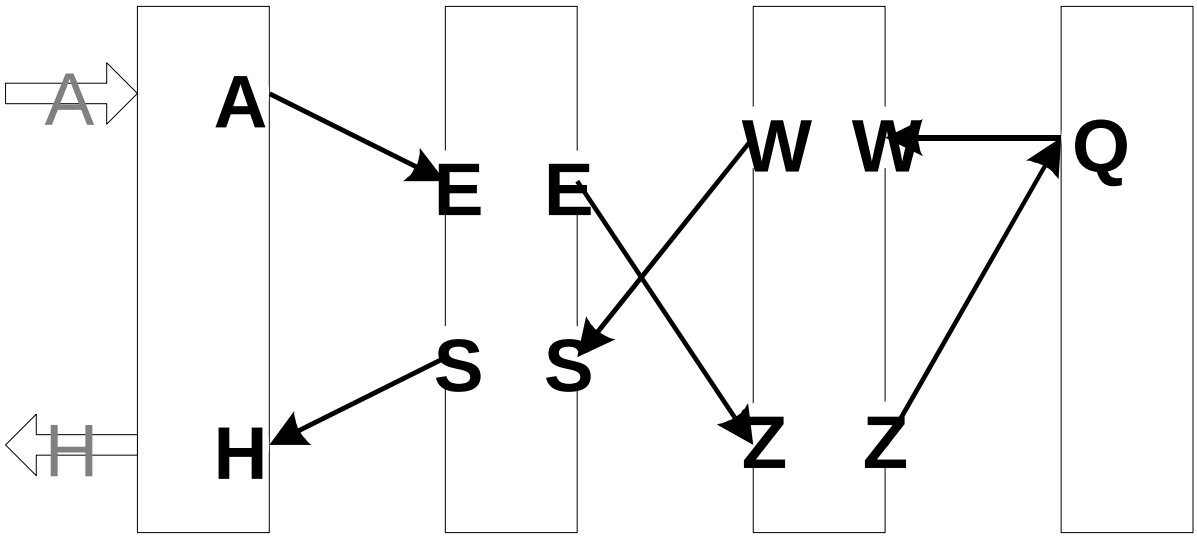
Beispiel 1: Enigma (24 Punkte)

Enigma war eine elektrische Codiermaschinen die zur Verschlüsselung von Nachrichten im zweiten Weltkrieg eingesetzt wurde.

Die Funktion ist einfach: Die Maschine besteht aus drei Codierscheiben, die auf jeder Seite für jedes Zeichen des Zeichenvorrats einen Kontakt haben. Zwischen den Seiten bestehen mehr oder weniger willkürliche Verbindungen. Dadurch ergibt sich eine 1:1 Übersetzung von einem Zeichen auf ein jeweils anderes. Die drei Scheiben arbeiten hintereinandergeschaltet. Nach der letzten Scheibe befindet sich ein sog. Reflektor. Das ist eine Scheibe mit Kontakten auf nur einer Seite, die paarweise verbunden sind. Dadurch wird das Signal, das nach den drei Codierscheiben herauskommt, wieder auf einem anderen Weg durch die drei Scheiben zurückgeschickt.

Letztendlich sind die Kontakte der ersten Scheibe durch diesen Mechanismus paarweise verbunden. Damit kann durch Drücken einer Taste für ein Zeichen der entsprechende Kontakt unter Strom gesetzt werden, und die Übersetzung wird durch ebenfalls an der ersten Scheibe angeschlossene Lampen (eine für jedes Zeichen) übersetzt. Außerdem sind zwei Eigenschaften durch diese Anordnung garantiert:

- die Verschlüsselung arbeitet symmetrisch
- ein Zeichen wird nie in sich selbst übersetzt



Dies ganrantiert, dass wenn ein Zeichen codiert wird und man das codierte Zeichen wieder codiert, man das Originalzeichen wieder erhält.

Die Übersetzung eines Zeichens ist also nach obiger Beschreibung nur eine paarweise Ersetzung. Das könnte man auch einfacher haben. Der Trick der Verschlüsselungsmaschine besteht nun darin, daß nach dem Übersetzen eines Zeichens die drei Codierscheiben gedreht werden. Nach jedem Zeichen wird die letzte Scheibe um eine Position gedreht. Sobald diese eine volle Umdrehung gemacht hat, wird die nächste Scheibe um eine Position weitergedreht, usw. Der Schlüssel für eine Übersetzung besteht aus der Startstellung und der Reihenfolge der austauschbaren Scheiben.

Implementierung:

Implementieren Sie eine einfache Enigma mit drei fixen Codierscheiben, die am Beginn der Codierung eine fixe Startstellung haben (=Schlüssel der Codierung nicht veränderbar).

Die Maschine soll Großbuchstaben, "." und Leerzeichen verarbeiten können. Kleinbuchstaben sollen in Großbuchstaben übersetzt werden. Alle anderen Zeichen lösen einen Fehler aus.

Verwenden Sie zum Einlesen der Eingabe die Funktion *getchar* (stdio.h) bzw. Zur Ausgabe *putchar*. Damit arbeitet die Ein-/Ausgabe mit der Standardeingabe/-ausgabe.

Ohne zusätzliche Parameter beim Programmstart arbeitet Ihr Programm mit Eingabe von der Tastatur bzw. Ausgabe auf dem Bildschirm. Durch "Input/Output Redirection" können Sie Dateien verarbeiten:

Bsp.:

beim Start des Programms (enigma.exe) werden folgende Parameter angegeben:

c:\> enigma < in.dat > out.dat

damit wird die Eingabe aus der Datei in.dat gelesen und die Ausgabe in die Datei out.dat geschrieben.

Standards:

Es gelten die üblichen Standards.

Abgabe: bis 12.4. 0:00 Uhr elektronisch (*Verzeichnis uebung1 einrichten!*) und am 13.4. bzw. 14.4. jeweils zu Beginn des Praktikums auf Papier (Listing der Quelldateien).