JOHANN HEINRICH PESTALOZZI GYMNASIUM

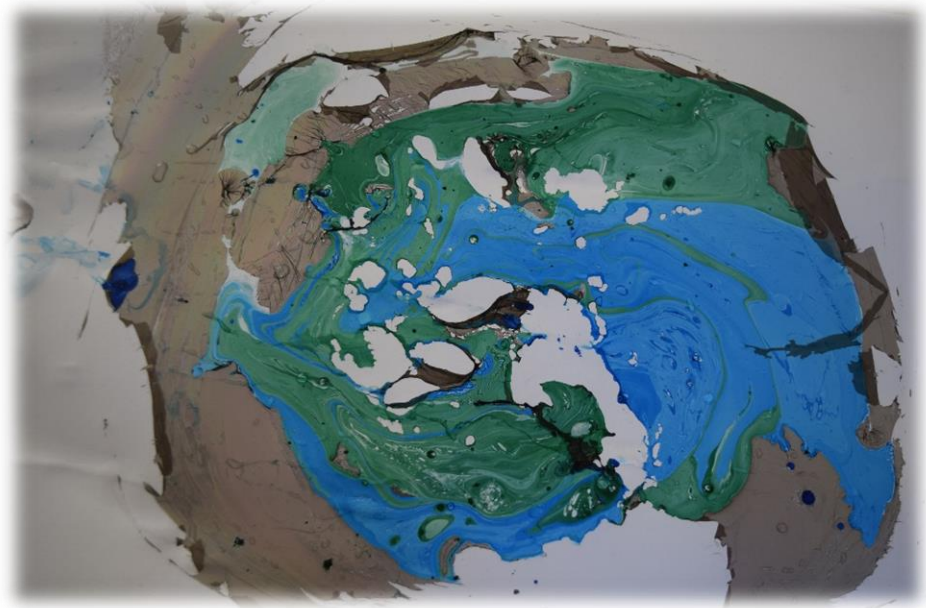
www.pesta-rodewisch.de

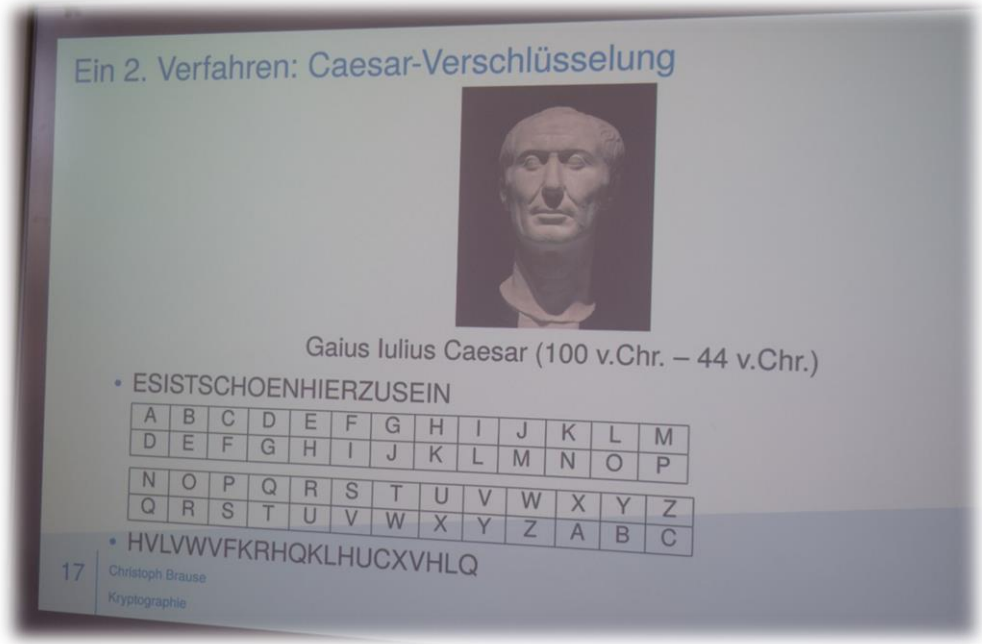
08228 Rodewisch · Str. des Friedens 5 · Tel.: 03744/189880

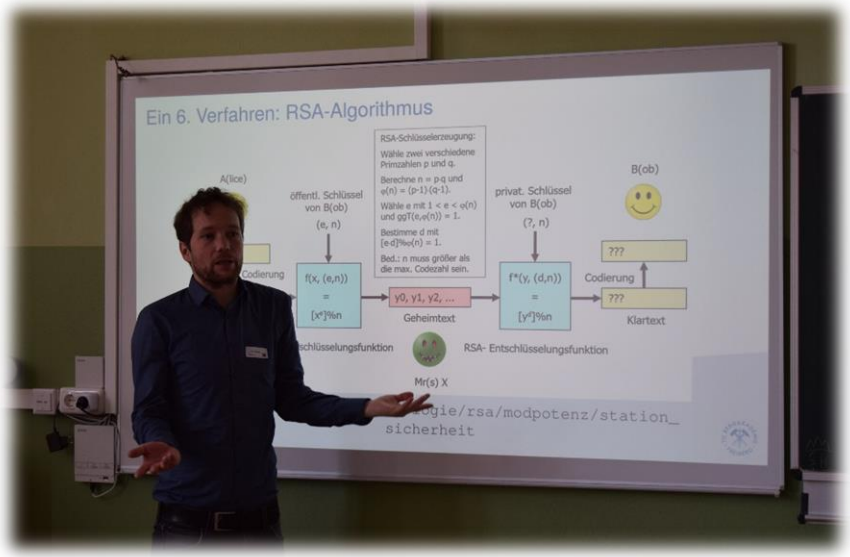
LERNCAMP 2025

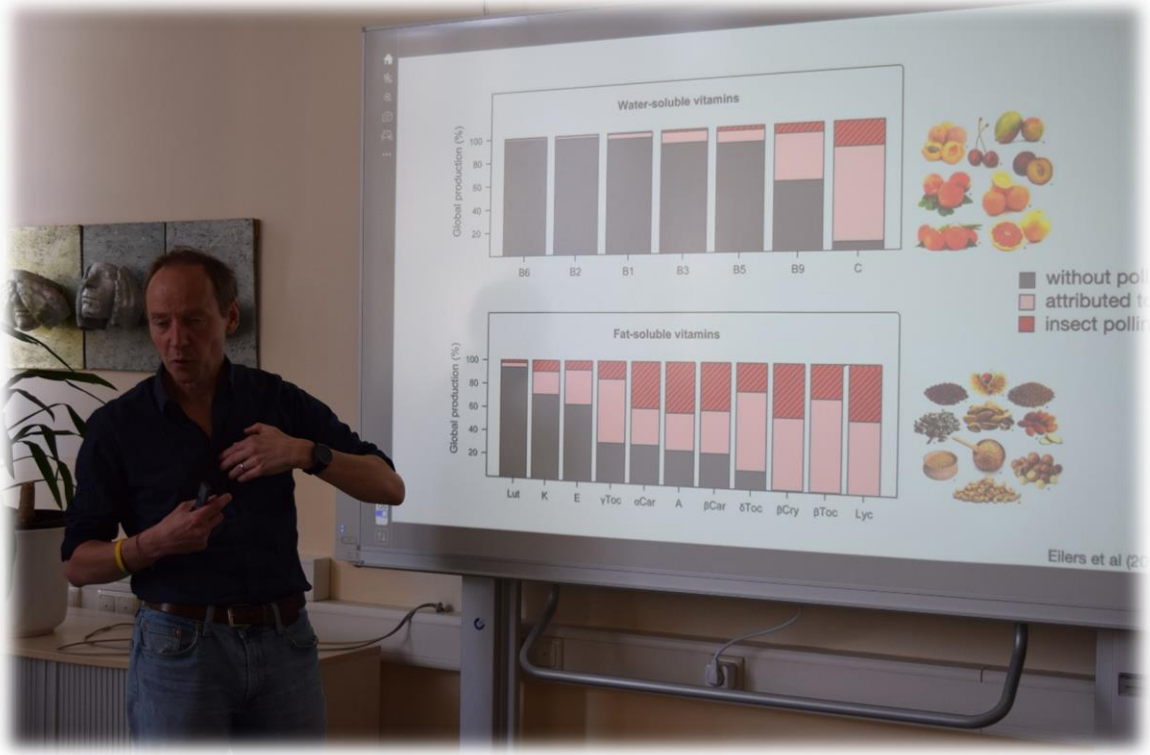
GYMNASIUM MARKNEUKIRCHEN

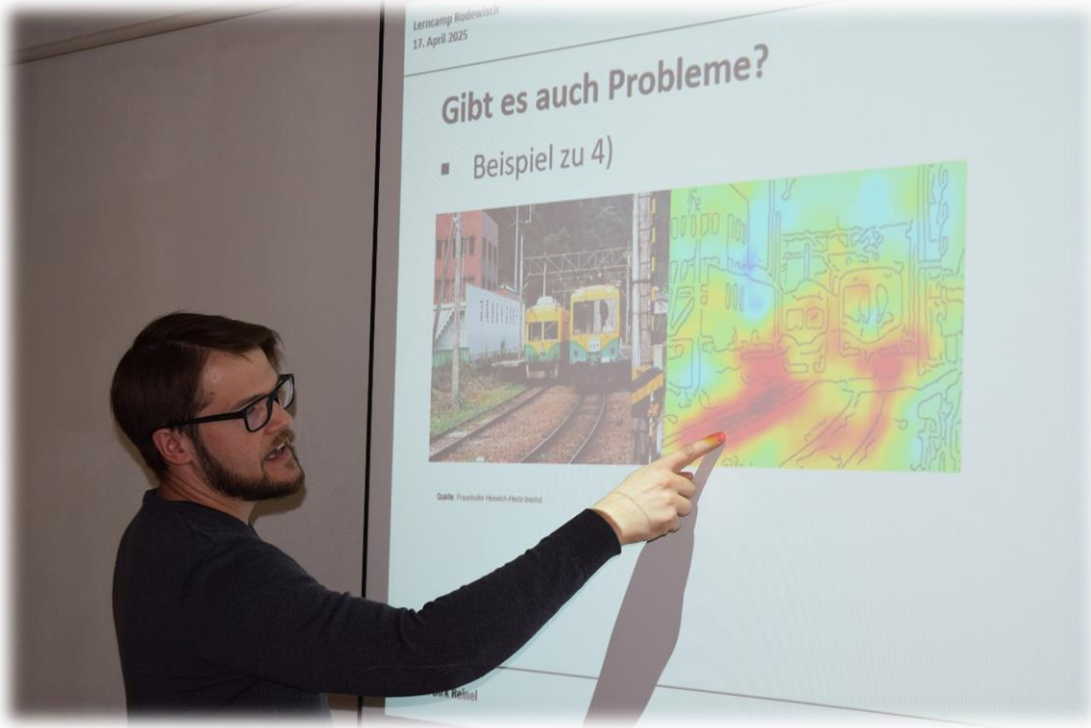

FLIEßEN
TÖTEN
ERODIEREN
Carlfriedrich Claus (1930-1998)




Ein 2. Verfahren: Caesar-Verschlüsselung
Gaius Iulius Caesar (100 v.Chr. – 44 v.Chr.)
ESISTSCHOENHIERZUSEIN
A B C D E F G H I J K L M
D E F G H I J K L M N O P
N O P Q R S T U V W X Y Z
Q R S T U V W X Y Z A B C
HVLVWVFKRHQKLHUCXVHLQ
17
Christoph Brause
Kryptographie


Ein 6. Verfahren: RSA-Algorithmus
RSA-Schlüsselerzeugung:
Wähle zwei verschiedene Primzahlen p und q.
Berechne n = p·q und φ(n) = (p-1)·(q-1).
Wähle e mit 1 < e < φ(n) und ggT(e,φ(n)) = 1.
Bestimme d mit [e·d]%φ(n) = 1.
Bed.: n muss größer als die max. Codezahl sein.
A(lice)
B(ob)
öffentl. Schlüssel von B(ob)
(e, n)
privat. Schlüssel von B(ob)
(?, n)
Codierung
f(x, (e,n)) = [x^e]%n
y0, y1, y2, ...
Geheimtext
f*(y, (d,n)) = [y^d]%n
???
Klartext
RSA- Entschlüsselungsfunktion
Mr(s) X
sicherheit


Water-soluble vitamins
Global production (%)
100
80
60
40
20
B6
B2
B1
B3
B5
B9
C
without pol
attributed t
insect pollin
Fat-soluble vitamins
Global production (%)
100
80
60
40
20
Lut
K
E
γToc
αCar
A
βCar
δToc
βCry
βToc
Lyc
Eilers et al (2


Lerncamp Rodewisch
17. April 2025
Gibt es auch Probleme?
Beispiel zu 4)