

## Verschlüsselung im Einsatz

### Caesar Verschlüsselung - Arbeitsphase 1:

- Nehmt euch jeder ein gelbes Kärtchen und ein weißes Kärtchen.
- Auf das weiße Kärtchen schreibt ihr euren Schlüssel.
- Auf das gelbe Kärtchen schreibt ihr euren mit der **Caesar-Verschlüsselung** verschlüsselten Text.

### Caesar Verschlüsselung - Arbeitsphase 2:

- Tauscht mit eurem Teampartner/in zuerst die Schlüssel (weiße Kärtchen) aus.
- Danach tauscht mit eurem Teampartner/in die verschlüsselten Nachrichten (gelbe Kärtchen) aus.
- Jede/r entschlüsselt die erhaltene Nachricht.
- Überlegt nun, welche eurer Übertragungen abgefangen werden müssten, damit ein AngreiferIn eure Kommunikation mitlesen kann.
- Was könnte ein AngreiferIn mit euren jeweiligen Übertragungen anstellen? Diskutiert mit euren Teammitgliedern.

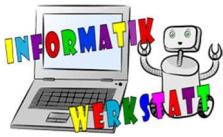
### Vorbereitung RSA-Verfahren: ASCII-Codierung

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

HALLO = 72 65 76 76 79

### RSA – Verfahren Arbeitsphase 1:

- Arbeitet zu zweit auf einem Rechner!
- Jeder benötigt ein Schlüsselpaar.  
Notiert öffentlichen (grünes Kärtchen) und privaten Schlüssel (rotes Kärtchen) jeweils auf ein Kärtchen. Tauscht dann die öffentlichen Schlüssel (grünes Kärtchen) mit eurem Gegenüber aus.
- Überlegt euch ein geheimes Wort, codiert es in ASCII-Code und schreibt den Code auf ein weißes Kärtchen.



## Vorbereitung RSA – Verfahren Arbeitsphase 2:

Schlüsselpaar	Öffentlich	Privat
Schlüsselpaar 1	Modul 91, Exponent 5	Modul 91, Exponent 29
Schlüsselpaar 2	Modul 143, Exponent 7	Modul 143, Exponent 103

Verschlüsselung:

$$(Nachricht)^{e\_exponent} \bmod \text{Modul} = V\_Nachricht$$

Entschlüsselung:

$$(V\_Nachricht)^{d\_exponent} \bmod \text{Modul} = Nachricht$$

- Verwendet den Taschenrechner und das **RSA-Verfahren**, um die ASCII-Codes mit dem öffentlichen Schlüssel zu verschlüsseln und schreibt den Geheimtext auf ein **gelbes** Kärtchen.
- Tauscht nun die Geheimtexte (**gelbe** Kärtchen) aus und versucht sie mit eurem privaten Schlüssel (**rote** Kärtchen) zu entschlüsseln.

## RSA – Verfahren Arbeitsphase 3:

- Arbeitet zu zweit auf einem Rechner!
- Verwendet die Verschlüsselungsverfahren auf <https://www.cryptool.org/de/cto-highlights/rsa-schritt-fuer-schritt>.
- Probiert unterschiedliche Kombinationen von Schlüsseln zum Ver- und Entschlüsseln aus! Macht euch Gedanken über öffentliche / private Schlüssel und über mögliche Angriffe.