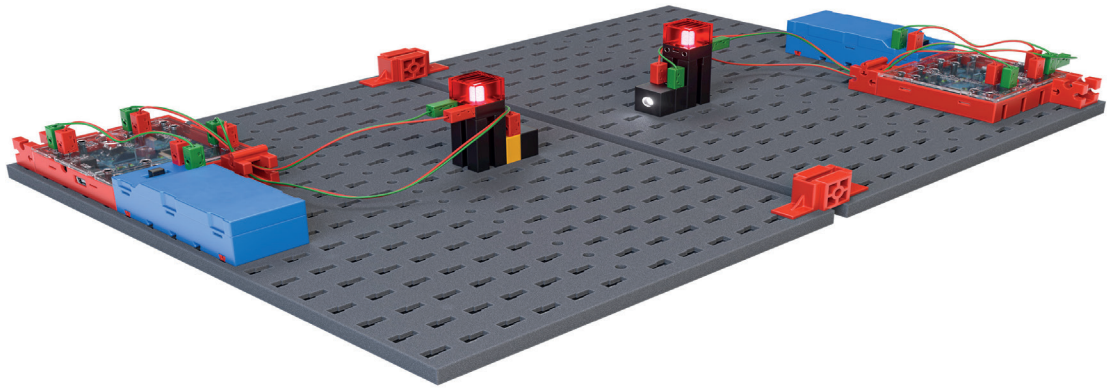
Modell 8: Verschlüsselung

Worum geht es? Nachrichten endlich wirklich abhörsicher mit der besten Freundin oder dem besten Freund austauschen?
Bei diesem Modell erfährst du viel über Sicherheit bei der Nachrichtenübertragung. Und damit auch darüber, warum man auch im Internet auf Sicherheit achten sollte.



Einführung

Die Nachrichtenübermittlung mit Lichtsignalen (Modell Telegraf) hat einen Nachteil: Wenn jemand einen Fototransistor in die Übertragungsstrecke hält, kann er die übertragene Nachricht mitlesen.

Davor schützt eine **Verschlüsselung** der Nachricht.

Bei diesem Modell lernst zu zwei einfache **Verschlüsselungsverfahren** kennen.

Auch Telefonleitung, WLAN, Internet-Verbindung können abgehört werden und werden daher heute nach Möglichkeit durch Verschlüsselung geschützt.

1 Konstruktionsaufgabe
Für diese Aufgabe benötigst du die Telegrafenstation dem vorherigen Aufgabenblatt.

Programmieraufgaben

2 Ersetzungs-Chiffre

Deine Nachrichtenübermittlung mit Lichtsignalen (beim Telegraf) soll nun durch eine **Verschlüsselung** davor geschützt werden, dass jemand die Übertragung abhört.

Eine sehr alte **Verschlüsselungsmethode** ist die Verwendung eines Alphabets, in dem die Buchstaben untereinander vertauscht werden.

Das geht sehr einfach, indem du die Buchstaben des Alphabets nicht von 1 bis 26 durchnummerierst, sondern ihnen in der Tabelle hier die Nummern 1 bis 26 **zufällig** zuordnest

Dieses Verschlüsselungsverfahren nennt man auch **„Ersetzungs-Chiffre“**, weil einzelne Zeichen durch andere ersetzt werden.

Überlege dir eine zufällige Nummerierung der Buchstaben und trage sie in die folgende Tabelle ein. Achte darauf, dass du jede der Zahlen 1-26 nur einmal verwendest:

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	

Kodiere nun den Text „Hallo Welt“ mit diesem Alphabet und **übertrage** ihn mit dem Programm deiner Telegrafenstation.

Überlege: Was ist der Nachteil dieser Chiffre?

Programmieraufgaben

3 Verschiebe-Chiffre

Die Vereinbarung eines ganzen Alphabets als „Geheimnis“, das Sender und Empfänger der verschlüsselten Nachricht kennen müssen, ist sehr aufwändig: Du musst immer die gesamte Tabelle zur Hand haben.

Das ist vor allem schwierig, wenn du mit vielen verschiedenen Empfängern verschlüsselte Nachrichten austauschen möchtest, die nur der jeweilige Empfänger entschlüsseln kann, wird das kompliziert.

Daher hat schon Julius Caesar im ersten Jahrhundert vor Christus eine Verschlüsselung erfunden, die mit einem sehr einfachen „**Schlüssel**“ auskommt, den man sich sogar merken kann: **Er hat die Nummern der Buchstaben des Alphabets einfach nur um eine feste Zahl „verschoben“.**

Merken musste er sich als „Schlüssel“, den Sender und Empfänger kennen müssen, nur die Zahl der Stellen, um die die Nummern verschoben werden.
Den Wert des Schlüssels muss der Empfänger beim Entchlüsseln einfach nur wieder abziehen, und er findet den richtigen Buchstaben.

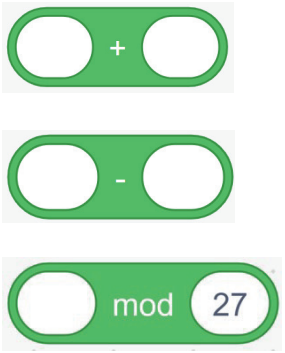
Diese Verschlüsselung kannst du sehr einfach programmieren, indem du zu jedem Buchstaben (der Zahl aus der Tabelle) deiner Nachricht den Schlüssel hinzuaddierst.

Damit die Zahl nicht größer wird als 26, macht man einen Trick: du teilst größere Zahlen durch 27 und rechnest mit dem Rest weiter.

Hier siehst du einen Vorteil von Computern: selbst wenn du so etwas nicht oder noch nicht rechnen kannst: du kannst es programmieren und der Computer rechnet für dich! :)

Der Empfänger macht dasselbe, nur „rückwärts“: Von der empfangenen Zahl wird der Schlüssel abgezogen; der Rest nach Teilen durch 26 ist die Zahl (= der Buchstabe des Alphabets) der ursprünglichen Nachricht.

Die Rechenschritte nehmen dir die folgenden Scratch-Operationen „+“, „-“ und „modulo“ ab:



Ändere dein Sende- und dein Empfangs-Programm dem Modell Telegraf nun so ab, dass

1. zu der Variablen „Zahl“ (also der Nummer des Buchstabens, den du senden möchtest) vor dem Senden die Variable „Schlüssel“ modulo 27 addiert und

2. nach dem Empfangen von „Zahl“ der Schlüssel modulo 27 subtrahiert wird.

Teste das Programm mit dem Text „Hallo Welt“ und **speichere** es unter dem Namen **„Sender mit Verschlüsselung“** bzw. **„Empfänger mit Entschlüsselung“** (beim Modell Telegrafenstation „Sender-Empfänger mit Ver- und Entschlüsselung“).

Überlege: Wie viele verschiedene Schlüssel kannst du bei dieser Chiffre wählen?

Experimentieraufgabe

4 Sprachausgabe

Dein Empfangsprogramm soll nun den Buchstaben der empfangenen Nachricht als Sprache ausgeben.

Wie die **Sprachausgabe** funktioniert, hast du bei den Modellen "Schranke" und "Münzzähler" kennengelernt.

Programmiere einen eigenen **Block „Sprachausgabe“**, an den du die entschlüsselte Zahl übergeben kannst, und der den zugehörigen Buchstaben spricht.

Tipp: Die Sprachausgabe benötigt etwas Zeit. Damit dein Empfänger währenddessen kein Signal „übersieht“, solltest du beim Sender die Pause nach dem Senden einer Zahl auf 2,5 bis 3 Sekunden vergrößern.

Teste dein Programm und **speichere** es unter dem Namen „**Sprachausgabe Empfänger mit Verschlüsselung“.**