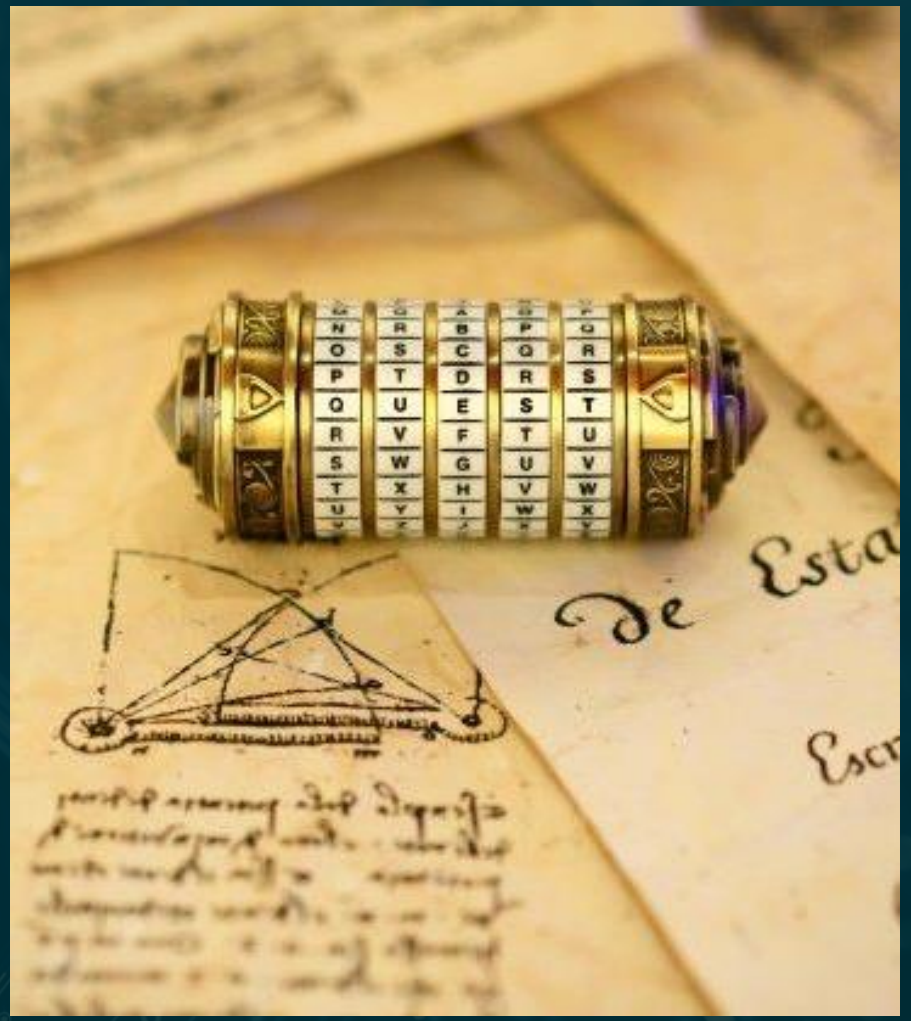
Präsentationsprojekt als LEK zu Fach FI-ITS-Sec

VERWENDUNG VON KRYPTOGRAPHIE

US IT 2023 Sommer August FIAE A
Sascha Riemenschneider
27.Mai 2024

INHALT

- Was ist Kryptographie
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Gegenseitige Ergänzung von symmetrischer und asymmetrischer
- Anwendungsfälle
- Verwendete Literatur



KRYPTOGRAPHIE

Der Begriff **„Kryptographie“** stammt aus dem Altgriechischen und bedeutet **„geheim schreiben“**. Es handelt sich um die Wissenschaft der Verschlüsselung von Texten und Dateien, um den Zugriff für Unbefugte zu verhindern.

Schon im **dritten Jahrtausend** vor Christus wurden die **ersten Texte verschlüsselt**. Im Römischen Reich und im Mittelalter wurden wichtige Nachrichten oder Kriegsbefehle kryptographisch gesichert.

Julius Caesar verwendete eine einfache Form der Kryptographie, indem er jeden Buchstaben durch den drittnächsten im Alphabet ersetzte.

Im Zweiten Weltkrieg wurden Maschinen (Enigma-M4) zur Verschlüsselung genutzt, was die Kryptographie komplexer machte. Die Briten benötigten mehrere Jahre, um die Schlüssel zu knacken und die Nachrichten zu entschlüsseln.

KRYPTOGRAPHIE

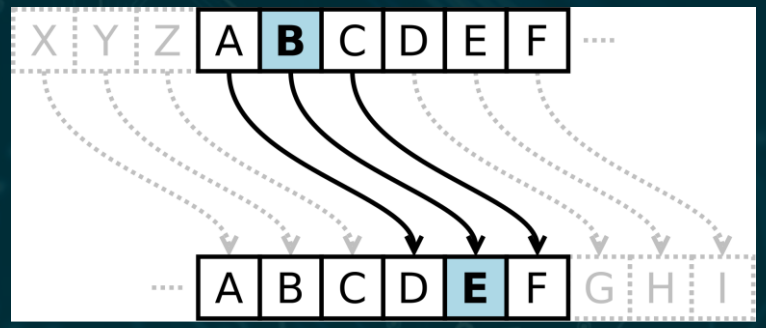
Caesar-Verschlüsselung

Quellcode

```python
import string

alphabets = string.ascii_lowercase * 2
encode_inputs = ["encode", "encrypt"]
decode_inputs = ["decode", "decrypt"]
valid_inputs = encode_inputs + decode_inputs


def caesar(cipher_direction, start_text, shift_amount):
    end_text = ""
    dir = "encrypting"
    # if the direction is valid, then make the shift amount negative
    if cipher_direction in decode_inputs:
        dir = "decrypting"
        shift_amount *= -1
    for char in start_text:
        if char in alphabets:
            # get the index
            index = alphabets.index(char)
            # shift the index
            new_index = index + shift_amount
            # add the alphabet at the given index to the end string
            end_text += alphabets[new_index]
        else:
            # if the char is not an alphabet, then add it as it is without shifting
            end_text += char
    print(f"\nText after {dir} is: {end_text}\n")


should_continue = True
while should_continue:
    direction = input("Enter {0} to encrypt or {1} to decrypt: "
                      .format(" or ".join(encode_inputs).casefold(),
                              " or ".join(decode_inputs))).casefold()
    if direction not in valid_inputs:
        print(f"{direction} is not a valid input.")
        continue
    text = input(f"\nEnter text to {direction}: ").casefold()
    shift = int(input("Enter the shift number: ")) % 26
    caesar(direction, text, shift)

    if input("Do you want to go again? (y/n): ").casefold() != "y":
        should_continue = False
        print("\nExiting.")
```

Ergebnis der Codeausführung

```
Enter encode or encrypt to encrypt or decode or decrypt to decrypt: encode

Enter text to encode: Mens sana in corpore sano
Enter the shift number: 13

Text after encrypting is: zraf fnan va pbecber fnab

Do you want to go again? (y/n): y
Enter encode or encrypt to encrypt or decode or decrypt to decrypt: decode

Enter text to decode: zraf fnan va pbecber fnab
Enter the shift number: 6

Text after decrypting is: tluz zhuh pu jvywvyl zhuv

Do you want to go again? (y/n): y
Enter encode or encrypt to encrypt or decode or decrypt to decrypt: decode

Enter text to decode: zraf fnan va pbecber fnab
Enter the shift number: 13

Text after decrypting is: mens sana in corpore sano

Do you want to go again? (y/n): n

Exiting.
```



SYMMETRISCHE VERSCHLÜSSELUNG

- Ver- und Entschlüsselung mit demselben Schlüssel(Private-Key)
- Schlüsselaustausch (Treffen, Briefpost, SMS oder Telefon)
- Die Verteilung über ein Netzwerk (Schlüsselaustauschprotokollen oder Anwendung asymmetrischer Verschlüsselungsverfahren)

VORTEIL

- schnell
- für große Datenmengen gut geeignet

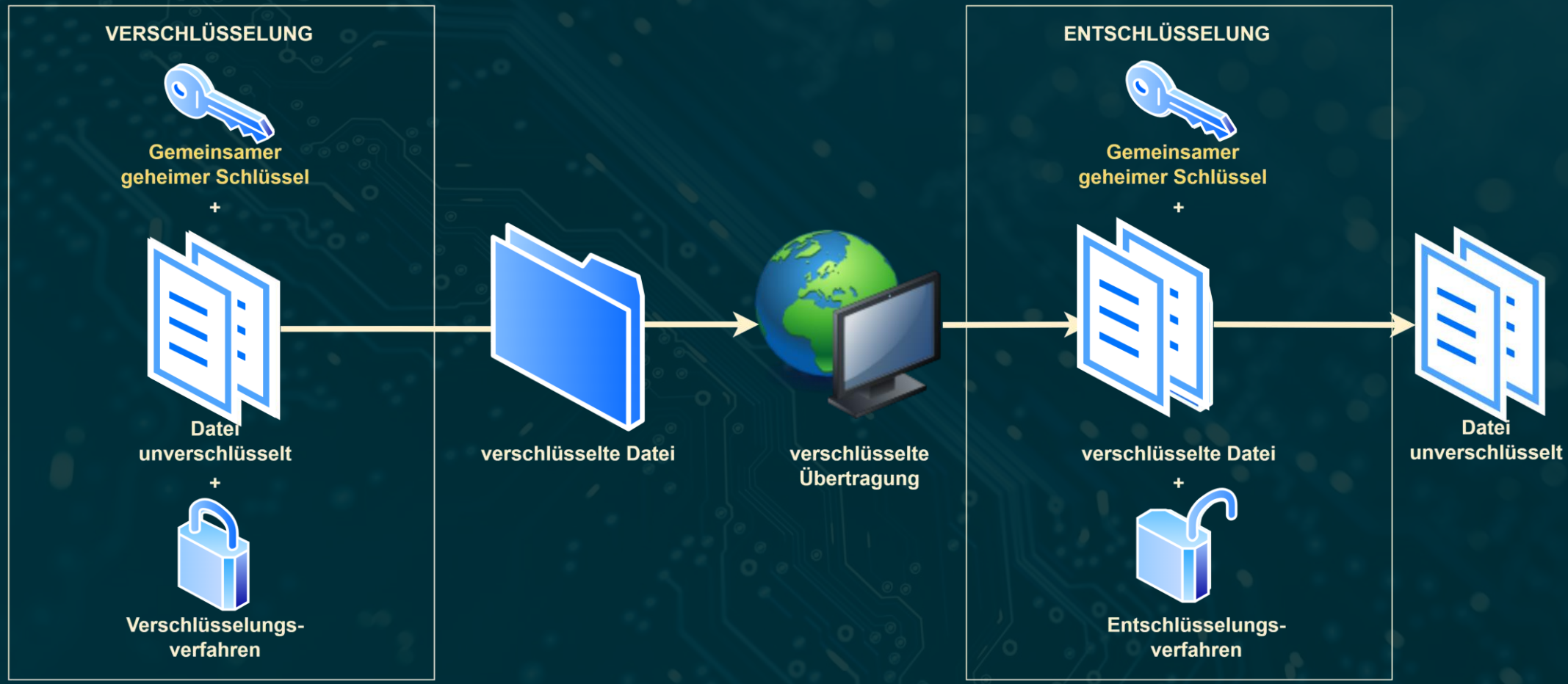
NACHTEIL

- ein sicherer Kanal für den Schlüsselaustausch erforderlich

Verschlüsselungsalgorithmen:

- AES (Advanced Encryption Standard)
- 3DES
- Twofish
- DES (Data Encryption Standard)
- Blowfish
- RC4

SYMMETRISCHE VERSCHLÜSSELUNG



ASYMMETRISCHE VERSCHLÜSSELUNG

- Public-Key-Verschlüsselungsverfahren
- Ein Schlüsselpaar für Ver- und Entschlüsselung :
  - Öffentlicher Schlüssel/Public-Key (Verschlüsselung)
  - Privater Schlüssel/Private-Key (Entschlüsselung)

VORTEIL

- nur ein privater Schlüssel für alle Kommunikationsverbindungen

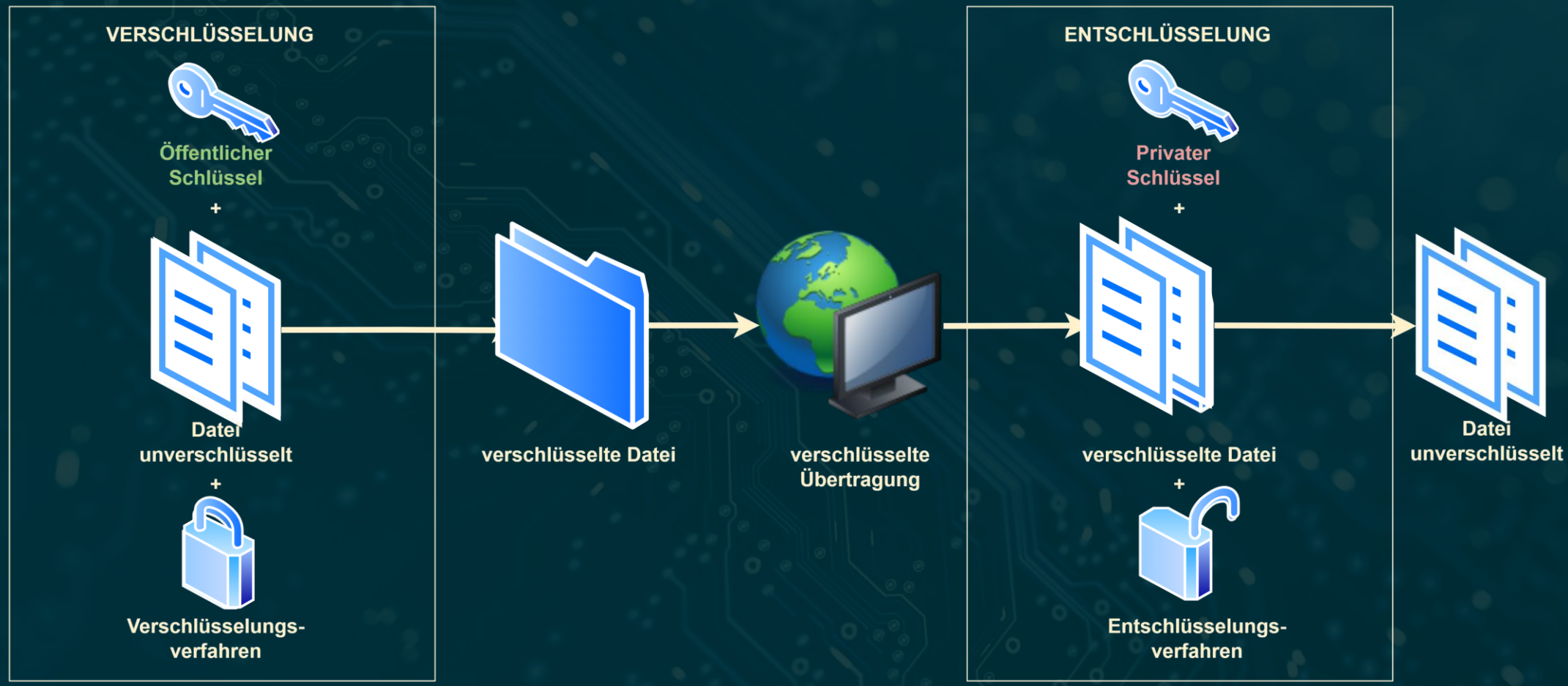
NACHTEIL

- die Schlüsselerzeugung ist aufwändig
- langsam
- für große Datenmengen nicht geeignet

Verschlüsselungsalgorithmen:

- RSA (Rivest-Shamir-Adleman)
- DSA (Digital Signature Algorithm)
- ECC (Elliptic Curve Cryptography)
- Diffie-Hellman (DH)
- ElGamal

ASYMMETRISCHE VERSCHLÜSSELUNG



GEGENSEITIGE ERGÄNZUNG VON SYMMETRISCHER UND ASYMMETRISCHER VERSCHLÜSSELUNG

Symmetrische und asymmetrische Verschlüsselung ergänzen sich gegenseitig durch ihre unterschiedlichen Stärken und Schwächen, was zu einer robusteren und sichereren Kommunikationsinfrastruktur führt.

Diese Kombination ermöglicht:

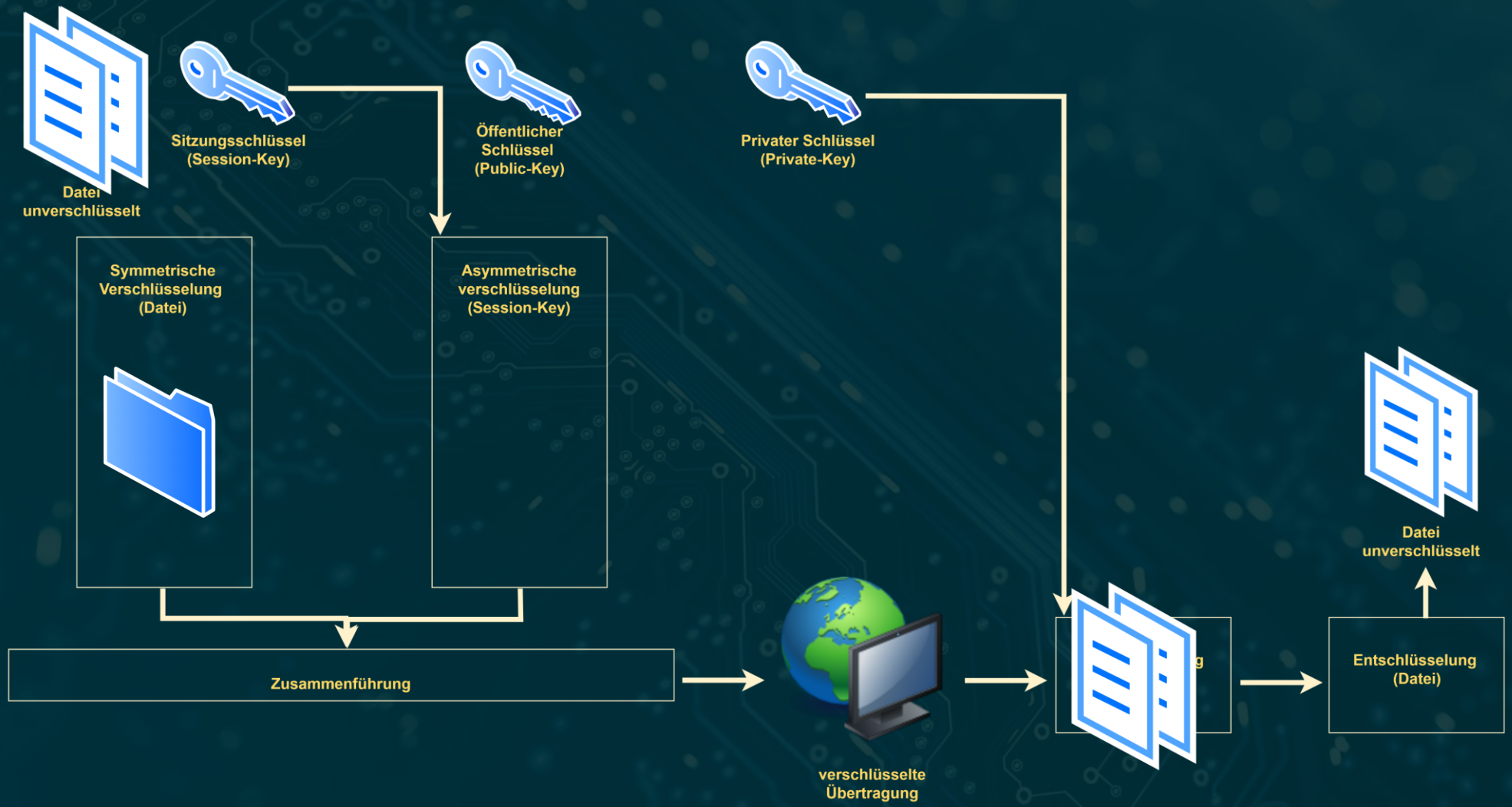
- **effiziente Datenübertragung**

  (durch **symmetrische** Verschlüsselung)

- **hoher Sicherheit der Schlüsselverteilung**

  (durch **asymmetrische** Verschlüsselung)

GEGENSEITIGE ERGÄNZUNG VON SYMMETRISCHER UND ASYMMETRISCHER VERSCHLÜSSELUNG



ANWENDUNGSFÄLLE

Sichere Datenübertragung in der Kommunikation

- TLS/SSL (Transport Layer Security / Secure Sockets Layer)
- PGP (Pretty Good Privacy) für E-Mail
- S/MIME (Secure/Multipurpose Internet Mail Extensions)
- IPSec (Internet Protocol Security)
- GPG (GNU Privacy Guard)
- Signal Protocol

Digitale Signatur und Authentifizierung

- Code-Signierung
- Zahlungssystemen
- Authentifizierung in mobilen
- Elektronische Dokumente und Verträge (z.B. DocuSign, Adobe Sign)

Hybride Kryptosysteme in Zahlungsprotokollen

- EMV-Chipkarten (Europay, MasterCard, Visa)
- SEPA (Single Euro Payments Area) Online-Überweisungen
- Apple Pay und Google Wallet

Sicherer Dateiaustausch in Cloud-Speicherdiensten

- Dropbox
- Microsoft OneDrive
- Google Drive

VERWENDETE LITERATUR

- **Westermann Gruppe, Heinrich Hübscher, Hans-Joachim Petersen, Carsten Rathgeber, Klaus Richter, Dirk Scharf, Nils Hinkelthein, Hannes Rewald: IT-Handbuch Technik (2022)**

  Verfügbar unter: https://www.westermann.de/artikel/978-3-14-235084-4/IT-Handbuch-Technik
- **GDATA CyberDefense AG, Janine Plickert: Was ist eigentlich Kryptographie?**

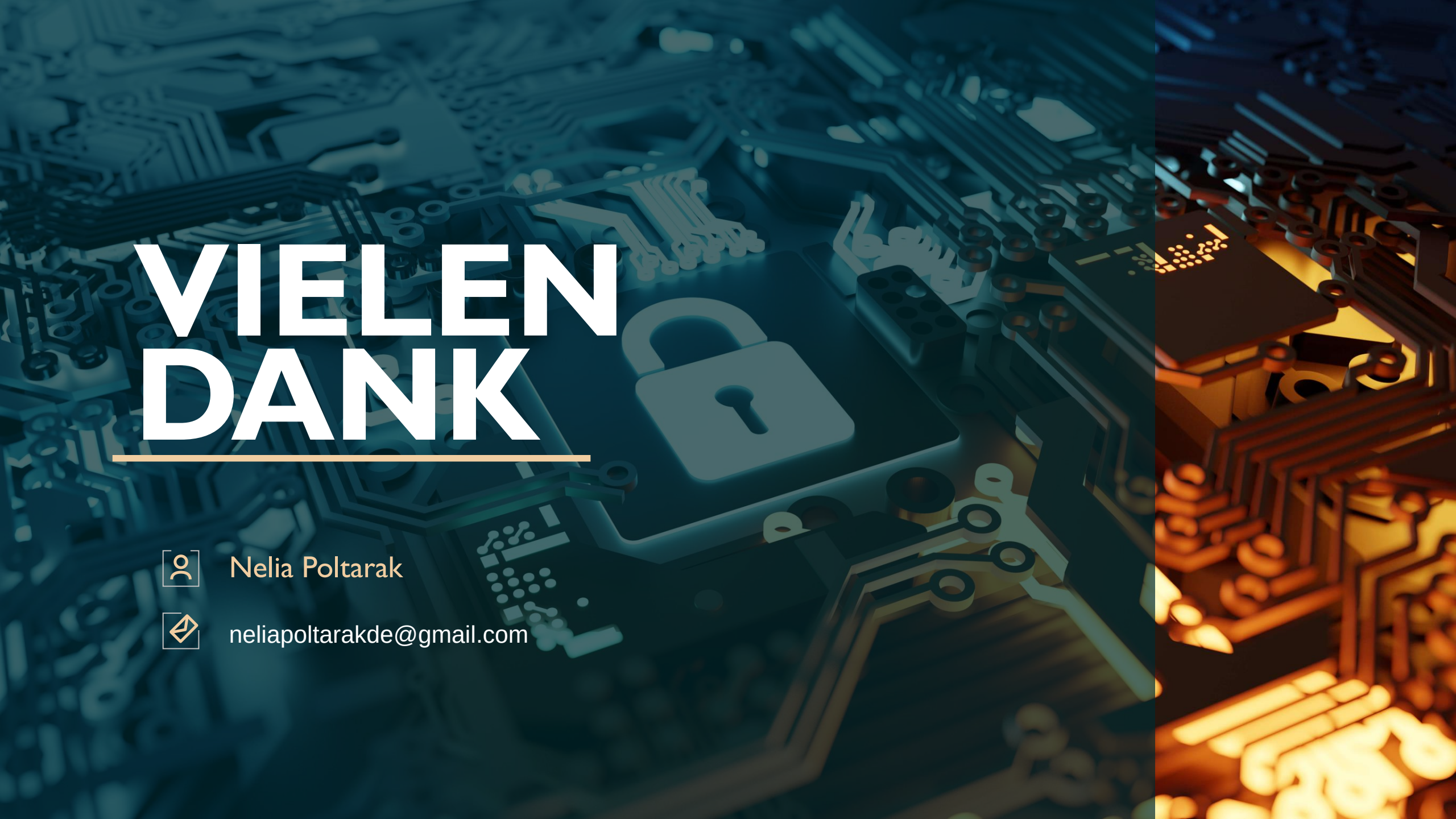
  Verfügbar unter: https://www.gdata.de/ratgeber/was-ist-eigentlich-kryptographie
- **CHIP, Tim Aschermann: Kryptographie einfach erklärt (2018)**

  Verfügbar unter: https://praxistipps.chip.de/kryptographie-einfach-erklaert_102083
- **Prim'X: Why Two Types of Encryption?**

  Verfügbar unter: https://www.primx.eu/en/tech-culture/symmetric-and-asymmetric-why-two-types-of-encryption/
- **Certera, Janki Mehta: Symmetric vs Asymmetric Encryption**

  Verfügbar unter: https://www.certera.com/blog/symmetric-vs-asymmetric-encryption-detailed-guide/
- **OpenAI (2024) ChatGPT-4o (Multimodal AI Model)**

  Verfügbar unter: https://chat.openai.com/chat



VIELEN DANK

Nelia Poltarak

neliapoltarakde@gmail.com