Codierung und Verschlüsselung

Codierung

→ siehe Präsentation Einführung Codierung

Codierung ist ein Regelwerk um Informationen in einer bestimmten Weise darzustellen. Beispiele:

Binär-, Dezimal- und Hexadezimalsystem

→ siehe Präsentation zu Stellenwertsysteme & Speichergrößen

Zahlen werden über das ***Stellenwertsystem*** dargestellt, bei dem die Wertigkeit eines Symbols/Ziffer von ihrer Position abhängt:

Beispiel: 127

> Die Ziffer 1 ist kleiner als die 2 aber an der dritten Stelle von rechts stellt die 1 die Ziffer 1 den Wert 100 dar und die 2 an der zweiten Stelle von rechts nur den Wert 20.

Hinweis: Das Vorgehen zum schriftlichen Addieren, Subtrahieren, Multiplizieren und Dividieren aus der Grundschule ist auf alle Zahlen anwendbar, die mit dem Stellenwertsystem dargestellt sind.

Es gibt auch Zahlendarstellungen, die nicht durch das Stellenwertsystem dargestellt sind: z.B. ***römische Zahlen MCMLXXXIV = 1984***

Dez	Bin	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Der Wert einer Zahl wird im Stellenwertsystem folgendermaßen berechnet:

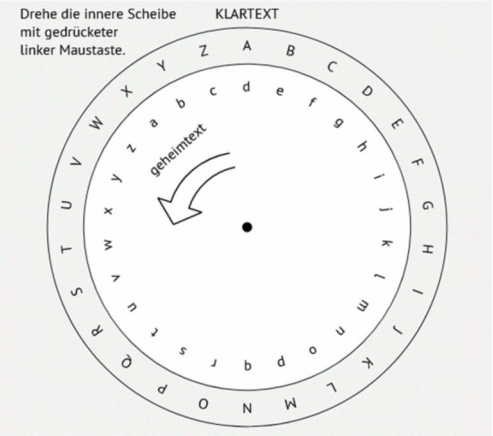
$$\ldots\ a_3 \cdot b^3 + a_2 \cdot b^2 + a_1 \cdot b^1 + a_0 \cdot b^0 = \sum_{i=0}^{n} a_i b^i$$

wobei a die einzelnen Ziffern einer Zahl darstellen und b die Basis/Ziffernvorrat für eine Stelle vorgibt.

- ***Dezimalsystem***: b = 10, also 10 verschiedene Ziffern 0,…,9
- ***Binärzahlen***/Dualsystem: b = 2, also 2 verschiedene Ziffern 0 und 1
- ***Hexadezimalsystem***: b = 16, also 16 verschiedene Ziffern von 0,…,9,a,…,f. Da wir aber kein einzelnes Zeichen für die Ziffern über 10 kennen, bedient man sich hier der Buchstaben: a=10, b=11, c=12, d=13, e=14, f=15 (usw. bei noch höheren Basen)

Beispiele:

- $5c8_{16} = 5 * 16^2 + 12 * 16 + 8 = 1480_{10}$
- $1001_{16} = 1 * 2^3 + 0 * 2^2 + 0 * 2 + 1 = 9_{10}$



Caesar-Verschlüsselung

Die ***Caesar-Verschlüsselung*** ist ein einfaches Verschlüsselungsverfahren, welche die zu verschlüsselnden Buchstaben um eine bestimmte Anzahl zyklisch verschiebt.

https://www.inf-schule.de/kids/datennetze/verschluesselung/caesar

Aufgabe:

a) Denke dir ein Wort aus. Verschiebe die Caesar-Scheibe auf eine bestimmte Position.

Schreibe als erstes auf den Zettel, um wie viele Buchstaben du verschiebst.

Schreibe anschließend das verschlüsselte Wort auf den Zettel und gib ihn ab.

Ziehe einen Zettel und entschlüssle das Wort.

b) Öffne die Excel-Datei Caesar Vorlage und vollziehe die 6 Berechnungsschritte der Verschlüsselungsformel nach. Nutze die Formel um anschließend den Ausgabebereich zu implementieren.

c) Implementiere die Caesar-Verschlüsselung in Java. → Modulo-Problematik

QR-Codes decodieren

Aufgabe:

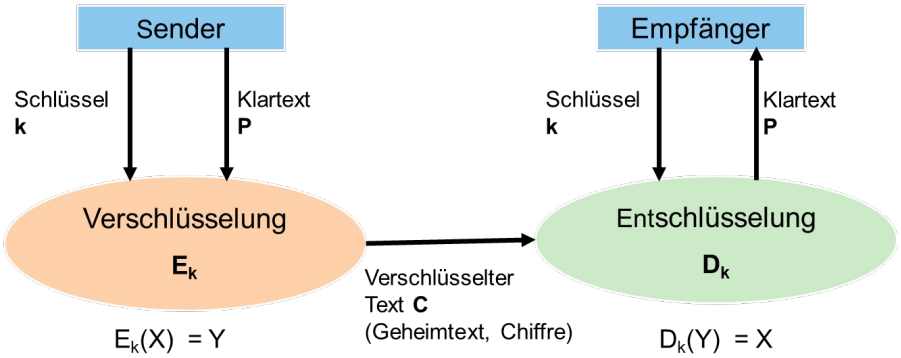
a) Sieh dir dieses Video zur Einführung an.
https://www.youtube.com/watch?v=yiLjWBfQyF4

b) Öffne die **Präsentation zu Decodierung von QR-Codes** und öffne das BlueJ-Projekt „**QR-Test BlueJ**“ und erstelle ein Objekt von QR.

Löse mithilfe der Präsentation die Aufgaben des QR-Tests in BlueJ und decodiere den QR-Code!

Symmetrische vs. asymmetrische Verschlüsselung

→ siehe Präsentation Asym. Verschlüsselung & RSA



P = plain text (Klartext)

C = cipher text (Geheimtext, Schlüsseltext)

k = key (Schlüssel für die Ver-/Entschlüsselungsfunktion)

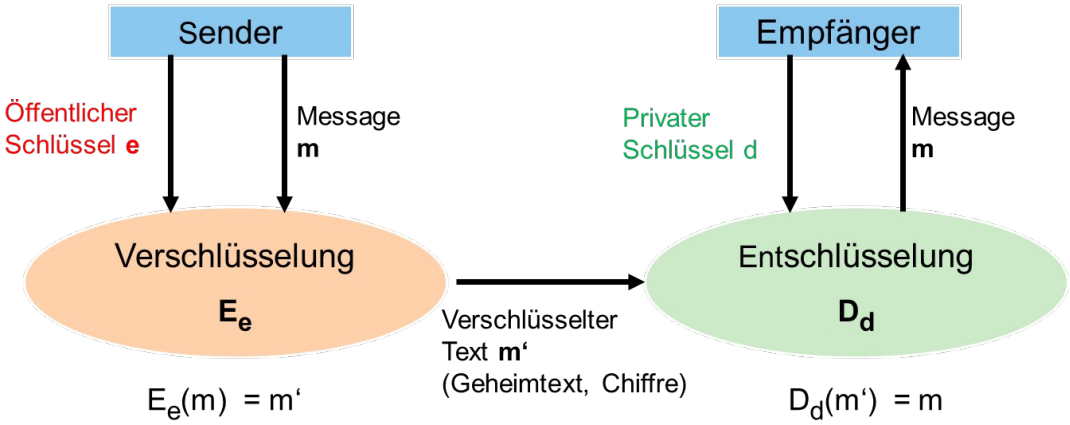
E = encrypt (Verschlüsselungsfunktion)

D = decrypt (Entschlüsselungsfunktion)

Entschlüsselungsgleichung::

$$D_k(E_k(P)) = P$$

Gleicher Schlüssel zur Ver- und Entschlüsselung → symmetrische Verschlüsselung



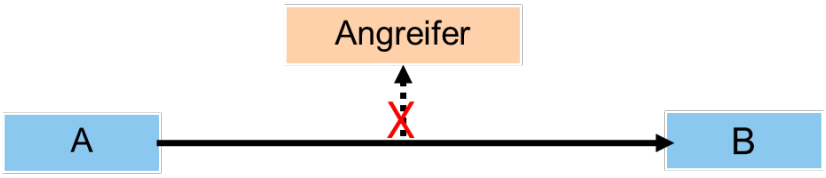
$$D_d(E_e(m)) = m$$

Öffentlicher Schlüssel e zum Verschlüsseln & **privater Schlüssel d** zum Entschlüsseln
→ ***Asymmetrische Verschlüsselung***

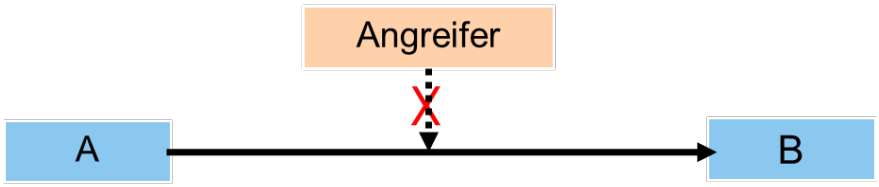
Digitales Signieren, kryptografische Hashfunktion und Zertifikate

→ **siehe Präsentation DS, kH & Z**

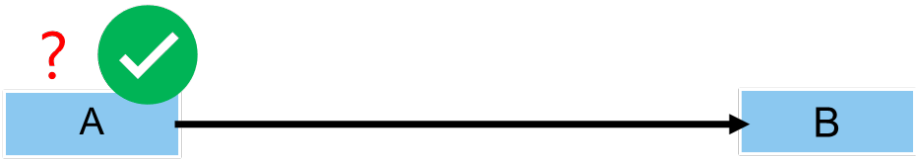
Vertraulichkeit: Nur B kann die Nachricht lesen.



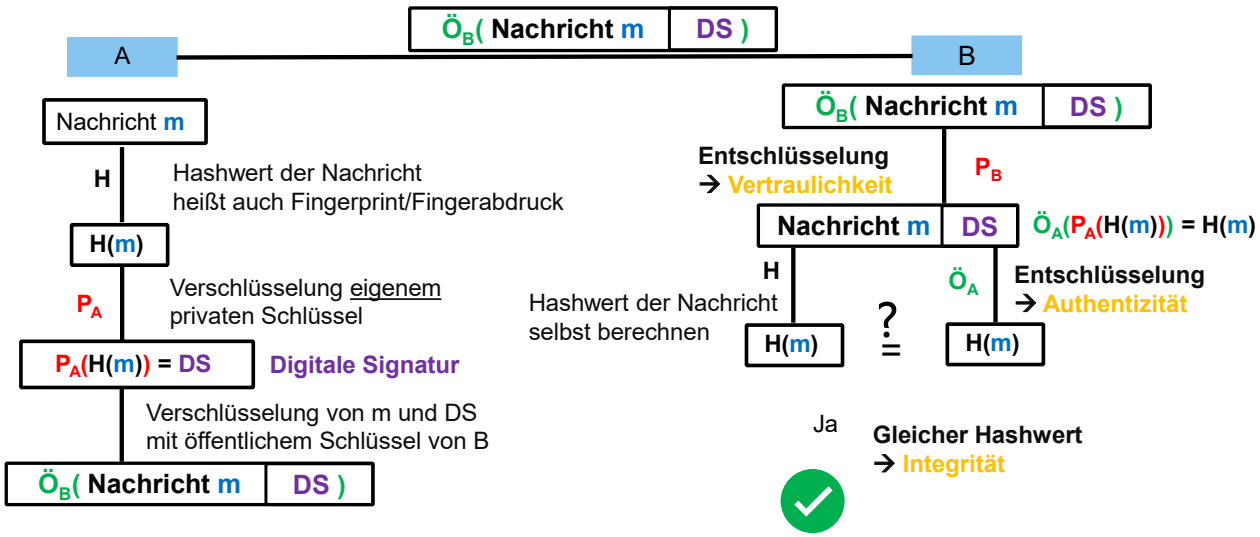
Integrität: Die Nachricht ist vollständig und unverändert.



Authentizität: B weiß sicher, dass der Absender A ist.



Sicheres Verschicken von Nachrichten



Vertiefungsbereich zu Codierung & Verschlüsselung

Optionale Verschlüsselungen für ganz Schnelle

Vigenère-Verschlüsselung

Die Vigenère-Verschlüsselung ist eine aus dem 16. Jahrhundert stammende Methode zu Verschlüsselung von Texten. Der Schlüssel ist hierbei keine Zahl (wie bei Caesar), sondern ein anderes Wort/Text, welches wiederholt genutzt wird, wenn der Klartext länger als das Schlüsselwort ist.

Mithilfe des Vigenère-Quadrats kann man dann den Text verschlüsseln. Beispiel:

Klartext: HALLO
Schlüssel: ABC

Verschlüsselung:

HALLO
ABCAB
→ HBNLP

Falls das Quadrat zu aufwändig erscheint, man kann auch den Buchstaben Werte geben, um welche der Buchstabe im Alphabet verschoben wird:

H + A (=0) = H
A + B (=1) = B
L + C (=2) = N
L + A (=0) = L
O + B (=1) = P

Vigenère-Quadrat

Schlüssel	Klartext: A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Geheimtext
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	

Erweitere deine Caesar-Verschlüsselung um die Klasse ***VIGENERE*** und implementiere analog die Methoden ***zeichenVerschlüsseln()/zeichenEntschlüsseln()*** sowie ***vigenereVerschlüsseln()/vigenereEntschlüsseln()***.

Knacken der Vigenère-Verschlüsselung

Die Vigenère-Verschlüsselung zu knacken ist im Vergleich zur Caesar-Verschlüsselung deutlich aufwändiger und erfolgt in mehreren Schritten:

Länge des Schlüsselworts ermitteln

Im Deutschen gibt es Wörter die relativ oft vorkommen: z. B. der, die, das, ein, eine usw.

Daher wird es bei einem längeren verschlüsselten Text öfter vorkommen, dass das Schlüsselwort exakt gleich auf die Klartextwörter (der, die, das, …) angewendet wird und somit auf der Schlüsseltext mehrere gleiche Wörter aufweist.

Hier ermittelt man jetzt die Abstände (=Anzahl der Zeichen) zwischen den jeweils gleich auftauchenden Schlüsseltextwörtern.

Der größte gemeinsamer Teiler dieser Abstände ist dann vermutlich die Länge des Schlüsselworts.

Aufteilen des Schlüsseltexts

Sobald man die vermutete Schlüssellänge ermittelt hat, teilt man den Schlüsseltext auf. Beispiel mit vermuteter Schlüssellänge von 7:

- Damit wäre das Zeichen an der Stelle 0, 7, 14, … im Klartext mit demselben Buchstaben verschlüsselt worden.
- Analog gilt das für die Zeichen im Text an der Stelle 1, 8, 15, …
- Oder für die Zeichen 2, 9, 16, … usw. bis 6, 13, 20, … usw.

Der Text wird hier im Beispiel dann in 7 Teiltexte aufgeteilt, sodass die Teiltexte alle Zeichen enthält, die mit demselben Buchstaben des Schlüsselworts verschlüsselt wurden.

Entschlüsseln des Texts

Die Teiltexte sind letztendlich jetzt „nur noch“ Caesar-verschlüsselt. Damit kann man eine Häufigkeitsanalyse durchführen und anhand dieser die jeweils einzelne Verschiebung der Teiltexte ermitteln. So kann man das Schlüsselwort erhalten und den Schlüsseltext anschließend entschlüsseln.

Öffne das BlueJ-Projekt ***Vigenere Vorlage*** und führe diese Schritte anhand der beiden Schlüsseltexte durch.