ICT Ausbildungszentrum Bern
Computerschule Bern AG, Zieglerstrasse 64, 3000 Bern 14 031 398 98 00 www.csbe.ch

Übungsheft

Fachbereich	ICT-Berufsausbildung
Thema	Modul 114 Codierungsverfahren, Kompressionsverfahren und Verschlüsselungsverfahren einsetzen
weitere Hilfsmittel	im Übungsheft erwähnt
Bemerkungen	Das vorliegende Dokument dient der praktischen Begleitung zum Modul 114. Die einzelnen Einheiten werden selbstständig oder in einer Gruppenarbeit abgehalten und abschliessend mit dem Kursleiter besprochen.

Inhaltsverzeichnis

Lerneinheit A

Zahlensysteme der Informatik

Der Kursleiter hat Ihnen im Unterricht die Begriffe **Codierung** und **Binärsystem** vorgestellt.

In dieser Aufgabe erarbeiten Sie sich das Wissen zu weiteren Zahlensysteme und ihrer Geschichte, welche in der Informatik wichtig sind.

Lernziele

Die Teilnehmer kennen die Geschichte der Zahlensysteme
Die Teilnehmer kennen die wichtigsten Zahlensysteme der Informatik

Vorgehen

Bilden Sie eine Vierergruppe

Lesen Sie den Text **Zahlensystem.pdf**

Teilen Sie die einzelnen Kapitel auf

- Ägypter, Babylonier
- Griechen, Römer
- Chinesen, Inder
- Araber, Europa

Schreiben Sie die wichtigsten Informationen zum Zahlensystem auf

Tauschen Sie nun Ihr neu erworbenes Wissen in der Gruppe aus, damit jedes Mitglied die wichtigsten Informationen zu **allen** Zahlensystemen kennt.

Lesen Sie nun den Text **Informatik-Grundlagenwissen: Zahlensysteme** auf der Webseite **http://www.tutorials.at/einfuehrung/03-zahlensysteme.html**

Lesen Sie den Text **itHandbuchZahlen.pdf**

Wenden Sie nun die verschiedenen Techniken an, indem Sie die Aufgaben aus dem **Protokollheft: Protokollblatt A** lösen.

Lerneinheit B

Rechnen mit dem Dualsystem

Der Kursleiter hat Ihnen im Unterricht die Begriffe **Codierung** und **Binärsystem** vorgestellt.

Sie kennen ausserdem weitere Zahlensysteme aus der letzten Lerneinheit. In der folgenden Lerneinheit erlernen Sie nun das rechnen mit dem Binärsystem.

Lernziele

Die Teilnehmer kennen die Regeln, um im Binärsystem zu rechnen
Die Teilnehmer können diese Regeln selbstständig anwenden, um im Binärsystem zu rechen

Vorgehen

Lesen Sie die Texte **Grundrechenarten im Dualsystem** und **Schriftliche Addition** auf der Seite **http://de.wikipedia.org/wiki/Dualsystem#Grundrechenarten_im_Dualsystem**

Versuchen Sie nun die Rechnung `1001 1011 + 0100 0011` zu lösen

Wie lassen sich die Regeln anwenden, welche Sie aus dem Artikel kennen? Besprechen Sie Ihre Erkenntnisse dem Banknachbar.


Es folgt nun zuerst eine Zwischenbesprechung im Plenum

Stellen Sie nun drei Rechenaufgaben für Ihren Partner zusammen und lösen Sie die drei Rechenaufgaben von Ihrem Partner.

Lesen Sie den Text **Schriftliche Subtraktion** auf der Seite
http://de.wikipedia.org/wiki/Dualsystem#Grundrechenarten_im_Dualsystem

Versuchen Sie nun die Rechnung `1001 1011 - 0100 0011` zu lösen

Wie lassen sich die Regeln anwenden, welche Sie aus dem Artikel kennen? Besprechen Sie Ihre Erkenntnisse dem Banknachbar.

- Es folgt nun zuerst eine Zwischenbesprechung im Plenum

Stellen Sie nun drei Rechenaufgaben für Ihren Partner zusammen und lösen Sie die drei Rechenaufgaben von Ihrem Partner.

Lesen Sie den Text **Zweierkomplement.pdf**

Stellen Sie nun drei Rechenaufgaben für Ihren Partner zusammen und lösen Sie die drei Rechenaufgaben von Ihrem Partner.

Kontrollieren Sie mit Ihrem Partner die Lösungen der Rechenaufgaben.

Lerneinheit C

Fehlerbehebung bei einer DVD

Ihr Kursleiter hat Ihnen im Unterricht die Begriffe **even parity** und **odd parity** vorgestellt.

In dieser Lernaufgabe lernen Sie nun den Hamming Code kennen und anwenden.

Lernziele

Die Teilnehmer kennen den Hamming Code und können Ihn sicher anwenden

Vorgehen

Bilden Sie Zweiergruppe

Lesen Sie die Texte **Hamming Code** auf der Seite
http://de.wikipedia.org/wiki/Hamming-Code

Lesen Sie den Text **Fehlerkorrektur.pdf**

Besprechen Sie mit Ihrem Partner Ihr erworbenes Wissen


Es folgt nun zuerst eine Zwischenbesprechung im Plenum

Erstellen Sie drei Hamming Codes und tauschen Sie diese mit Ihrem Partner aus, wobei Sie bewusst in einen oder zwei Codes einen Fehler einbauen.

Kontrollieren Sie mit Ihrem Partner die Lösungen der Rechenaufgaben.

Lerneinheit D

EAN Code

Ihr Kursleiter hat Ihnen im Unterricht die Begriffe **EAN-13** und **EAN-8** vorgestellt.

In dieser Lernaufgabe lernen Sie nun den Umgang mit dem EAN Code kennen.

Lernziele

Die Teilnehmer können den EAN Code (EAN-8) sicher anwenden.

Vorgehen

Bilden Sie Zweiergruppe

Lesen Sie den Text **EAN-Code.pdf**

Besprechen Sie mit Ihrem Partner Ihr erworbenes Wissen

Erstellen Sie nun auf im **Protokollheft: Protokollblatt D** drei EAN Codes und tauschen Sie diese mit Ihrem Partner aus, damit Sie die EAN Codes von Ihrem Partner wiederum auslesen können.

Lerneinheit E

Bilder codieren

Man kann Grafiken in verschiedensten Formaten speichern. Manche Formate werden gerade bei Webseiten häufig benutzt, weil sie sich dafür gut eignen. Manche Formate sind für Webseiten nicht so geeignet, dafür aber für andere Anwendungsbereiche umso besser.

In dieser Lernaufgabe lernen Sie verschiedene Grafikformate kennen und mit diesen zu arbeiten.

Lernziele

Die Teilnehmer kennen verschiedene Formate von Grafiken
Die Teilnehmer können verschiedene Grafikformate bearbeiten

Vorgehen

Öffnen Sie die Dateien **114dino.png** und **114dino.bmp** mit **Gimp** sowie die Datei **114dino.svg** mit **Inkscape**.

Vergrössern Sie nun die drei Dateien sehr stark

Vergleichen Sie die Qualität der Darstellung und die Grösse der Dateien miteinander.

Besprechen Sie Ihre Eindrücke in einer Dreiergruppe.

Öffnen Sie die Internetseite **http://de.wikipedia.org/wiki/Grafikformat**. Teilen Sie die einzelnen Grafikformate in der Gruppe auf

- bmp, gif
- jpg, png
- tif, svg

Lesen Sie nun den Wikipediaartikel zu Ihren Grafikformaten

Ergänzen Sie die Tabelle auf dem **Protokollheft: Protokollblatt E**

Lesen Sie den Text Portable Bitmap auf der Webseite
http://de.wikipedia.org/wiki/Portable_Bitmap

Laden Sie die Datei **114hallo.pbm** in ein Grafikprogramm und in einem Text-Editor und beantworten Sie die erste Frage auf dem **Protokollheft: Protokollblatt E**.

Erzeugen Sie mit einem Text-Editor eine Datei **initialen.pbm**, welche Ihre Initialen zeigt. Die Grösse des Bildes soll dabei 8x8 Pixel betragen. Es empfiehlt sich ein Entwurf auf dem **Protokollheft: Protokollblatt E** zu zeichnen. Teste nun das Bild in einem Grafikprogramm.

Beantworten Sie die zweite Frage auf dem **Protokollheft: Protokollblatt E**.

Lerneinheit F

Bildgrössen berechnen

Im Unterricht haben Sie die Grundlagen der Bildberechnung kennengelernt.

Lernziele

Die Teilnehmer können Bildgrössen mit unterschiedlichen Formaten sicher berechnen

Vorgehen

Lösen Sie die Aufgaben auf dem **Protokollheft: Protokollblatt F**.

Achten Sie dabei immer auf die richtigen Einheiten. Sie können beispielsweise nicht **dpi** mit **cm** miteinander berechnen.

Lerneinheit G

Huffman Code anwenden

Im Unterricht haben Sie bereits verschiedene Kompressionsverfahren kennengelernt.

In dieser Lernaufgabe beschäftigen Sie sich mit der Anwendung des Huffman Codes.

Lernziele

Die Teilnehmer können mit dem Huffman Code sicher komprimieren
Die Teilnehmer können den Komprimierunggrad von einem Huffman Code mit verschiedenen Originalformaten feststellen
Die Teilnehmer können eine Bitfolge mit Hilfe des Huffman Codes sicher dekomprimieren

Vorgehen

Beim Kofferpacken können wir durch Druck die Luft herauslassen und bringen somit mehr Kleidungsstücke in den Koffer. Im Unterricht haben wir vom Huffman Code gehört und wissen, dass er nach dem gleichen Prinzip funktioniert.

Wie muss der Eingabetext beschaffen sein, damit er sich gut komprimieren lässt?

Installieren Sie das Programm **jdk-6u45-windows-i586.exe**

Verwenden Sie zum Lösen dieser Aufgabe das Applet **huffman.jar**

Eine Kurzanleitung finden Sie auf dem Beiblatt **Huffmann Bedienungsanleitung.pdf**

Komprimieren Sie mehrere Wörter, um so auf die Lösung zu kommen. Zum Beispiel mit:

können | Schifffahrtsgesellschaft | Griffbrett | Maus | AAAAAABBCCED | ABCDEFGHIJKL

Formulieren Sie Ihre Antwort in höchstens drei ganzen Sätzen im **Protokollheft: Protokollblatt G**.

Als nächstes geht es um die genauere Untersuchung des Huffman Codes.

Versuchen Sie die Lösung anhand der Komprimierung von AAAAAABBCCED herauszufinden.

Vervollständigen Sie die Sätze im **Protokollheft: Protokollblatt G**. Hinter den Lücken finden Sie in Klammern mehrere Vorschläge.

Beschreiben Sie, wie der Huffman Baum aufgebaut wird.

Lesen Sie den Text Huffman Code auf der Webseite
http://de.wikipedia.org/wiki/Shannon-Fano-Kodierung#Huffman-Code

Versuchen Sie die Lösung anhand der Komprimierung von AAAAAABBCCED herauszufinden.

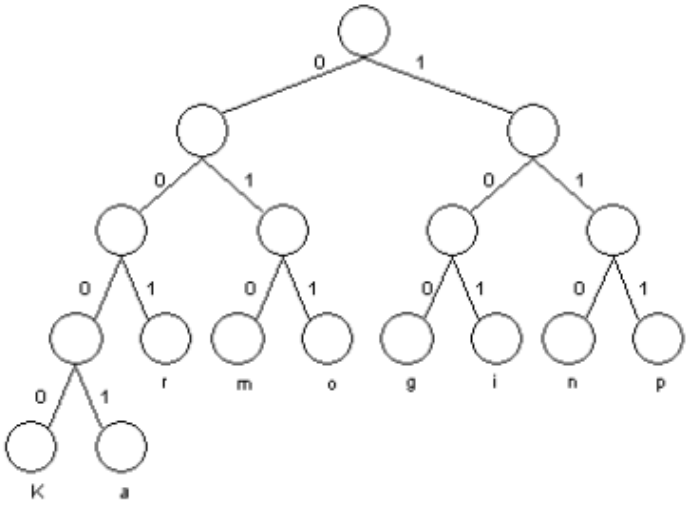
Formulieren Sie Ihre Antwort in höchstens fünf ganzen Sätzen im **Protokollheft: Protokollblatt G**.

Der Huffman-Code erlaubt es, eine codierte Folge von NULLEN und EINSEN sehr einfach wieder in den ursprünglichen Text zu verwandeln. Dazu braucht man den Codebaum, der bei der Komprimierung verwendet wurde.

Beschreiben Sie, wie bei der Dekomprimierung vorgegangen wird

Versuchen Sie folgenden String zu dekomprimieren
00001011100111110010111000010001010010

Benutzen Sie dazu folgenden Huffman Baum



Formulieren Sie Ihre Antwort in höchstens vier ganzen Sätzen im **Protokollheft: Protokollblatt G**.

Sie kennen den Huffman Code in der Zwischenzeit ziemlich gut. Wie gut die Komprimierung ist, hängt immer auch davon ab, wie oft Zeichen in einem Text vorkommen oder wie lange der Text ist.

Nehmen Sie für diese Aufgabe das Beispiel NEUENBURG als Hilfe und schreiben Sie Ihre Lösung am Ende der Seite.

Wie viel Speicherplatz benötigt das Wort, wenn Sie folgende Codierungen verwenden

- ASCII Code 8 bit pro Buchstabe
- Unicode 16 bit pro Buchstabe
- Huffmann Code Variable Bitlänge pro Buchstabe

Wie viel Speicherplatz sparen Sie nun, wenn Sie das Wort mit dem Huffman Code komprimieren? Berechnen Sie die Einsparung in Prozent im **Protokollheft: Protokollblatt G**.

Lerneinheit H

BWT anwenden

Im Unterricht haben Sie bereits verschiedene Kompressionsverfahren kennengelernt.

In dieser Lernaufgabe beschäftigen Sie sich mit der Anwendung der Burrows Wheeler Transformation.

Lernziele

Die Teilnehmer können mit dem BWT Verfahren sicher transformieren und rückwärts transformieren

Vorgehen

Die Burrows Wheeler Transformation verwenden Sie nicht als Kompressionsverfahren, sondern nur, um einen Text zu bündeln, damit er Komprimiert werden kann.

Lesen Sie die Kapitel **Grundlagen** und **Transformation anhand eines Beispiels** aus dem Text **BWT.pdf**

Versuchen Sie, das Beispiel anhand des Begleittextes nachzuverfolgen

Versuchen Sie nun folgende Transformationen durchzuführen anhand folgender Beispiele:

Schifffahrtsgesellschaft | Griffbrett

Die Burrows Wheeler Transformation hat den Vorteil, dass Sie den Originaltext wiederherstellen können.

Lesen Sie das Kapitel **Rückwärtstransformation anhand eines Beispiels** aus dem Text **BWT.pdf**

Versuchen Sie, das Beispiel anhand des Begleittextes nachzuverfolgen

Versuchen Sie nun folgende Rückwärtstransformationen durchzuführen anhand der vorherigen Aufgabe.

Lerneinheit I

Modulo Rechnen

Ihr Kursleiter hat Ihnen im Unterricht die Grundlagen der Kryptologie vorgestellt.

In dieser Lernaufgabe lernen Sie nun die Grundlagen, auf welchen die meisten Methoden aufbauen.

Lernziele

Die Teilnehmer können das Modulo Rechnen sicher anwenden

Vorgehen

Lesen Sie den Text **Modulo.pdf**

Lösen Sie anschliessend die Aufgaben im **Protokollheft: Protokollblatt I**.

Lerneinheit J

Symmetrische Kryptographie

Ihr Kursleiter hat Ihnen im Unterricht die Grundlagen der symmetrischen Verschlüsselung vorgestellt.

In dieser Lernaufgabe lernen Sie nun die drei klassischen Verschlüsselungsverfahren kennen um Machen Bekanntschaft mit zwei Methoden der Kryptoanalyse.

Lernziele

Die Teilnehmer können anhand historischer Verschlüsselungsverfahren erklären, was es braucht um eine Nachricht sicher zu übermitteln.
Die Teilnehmer kennen die grundsätzlichen Schwachstellen von Verschlüsselungsverfahren.
Die Teilnehmer kennen den Unterschied zwischen monoalphabetischen und polyalphabetischen Verschlüsselungsverfahren.
Die Teilnehmer können die 3 klassischen Verschlüsselungsverfahren Caesar, Substitution und Vigenère selbst auf eine beliebige Textnachricht anwenden.
Die Teilnehmer kennen zwei Methoden der Kryptoanalyse und können diese auf verschlüsselte Texte anwenden.

Vorgehen

Für diese Lernaufgabe suchen Sie sich einen Partner.

Sie werden Nachrichten verschlüsseln und entschlüsseln. Damit Sie nicht ihre eigenen Nachrichten entschlüsseln müssen, arbeiten Sie mit einem Partnerteam zusammen.

Mit diesem müssen Sie die geheimen Schlüssel austauschen, ihnen Ihre Nachrichten senden und Nachrichten von ihnen empfangen.

Hilfe / weitere Informationen

http://www.staff.uni-mainz.de/pommeren/Kryptologie/Klassisch/1_Monoalph/MonoSubst.html

http://www.regenechsen.de/phpwcms/index.php?krpto_analyse_frequenz

http://www.daniel-faber.de/schule/facharbeit/html/facharbeit-kryptologie.html

Kopieren Sie die Datei **.java.policy** in Ihr persönlichen Ordner **C:\Users\"IhrName"**.

Starten Sie nun Ihren Computer neu.

Vereinbaren Sie in der Zwischenzeit ein Schlüssel mit Ihrem Partnerteam

Öffnen Sie die Internetseite **krypto.htm** und verwenden Sie den Link **Ceasar Chiffre**

Schreiben Sie mit dem Hilfsprogram einen kurzen Klartext

Verschlüsseln Sie den Text mit dem abgemachten Schlüssel.

Kopieren Sie die verschlüsselte Nachricht in die Zwischenablage und senden Sie diese Nachricht an Ihr Partnerteam.

Warten Sie auf die Nachricht Ihres Partnerteams.

Entschlüsseln Sie die vom Partnerteam empfangene Nachricht mit dem ausgetauschten.

Bei Fragen und Unklarheiten klicken Sie auf den Link **Funktionsweise des Programms**.

Das Caesar-Verfahren ist schon über 2000 Jahre alt. Es ist deshalb nicht erstaunlich, dass es sehr leicht zu brechen ist. Die Analysemethode nennt sich *Brute-Force*, was nichts anderes heisst als *rohe Gewalt*. Der Trick besteht darin, dass einfach alle möglichen Schlüssel ausprobiert werden, und man schaut, was dabei jeweils als Klartext herauskommt.

Öffnen Sie die Internetseite **krypto.htm** und verwenden Sie den Link **Ceasar Chiffre**.

Schreiben Sie mit dem Hilfsprogram einen kurzen Klartext

Verschlüsseln Sie den Text mit einem Schlüssel, der dem Partnerteam unbekannt ist

Kopieren Sie die verschlüsselte Nachricht in die Zwischenablage und senden Sie diese Nachricht an Ihr Partnerteam.

Warten Sie auf die Nachricht Ihres Partnerteams.

Knacken Sie die Nachricht mit der **Brute-Force-Methode** und beantworten Sie die Fragen 1 und 2 im **Protokollheft: Protokollblatt J**.

Bei Fragen und Unklarheiten klicken Sie auf den Link **Funktionsweise des Programms**.

Irgendwann haben Caesars Nachfahren herausgefunden, dass dieses Verfahren nicht sehr sicher ist. Wenn jedoch die Anzahl der möglichen Schlüssel erhöht werden könnte, dann würde die Kryptoanalyse massiv erschwert werden. Dies gelingt mit dem Substitutionsverfahren.

Dabei wird jeder Buchstabe des Klartextes durch einen beliebigen Buchstaben aus dem Geheimtext ersetzt (*substituieren= ersetzen*). Es werden nicht mehr alle Buchstaben um gleich viele Stellen verschoben wie beim Caesar-Verfahren.

Damit man sich dazu den Schlüssel gut merken kann, geht man folgendermassen vor: Die Buchstaben des Klartextalphabetes werden der Reihe nach hingeschrieben. Darunter wird zuerst das Schlüsselwort (im Beispiel: *KRYPTO*) geschrieben, und dann kommen der Reihe nach alle im Schlüsselwort nicht benutzten Buchstaben des Alphabetes.

Beispiel mit Schlüsselwort *KRYPTO*: `abcdefghijklmnopqrstuvwxyz`

`KRYPTO``ABCDEFGHIJLMNQSUVWXZ`

Damit wird aus dem Klartext *hallo* der Geheimtext *BKFFI*.

Das Substitutionsverfahren ist ein symmetrisches Verfahren. Deshalb funktioniert die Entschlüsselung wie beim Caesar-Verfahren.

Vereinbaren Sie mit Ihrem Partnerteam einen neuen geheimen Schlüssel

Öffnen Sie die Internetseite **krypto.htm** und verwenden Sie den Link **Substitution**.

Schreiben Sie mit dem Hilfsprogram einen Klartext

Verschlüsseln Sie den Text mit dem abgemachten Schlüssel.

Kopieren Sie die verschlüsselte Nachricht in die Zwischenablage und senden Sie diese Nachricht an Ihr Partnerteam.

Warten Sie auf die Nachricht Ihres Partnerteams.

Entschlüsseln Sie die vom Partnerteam empfangene Nachricht mit dem ausgetauschten Schlüssel.

Beantworten Sie die Frage 3 im **Protokollheft: Protokollblatt J**.

Das Substitutionsverfahren scheint ziemlich sicher zu sein, gibt es doch theoretisch 403'291'461'126'605'635'584'000'000 mögliche Schlüssel. Eine Brute-Force-Analyse würde sehr lange dauern. Die Kryptoanalytiker haben aber eine andere Methode gefunden. Sie nennt sich *Häufigkeitsanalyse*: In jeder Sprache gibt es Buchstaben und Buchstabenpaare die häufiger vorkommen als andere. Zum Beispiel ist der Buchstabe E in der deutschen wie auch in der englischen Sprache mit Abstand der häufigste.

Das Substitutionsverfahren ist wie das Caesar-Verfahren ein monoalphabetisches Verfahren. Aus einem bestimmten Klartextbuchstaben wird immer der gleiche Geheimtextbuchstabe. Deshalb kann man folgendermassen vorgehen:

1. Man zählt wie oft die einzelnen Buchstaben auftreten.
2. Der Buchstabe, der am häufigsten auftritt, ist wahrscheinlich ein **E** (ausser der Text stammt aus dem Roman *Anton Voyls Fortgang* von Georges Perec, darin kommt kein einziges E vor…).
3. Kommt ein Wort mit nur 2 Buchstaben vor, bei dem der erste Buchstabe wahrscheinlich ein E ist, so ist der 2. Buchstabe vermutlich ein R. Begründung: ER ist ein häufiges Bigramm (Buchstabenpaar).
4. Es können auch Häufigkeitsdaten von Trigrammen benutzt werden. Trigramme sind Folgen von 3 Buchstaben.
5. Hat man erst einmal ein paar Buchstaben erraten ist es meist nicht allzu schwierig aus dem Kontext noch weitere Buchstaben zu erraten.

Vereinbaren Sie mit Ihrem Partnerteam einen geheimen Schlüssel

Öffnen Sie die Internetseite **krypto.htm** und verwenden Sie den Link **Substitution**.

Schreiben Sie mit dem Hilfsprogram einen Klartext

Verschlüsseln Sie den Text mit einem Schlüssel, der dem Partnerteam unbekannt ist

Kopieren Sie die verschlüsselte Nachricht in die Zwischenablage und senden Sie diese Nachricht an Ihr Partnerteam.

Warten Sie auf die Nachricht Ihres Partnerteams.

Führen Sie nun eine manuelle Häufigkeitsanalyse durch. Benutzen Sie die Fakten über die Sprache und die Häufigkeitsverteilung. In den Feldern oben rechts können Sie ihre Vermutungen für die einzelnen Buchstaben eingeben. Die Änderungen erscheinen dann sofort darunter im Text. Die grün hinterlegten Buchstaben sind noch frei.

Beantworten Sie die Frage 4 im **Protokollheft: Protokollblatt J**.

Nachdem die Kryptoanalytiker auch das Substitutionsverfahren geknackt hatten, waren die Verschlüsselungsspezialisten wieder gefragt. Solange aus einem Klartextbuchstaben immer der gleiche Geheimtextbuchstabe entsteht kann man immer die Häufigkeitsanalyse anwenden. So entstand die polyalphabetische Verschlüsselung, bei der aus einem Klartextbuchstaben nicht immer der gleiche Geheimtextbuchstabe wird (*poly = viel*). Das bekannteste polyalphabetische Verschlüsselungsverfahren heisst Vigenère und funktioniert folgendermassen:

```
diesistderklartext
keykeykeykeykeykey
------------------
ONDDNREIDCPKLWSPCS
```

Der Schlüssel *KEY* wird endlos wiederholt unter den Klartext geschrieben. Danach werden zu den Buchstaben des Klartextes die Buchstaben des Schlüssels hinzuaddiert. So wird aus **D** (4. Buchstabe) plus **K** (11. Buchstabe) ein
O (4 + 11 = 15. Buchstabe). Eine verschlüsselte Nachricht wird entschlüsselt, indem der Schlüssel vom Geheimtext subtrahiert wird.

Öffnen Sie die Internetseite **krypto.htm** und verwenden Sie den Link **Vinegère**.

Schreiben Sie mit dem Hilfsprogram einen Klartext von mindestens 200 Zeichen

Verschlüsseln Sie den Text mit dem abgemachten Schlüssel.

Kopieren Sie die verschlüsselte Nachricht in die Zwischenablage und senden Sie diese Nachricht an Ihr Partnerteam.

Warten Sie auf die Nachricht Ihres Partnerteams.

Entschlüsseln Sie die vom Partnerteam empfangene Nachricht mit dem ausgetauschten Schlüssel.

Beantworten Sie die Frage 5 im **Protokollheft: Protokollblatt J**.

Das Vigenère Verfahren wurde auch als *Le chiffre indéchiffrable* bezeichnet

Öffnen Sie die Internetseite **krypto.htm** und verwenden Sie den Link **Vinegère**.

Schreiben Sie mit dem Hilfsprogram einen Klartext von mindestens 200 Zeichen

Verschlüsseln Sie den Text mit einem Schlüssel, der dem Partnerteam unbekannt ist

Kopieren Sie die verschlüsselte Nachricht in die Zwischenablage und senden Sie diese Nachricht an Ihr Partnerteam.

Warten Sie auf die Nachricht Ihres Partnerteams.

Versuchen Sie eine Häufigkeitsanalyse auf diese Nachricht

Testen Sie die automatische Vigenère-Analyse

Wenn die Nachricht lange genug ist, dann kann die automatische Analyse den Schlüssel wahrscheinlich knacken

Beantworten Sie die Fragen 6-8 im **Protokollheft: Protokollblatt J**.