**Aufgabe 1** Bildet eine Dreiergruppe und spielt den Diffie-Hellman-Algorithmus durch. Eine/r von euch ist Alice, eine/r Bob und der oder die Dritte ist Eve.
Alice und Bob tauschen den Schlüssel aus und Eve versucht den Schlüssel (K) herauszufinden, um die geheime Nachricht lesen zu können.
Führt den Algorithmus mit $p = 11$ und $g = 3$ ein- bis dreimal mit verschiedenen Rollen aus. Die unten stehende Tabelle ist euch beim Rechnen behilflich.
Notiert euer Ergebnis. Hat Eve den Schlüssel herausgefunden?

**Tabelle mit vorberechneten Werten für $x^y$:**

| $x$ \ $y$ | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| **1** | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| **2** | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024 |
| **3** | 3 | 9 | 27 | 81 | 243 | 729 | 2187 | 6561 | 19683 | 59049 |
| **4** | 4 | 16 | 64 | 256 | 1024 | 4096 | 16384 | 65536 | 262144 | 1048576 |
| **5** | 5 | 25 | 125 | 625 | 3125 | 15625 | 78125 | 390625 | 1953125 | 9765625 |
| **6** | 6 | 36 | 216 | 1296 | 7776 | 46656 | 279936 | 1679616 | 10077696 | 60466176 |
| **7** | 7 | 49 | 343 | 2401 | 16807 | 117649 | 823543 | 5764801 | 40353607 | 282475249 |
| **8** | 8 | 64 | 512 | 4096 | 32768 | 262144 | 2097152 | 16777216 | 134217728 | 1073741824 |
| **9** | 9 | 81 | 729 | 6561 | 59049 | 531441 | 4782969 | 43046721 | 387420489 | 3486784401 |
| **10** | 10 | 100 | 1000 | 10000 | 100000 | 1000000 | 10000000 | 100000000 | 1000000000 | 10000000000 |

Hinweis: Bei dieser Tabelle kann $x$ die Werte von $g$, $A$ oder $B$ und $y$ die Werte von $a$ oder $b$ annehmen.





v2 21. Juni 2015

**Aufgabe 1** **Berechne wie in den Beispielen auf dem Stationsblatt:**

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 25 | $mod$ | 7 | = | | , da | 25 | : | 7 | = | | , **Rest** | |
| 90 | $mod$ | 11 | = | | , da | 90 | : | 11 | = | | , **Rest** | |
| 23 | $mod$ | 8 | = | | , da | 23 | : | 8 | = | | , **Rest** | |
| 10 | $mod$ | 19 | = | | , da | 10 | : | 19 | = | | , **Rest** | |
| 106 | $mod$ | 21 | = | | , da | 106 | : | 21 | = | | , **Rest** | |
| 42 | $mod$ | 4 | = | | , da | 42 | : | 4 | = | | , **Rest** | |
| 8 | $mod$ | 3 | = | | , da | 8 | : | 3 | = | | , **Rest** | |
| 33 | $mod$ | 15 | = | | , da | | : | | = | | , **Rest** | |
| 107 | $mod$ | 25 | = | | , da | | : | | = | | , **Rest** | |
| 2180 | $mod$ | 54 | = | | , da | | : | | = | | , **Rest** | |
| 1011 | $mod$ | 12 | = | | , da | | : | | = | | , **Rest** | |
| 1001 | $mod$ | 13 | = | | , da | | : | | = | | , **Rest** | |
| 45 | $mod$ | 14 | = | | , da | | : | | = | | , **Rest** | |
| 785 | $mod$ | 43 | = | | , da | | : | | = | | , **Rest** | |





v2 21. Juni 2015

Stecke einen Text. Probiert zu zweit aus, ob die/der jeweils andere den Text mit dem Finger erfühlen kann. Nimm die Tabelle auf dem Stationsblatt für die Buchstabencodes hinzu.

Du brauchst Stecknadeln (nicht zu lang!) zum Stecken der Braille Schrift.





v3 – 21. Juni 2015

**Aufgabe 1** Kannst du folgende Nachricht verstehen?

**Aufgabe 2** Aufgabe 1 war ziemlich leicht. Kannst Du auch das hier »lesen«?

**Aufgabe 3** An der Station findet ihr ein Blatt, auf dem ihr selbst Nachrichten »schreiben« könnt. Arbeitet im Team. Eine(r) schreibt ein Wort durch Stecken der Nadeln auf das Brett. Die/der andere liest dann wie ein Blinder — Augen schließen. Nicht schummeln! — und versucht, die Nachricht zu ertasten. Beschreibt eurem Partner Buchstabe für Buchstabe, welche Punkte erhöht sind. Zum Beispiel für ein **N**:

***oben links, oben rechts, mitte rechts, unten links***

Der Sehende kann dann nachschauen, welcher Buchstabe das ist. Wechselt nach dem Wort die Rollen.





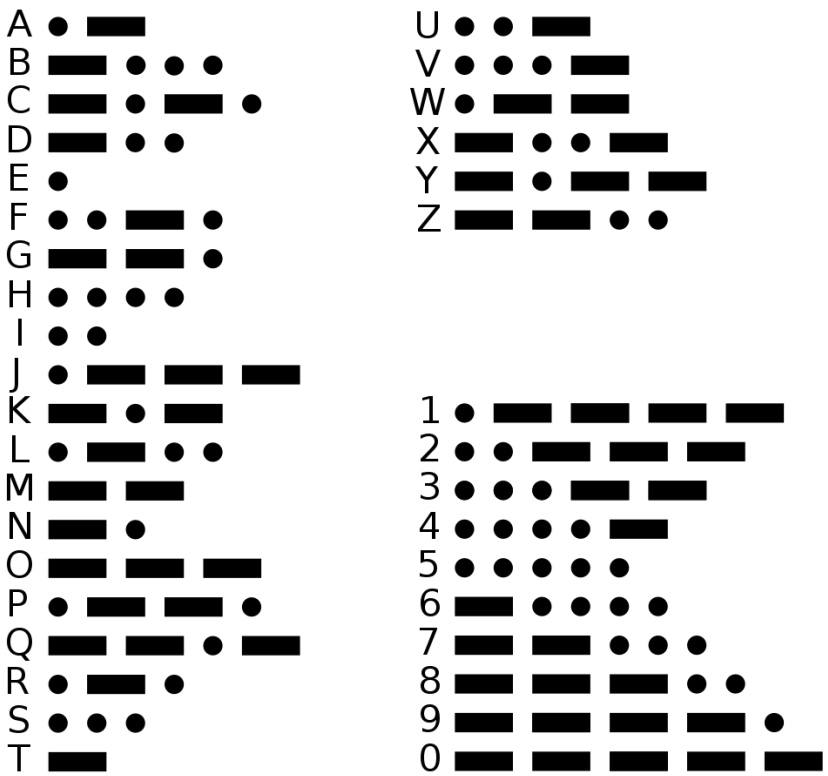
v3 – 21. Juni 2015

**Aufgabe 1** Könnt ihr folgende Nachricht verstehen?

.... .- .-.. .-.. - - -

**Aufgabe 2** Wie lautet das Morse-Signal für SOS? (Das ist das internationale Hilfesignal.)

**Aufgabe 3** An der Station findet ihr eine Taschenlampe. Stellt euch zu zweit mit ein paar Metern Entfernung gegenüber auf, jeder mit einem Morse-Alphabet. Buchstabiert euch mit der Taschenlampe gegenseitig jeweils ein Wort.

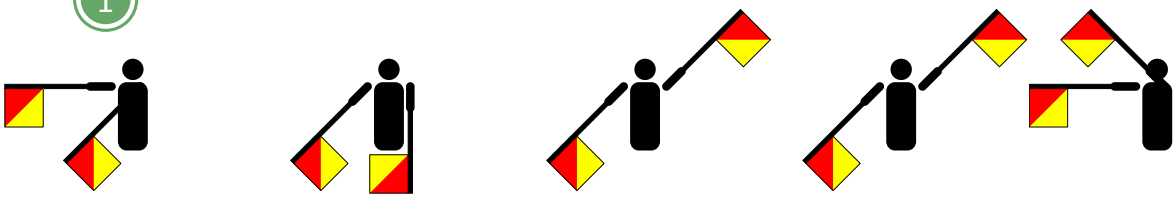






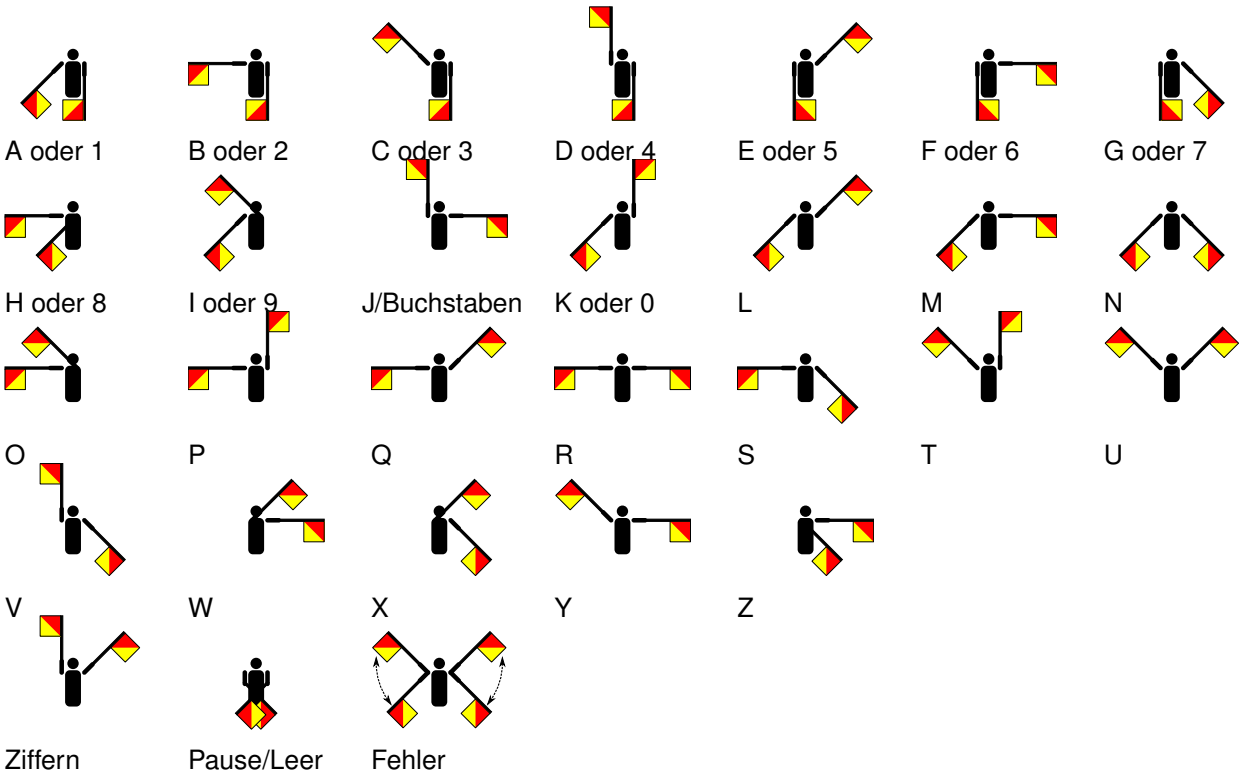

v3 21. Juni 2015

**Aufgabe 1** Entschlüssele folgende Nachricht!



**Aufgabe 2** An der Station findet ihr Flaggen. Nehmt jeder zwei und stellt euch mit ein paar Metern Entfernung gegenüber auf. Buchstabiert euch mit den Flaggen gegenseitig jeweils ein Wort.

## Das Winkeralphabet








v2 21. Juni 2015

**Aufgabe 1** Verschlüsselt euren Namen mit dem Schlüsselwort **FUCHS**.

**Aufgabe 2** Entschlüsselt folgenden Text. Das Schlüsselwort ist **WOLKENBRUCH**:

**YF DF BD WT ZG DI BD WY MI NG**

**Aufgabe 3** Beschreibe das Verfahren für das Entschlüsseln der Nachricht? Was ist hier anders?

**Aufgabe 4** Verschlüsselt euch gegenseitig mit einem ausgehandelten Schlüsselwort einen Text. Entschlüsselt die Nachricht!

**Aufgabe 1** Könnt ihr die Nachricht ohne bekannten Schlüssel entschlüsseln?

**YHQL YLGL YLFL**

**Aufgabe 2** Entschlüsselt mit der Chiffrierscheibe die folgenden Nachrichten. Mögliche Schlüssel sind: **2**, **7**, **10**, **13**. Einer ist jeweils der richtige Schlüssel. Das heißt, dass man bei Verschiebung um diese Zahl die Nachricht erhält.

a) **SPLIL RSLVWHAYH, AYLMMLU DPY BUZ ILP KLU WFYHTPKLU?**

b) **YVRORE PNRFNE, VPU JREQR QN FRVA.**

**Aufgabe 3** Warum ist dieses Verschlüsselungsverfahren leicht zu »knacken«?

**Aufgabe 4** Verschlüsselt und entschlüsselt gegenseitig den Titel eures Lieblingsbuches mit dem Schlüsselwort **LESERATTE**.

**Aufgabe 5** Entschlüssele die folgende Nachricht. Das Schüsselwort ist **SCHATZSUCHE** oder **MEISTERDETEKTIV**.

**STG HIKMJU YVTDJ KVAJTG STG CMGXEMAX**

**Aufgabe 6** Was ist der Vorteil bei dem Schlüsselwort-Caesar-Verfahren?

**Aufgabe 7** Fällt dir eine Möglichkeit ein, wie du einen Text entschlüsseln kannst, ohne alle Schlüssel durchzuprobieren? *Tipp:* Nutze dabei eine bestimmte Eigenschaft einer Sprache (z. B. Deutsch) aus.





v3 21. Juni 2015

**Aufgabe 1** Kannst du folgenden Text entschlüsseln?

**Aufgabe 2** Schreibt euch eine Nachricht mit dem Freimaurer-Chiffre.

**Aufgabe 3** Wie kann man ohne Schlüssel die Nachrichten entziffern?





v3 21. Juni 2015

**Aufgabe 1** Arbeitet zu zweit: Verschlüsselt jeweils ein Wort mit dem Schlüsselbuchstaben **G**. Tauscht die Nachrichten aus und versucht, den Text wieder zu entschlüsseln.

**Aufgabe 2** Entschlüssele folgende Texte:

a) **SOVLZUFTCNKGRVR** (Verwende Rotor I mit dem Schlüsselbuchstaben **C**.)

b) **IJMJQEHVY** (Verwende Rotor II und stelle den Schlüsselbuchstaben **L** ein.)

**Aufgabe 3** Warum ist das Drehen so wichtig? Welche Art der Verschlüsselung entsteht, wenn der Rotor zwischen den Buchstaben nicht gedreht wird?

**Aufgabe 4** Was passiert, wenn man z. B. die Nachricht **AAAA** verschlüsselt? Schaffst du es, eine Nachricht zu schreiben, die verschlüsselt **XXXX** ergibt?

**Aufgabe 5** (Schwer) Was glaubst du, wie man eine Nachricht ohne Rotor knacken könnte? Könntest du folgenden Text entziffern: **ZUFGDSYNMQR** ?





v3 21. Juni 2015

**Aufgabe 1** Verschlüsselt euren Namen mit dem Schlüsselwort **HUT**.

**Aufgabe 2** Entschlüsselt folgenden Text. Das Schlüsselwort ist **ROT**:
**XIM XSFRQAK**

**Aufgabe 3** Beschreibe ähnlich zum Verschlüsseln, wie das Entschlüsseln funktioniert.





v3 21. Juni 2015

**Aufgabe 1** Versuche, die folgende »gepflügte« Nachricht zu entschlüsseln. Der Schlüssel ist **6**.

**X G C N E I T M I S R S E H I E H T C I D A H E**

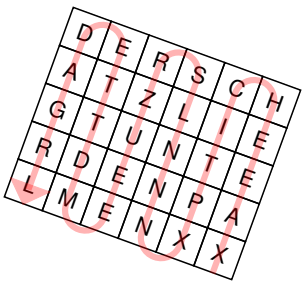
**Aufgabe 2** Beschreibe, wie du eine empfangene Nachricht mit bekanntem Schlüssel (= Anzahl Buchstaben pro Zeile) entschlüsseln kannst.

**Aufgabe 3** Schreibt euch gegenseitig eine Nachricht! Einigt euch auf den Schlüssel (= Anzahl Buchstaben pro Zeile)!

**Aufgabe 4** Kannst du den folgenden Text ohne bekannten Schlüssel entschlüsseln? Du fängst eine Nachricht ab und möchtest herausbekommen, was darin steht. Du weißt, dass »Pflügen« als Verschlüsselungsverfahren benutzt wurde. Hier ist die Nachricht:

**H I H A N N K E G C E C A O I T K S A C S N S F N T R I A D**

*Tipp:* Die Anzahl der Buchstaben ist immer durch die zuvor festgelegte Anzahl von Buchstaben pro Zeile teilbar.







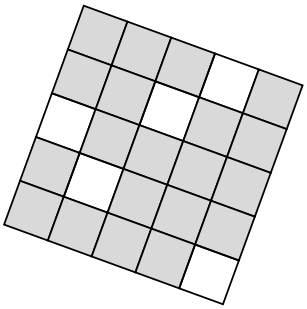

v3 21. Juni 2015

**Aufgabe 1** Du findest an der Station einige verschlüsselte Nachrichten. Kannst du sie mit den Schablonen entschlüsseln?

**Aufgabe 2** Schreibt euch gegenseitig eine Nachricht mit einer der Schablonen an der Station.

**Aufgabe 3** Erkennst du das Muster, wie eine solche Schablone aufgebaut ist?
Überlege dir die Antwort anhand folgender Hilfsfragen: Wie dürfen die Löcher angeordnet sein? Wie viele Kästchen musst du ausschneiden, damit am Ende alle Kästchen komplett mit Buchstaben ausgefüllt sind? Wenn ein Kästchen ausgeschnitten ist, welche anderen Kästchen dürfen dann nicht ausgeschnitten werden?

**Aufgabe 4** Entwirf selbst eine Schablone und verschlüssele mit deiner eigenen Schablone eine Nachricht.







v3 – 21. Juni 2015

**Aufgabe 1** An der Station findest du einige *Skytale-Nachrichten* und auch verschiedene *Skytalen*. Kannst du die Nachrichten entschlüsseln?

**Aufgabe 2** Worauf müssen sich Sender und Empfänger geeinigt haben, bevor sie sich *Skytale-Nachrichten* schicken? Was darf niemand außer ihnen wissen?

**Aufgabe 3** Kannst du folgende Nachricht ohne Skytale »knacken«?

**K R C I O G H N M E B X M N E D M N R K O A L P**

(Warum ist das »knacken« und nicht »entschlüsseln«?)