

# **Symmetric Encryption**

**Symmetrisches Verschlüsselung**

**23.01.2024, Lili Wilson**

# Vocabulary

<i>Auf Englisch</i>	<i>Auf Deutsch</i>
Encryption	
Encrypt	
Decrypt	
Key	
Plaintext	
Ciphertext	
Security	
Attacks	

# What is encryption? (*Verschlüsselung*)



***encrypt***

*(verschlüsseln)*



c0535e4be2b79ffd  
93291305436bf889  
314e4a3faec05ecff  
cbb7df31ad9e51a



***decrypt***

*(entschlüsseln)*



Hello world!

***plaintext***

*(Klartext)*

Hello world!

***ciphertext***

*(Geheimtext)*

# Why encrypt?

- **Security** (Sicherheit)
- **Privacy** (Privatsphäre)
- Protect **data** in *transit* and at *rest* from **attacks** (Angriffe)

# Vocabulary

<i>Auf Englisch</i>	<i>Auf Deutsch</i>
Encryption	Verschlüsselung
Encrypt	Verschlüsseln
Decrypt	Entschlüsseln
Key	Schlüssel
Plaintext	Klartext
Ciphertext	Geheimtext
Security	Sicherheit
Attacks	Angriffe

# What does this mean?

LQM KIMAIZ DMZAKPTCMAAMTCVO WLMZ KIMAIZ KPQNNZM QAB MQV  
AGUUMBZQAKPMA DMZAKPTCMAAMTCVOADMZNIPZMV , LIA ICN LMZ  
DMZAKPQMJCVO LMA ITXPIJMBA JIAQMZB. QV LQMAMZ ABCVLM OMPB  
MA LIZCU, EQM UIV UQB LMZ KIMAIZ DMZAKPTCMAAMTCVO MQVMV  
BMFB DMZAKPTCMAAMTV CVL EQMLMZ MVBAKPTCMAAMTV SIVV CVL WJ  
UIV LIA DMZNIPZMV ITA AQKPMZ MQVABCNMV SIVV.

# What does this mean?

LQM KIMAIZ DMZAKPTCMAAMTCVO WLMZ KIMAIZ KPQNNZM QAB MQV  
AGUUMBZQAKPMA DMZAKPTCMAAMTCVOADMZNIPZMV , LIA ICN LMZ  
DMZAKPQMJCVO LMA ITXPIJMBA JIAQMZB. QV LQMAMZ ABCVLM OMPB  
MA LIZCU, EQM UIV UQB LMZ KIMAIZ DMZAKPTCMAAMTCVO MQVMV  
BMFB DMZAKPTCMAAMTV CVL EQMLMZ MVBAKPTCMAAMTV SIVV CVL WJ  
UIV LIA DMZNIPZMV ITA AQKPMZ MQVABCNMV SIVV.

*Hint: the letter “E” is the most common letter in German*

# What does this mean?

LQM KIMAIZ DMZAKPTCMAAMTCVO WLMZ KIMAIZ KPQNNZM QAB MQV  
AGUUMBZQAKPMA DMZAKPTCMAAMTCVOADMZNIPZMV , LIA ICN LMZ  
DMZAKPQMJCVO LMA ITXPIJMBA JIAQMZB. QV LQMAMZ ABCVLM OMPB  
MA LIZCU, EQM UIV UQB LMZ KIMAIZ DMZAKPTCMAAMTCVO MQVMV  
BMFB DMZAKPTCMAAMTV CVL EQMLMZ MVBAKPTCMAAMTV SIVV CVL WJ  
UIV LIA DMZNIPZMV ITA AQKPMZ MQVABCNMV SIVV.

*Hint: the letter “E” is the most common letter in German*

*Hint: you can use **Strg** + **F** to count the number of times a letter appears in Word*



# What does this mean?

DIE CAESAR VERSCHLUESSELUNG ODER CAESAR CHIFFRE IST EIN SYMMETRISCHES VERSCHLUESSELUNGSVERFAHREN , DAS AUF DER VERSCHIEBUNG DES ALPHABETS BASIERT. IN DIESER STUNDE GEHT ES DARUM, WIE MAN MIT DER CAESAR VERSCHLUESSELUNG EINEN TEXT VERSCHLUESSELN UND WIEDER ENTSCHLUESSELN KANN UND OB MAN DAS VERFAHREN ALS SICHER EINSTUFEN KANN.

# Caesar Cipher

A form of *symmetric* encryption, shift letters by a number **x**.

Both the sender and the receiver need to know the value of **x** to **encode** and **decode** things properly.

*If you want to learn more about encryption or cybersecurity...*

Donnerstag 25.01, 14:00, Rm. 011

**Intro to cybersecurity: passwords** (with me!)

# Caesar CIPHER *(implementation)*

Caesar-Chiffre *(Implementierung)*

25.01.2024, Lili Wilson

# Vocabulary Review

<i>Auf Englisch</i>	<i>Auf Deutsch</i>
Encryption	Verschlüsselung
Encrypt	Verschlüsseln
Decrypt	Entschlüsseln
Key	Schlüssel
Plaintext	Klartext
Ciphertext	Geheimtext
Security	Sicherheit
Attacks	Angriffe
Caesar Cipher	Caesar Chiffre

# Implementing the Caesar Cipher: Struktogramm



# Implementing the Caesar Cipher: Struktogramm

```
leeren String geheimtext anlegen
```

# Implementing the Caesar Cipher: Struktogramm

leeren String geheimtext anlegen

für jeden Buchstaben des Klartexts von links nach rechts



# Implementing the Caesar Cipher: Struktogramm

leeren String geheimtext anlegen

für jeden Buchstaben des Klartexts von links nach rechts

lokale Variable buchstabe mit diesem Buchstaben belegen

# Implementing the Caesar Cipher: Struktogramm

leeren String geheimtext anlegen

für jeden Buchstaben des Klartexts von links nach rechts

lokale Variable buchstabe mit diesem Buchstaben belegen

der lokalen int-Variablen y diesen buchstaben zuweisen

# Implementing the Caesar Cipher: Struktogramm

leeren String geheimtext anlegen

für jeden Buchstaben des Klartexts von links nach rechts

lokale Variable buchstabe mit diesem Buchstaben belegen

der lokalen int-Variablen y diesen buchstaben zuweisen

von y 65 abziehen (damit A mit 0 gleichgesetzt wird)

# Implementing the Caesar Cipher: Struktogramm

leeren String geheimtext anlegen

für jeden Buchstaben des Klartexts von links nach rechts

lokale Variable buchstabe mit diesem Buchstaben belegen

der lokalen int-Variablen y diesen buchstaben zuweisen

von y 65 abziehen (damit A mit 0 gleichgesetzt wird)

die lokale Variabel z auf  $(y + \text{schluessel}) \bmod 26$  setzen



# Implementing the Caesar Cipher: Struktogramm

leeren String geheimtext anlegen

für jeden Buchstaben des Klartexts von links nach rechts

lokale Variable buchstabe mit diesem Buchstaben belegen

der lokalen int-Variablen y diesen buchstaben zuweisen

von y 65 abziehen (damit A mit 0 gleichgesetzt wird)

die lokale Variabel z auf  $(y + \text{schluessel}) \bmod 26$  setzen

zu z wieder 65 addieren

# Implementing the Caesar Cipher: Struktogramm

leeren String geheimtext anlegen

für jeden Buchstaben des Klartexts von links nach rechts

lokale Variable buchstabe mit diesem Buchstaben belegen

der lokalen int-Variablen y diesen buchstaben zuweisen

von y 65 abziehen (damit A mit 0 gleichgesetzt wird)

die lokale Variabel z auf  $(y + \text{schluessel}) \bmod 26$  setzen

zu z wieder 65 addieren

z in den entsprechenden Großbuchstaben c umwandeln



# Implementing the Caesar Cipher: Struktogramm

leeren String geheimtext anlegen

für jeden Buchstaben des Klartexts von links nach rechts

lokale Variable buchstabe mit diesem Buchstaben belegen

der lokalen int-Variablen y diesen buchstaben zuweisen

von y 65 abziehen (damit A mit 0 gleichgesetzt wird)

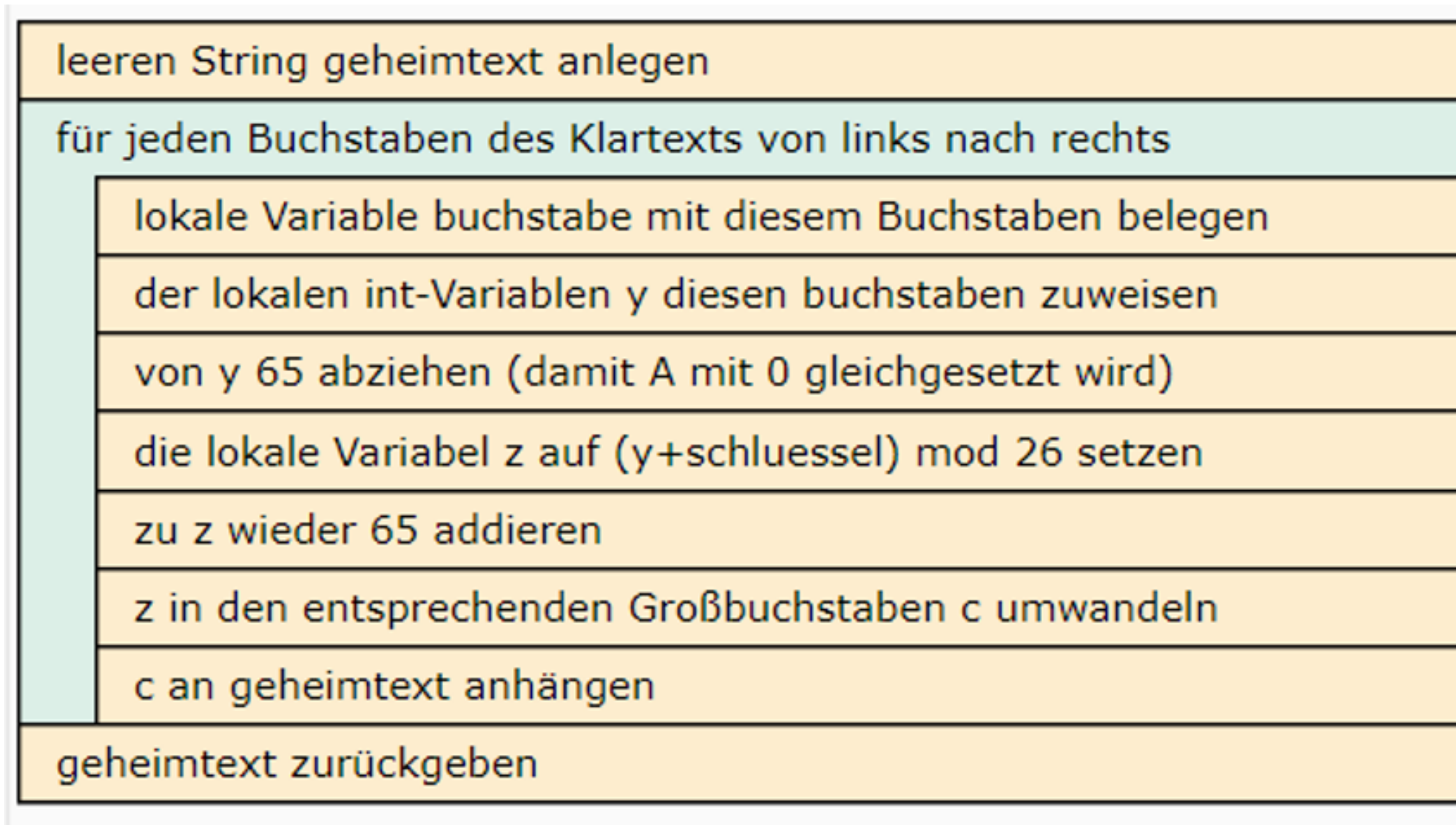
die lokale Variabel z auf  $(y + \text{schluessel}) \bmod 26$  setzen

zu z wieder 65 addieren

z in den entsprechenden Großbuchstaben c umwandeln

c an geheimtext anhängen

# Implementing the Caesar Cipher: Struktogramm





*If you want to learn more about encryption or cybersecurity...*

Heute 25.01, 14:00, Rm. 011

**Intro to cybersecurity: passwords** (with me!)