Christian-Albrechts-Universität zu Kiel
Institut für Informatik und Praktische Mathematik

Prof. Dr. W.-P. de Roever
Martin Steffen

Softwarepraktikum: Enigma

Sommersemester 2003 — 7. April 2003

Handout 3

<u>Handout 3:</u> Allgemeine Aufgabenstellung und erster Abschnitt: Der Enigma-Automat

Ausgabetermin: 7. April 2003

Allgemeine Aufgabenstellung

Die Enigma ist die berühmteste Vertreterin elektomechanischer Verschlüsselungsmaschinen. Sie wurde im zweiten Weltkrieg vom deutschen Militär zur verschüsselten Übermittlung von Morsesignalen auf taktischer Ebene eingesetzt. Es gelang den Allierten, in der Hauptsache den Briten mit entscheidenden Vorarbeiten der Polen, verschiedene Schwächen der Maschine selbst, ihrer Verschlüsselungsprozeduren, und allgemein fehlerhafte und schlampige Bedienung auszunutzen und so routinemäßig, wenn auch mit Unterbrechungen, den Funkverker der Achsenmächte mitzulesen.

Der Gegenstand des Praktikums ist der *Entwurf* und die *Realisierung*

1. einer generischen Enigma sowie einer bestimmten Variante,
2. ihre Visualisierung in einer *graphischen Benutzeroberfläche* sowie
3. die Umsetzung verschiedener *kryptographischer Angriffe*.

Die Implementierungsprache ist *Java*.

Enigma: Variationen und Konventionen

Enigmas wurden in vielen unterschiedlichen Varianten gebaut, kommerziellen wie militärischen. Im Praktikum werden wir aber im wesentlichen an einer Variante orientieren, die während des zweiten Weltkriegs von der Wehrmacht benutzt und als Enigma I bezeichnet wurde. Eine genauere Beschreibung kann aus den auf unserer Seite erwähnten Literaturangaben und Links entnommen werden, zum Beispiel aus [DK85] [HS93], sowie `http://www.codesandciphers.org.uk`.

Zur Vereinfachung der Kommunikation werden die folgenden Sprechweisen im Zusammenhang mit der Verwendung von Walzen vorgegeben. Die konkreten Walzen werden wie üblich mit römischen Ziffern bezeichnet: Walze I, Walze II, ... Die in einer Enigma eingesetzten Walzen werden jeweils als 1. Walze, 2. Walze, ... bezeichnet. Dabei ist die erste Walze diejenige, die der Eingangspermutation am nächsten steht und sich damit am schnellsten dreht.

Daneben sprechen wir vom frühen Modus, wenn eine gemeinsame Grundstellung angenommen wird (bis zum 15.09.1938 genutzt), während wir vom späten Modus sprechen, wenn die Grundstellung vom Bediener selbstgewählt wurde.

Aufgabenstellung: "Enigma"-Automat

Die Aufgabe besteht darin, Enigmas samt ihrer wichtigsten Bestandteile (Walzen, Umkehrwalze, Eintrittswalze, Steckerbrett, ...) nachzubilden und Ver- sowie Entschlüsselung mit Enigmas zu programmieren.

Die Aufgabe ist zweistufig: Es soll eine

- *generische,* anpassbare Enigma sowie eine
- *konkrete* Enigma

realisiert werden. Dabei soll die konkrete Enigma aus der abstrakten (programmiertechnisch) abgeleitet werden.[1] Die generische Enigma soll in folgenden Punkten variabel und anpassbar sein:[2]

- Anzahl und Definition der Walzen
- Definition der Umkehrwalze
- Eingangspermutation/Eingangswalze
- Steckbrett
- Anzahl und Position der Übertragstifte

Für den frei definierbaren Bestandteile der Enigma sollen Sie überprüfen, ob der Benutzer etwas prinzipiell realisierbares definiert oder nicht. Je nach der von Ihnen gewählten

[1] Beachten Sie das sauberes Design mit in die Bewertung miteinfließt.

[2] Was explizit nicht generisch sein soll ist das Alphabet; gehen sie von dem üblichen 26-elementigem Alphabet aus.

Datenrepräsentierung könnte es beispielsweise möglich sein, daß ein Buchstabe im Steckerbrett mit *zwei* weiteren verbunden ist, was den physikalischen Gegebenheiten (ein Kabel mit zwei Klinkersteckern) oder wenn Sie so wollen, den logischen Gegebenheiten (das Steckerbrett realisiert eine Permutation) widerspricht. Fangen Sie derartige Fehlbedienungen ab. Verwenden Sie dazu sinnvoll (d.h. aussagekräftige) *Ausnahmen* (*exceptions*).

Was die *konkrete* Variante betrifft, sollen Sie die realen Walzen mit ihrer Verdrahtung zur Verfügung stellen um daraus eine Instanz der Enigma I generieren zu können. Diese konkrete Enigma ist natürlich wiederum individuell, was ihren Anfangszustand oder allgemein ihren Zustand betrifft, d.h., die Auswahl und Reihenfolge der Walzen, die Ringstellung, die Position der Stecker auf dem Steckerbrett . . . . Darüberhinaus sollten Sie gleichzeitig mehrere Enigmas simulieren können, d.h., es wäre nicht ausreichend, lediglich ein Objekt für Walze II zu haben.

Ein Enigma-Objekt soll Auskunft über den aktuellen Zustand der Enigma geben können (wichtig im Hinblick auf die Visualisierung), einen vorgegebenen Buchstabenverschlüsseln und einen Schritt weitergeschaltet werden können. Dabei sollte das Weiterschalten vom Verschlüsseln entkoppelt sein.

Für den praktischen Einsatz der Enigma sollten Methoden zur Verfügung gestellt werden, die beliebige Zeichenketten im frühen und im späten Modus Ver- und Entschlüsseln. Dabei soll das Schlüsselmaterial sowohl zu fällig hergestellt wie auch direkt vorgegeben werden können.

Testen, Dateiformat Um Ihre Enigmas einfach testen und bewerten zu können, soll es möglich sein, eine *Datei in standartisiertem Format* einlesen und ebenso standartisiert auch wieder *ausgeben* zu können.

Das Format soll darin bestehen, daß der Text aus Großbuchtstaben des Standartalphabetes mit 26 Buchstaben besteht. Der Text ist in *Blöcken* von je 5 Buchstaben unterteilt, dazwischen ein Leerzeichen. Je *10 Blöcke* bilden eine Zeile.

Modellierungsdetails: Bei den Walzen ist zu beachten, daß die Übertragsstifte an den Ringen und nicht am Walzenzylinder angebracht werden.

Hinweis zur Effizienz: Legen Sie Ihren Entwurf so aus, daß die Verschlüsselung eines Buchstabens konstanten Zeitaufwand benötigt unter der Annahme, daß die Alphabetgröße variabel ist.

Termine

In einem ersten Schritt sind Entwürfe zu erstellen, insbesondere UML-Entwürfe. Diese sollen in der Woche vom 21.04.03[3] mit den Betreuern diskutiert werden. Die Abnahme der Aufgabe erfolgt in der Woche vom 5. Mai 2003.

[3] Der 21. April selbst ist Ostermontag sodaß es in dieser Woche keinen Vorlesungsteil gibt.

Literatur

[DK85] Cipher A. Deavours and Louis Kruh. *Machine Cryptography and Modern Cryptanalysis*. IPF. Artech House Books, 1985.

[HS93] F. H. Hinsley and Alan Stripp, editors. *Code Breakers. The Inside Story of Bletchley Park*. Oxford Paperbacks, 1993.