Arbeitsblatt – Verschlüsselung

Name:	Vorname	Klasse:	Datum:
BE:	Punkte:	Zensur:	

Die Enigma (Abb.1)[1] ist eine Rotor-Schlüsselmaschine, die im Zweiten Weltkrieg zur Verschlüsselung des Nachrichtenverkehrs des deutschen Militärs verwendet wurde. Trotz mannigfaltiger, vor und während des Krieges schrittweise eingeführter Verbesserungen der Verschlüsselungsqualität, gelang es den Alliierten mit hohem personellen und maschinellen Aufwand, die deutschen Funksprüche nahezu kontinuierlich zu entziffern.

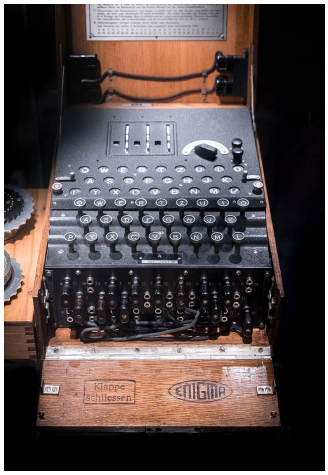
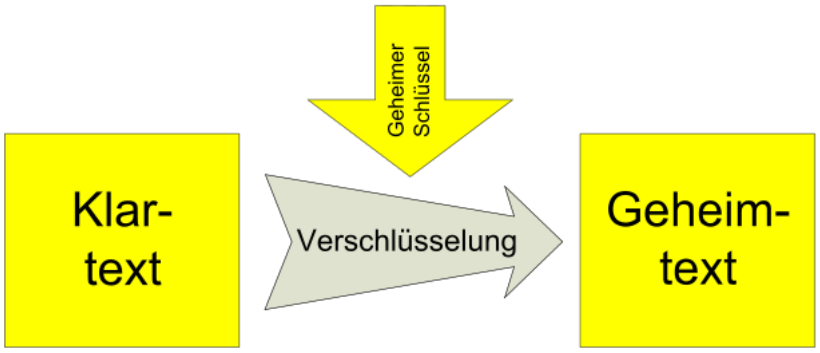


Abbildung 1: Enigma

Verschlüsselung (auch: Chiffrierung) ist die von einem Schlüssel abhängige Umwandlung von „Klartext“ genannten Daten in einen „Geheimtext“ (auch: „Chiffrat“), so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann. Sie dient zur Geheimhaltung von Nachrichten, beispielsweise um Daten gegenüber unbefugtem Zugriff zu schützen oder um Nachrichten vertraulich übermitteln zu können.



[2]

Das Verschlüsseln

Durch Verschlüsseln wird ein „Klartext“, also ein klar lesbarer Text,
in einen „Geheimtext“, also in eine unverständliche Zeichenfolge umgewandelt. Die Begriffe Klartext und Geheimtext sind historisch gewachsen und symbolisch zu sehen. Außer Textnachrichten lassen sich auch andere Arten von Information verschlüsseln, wie Sprachnachrichten, Bildaufzeichnungen oder der Quellcode von Programmen. Die dahinterstehenden kryptographischen Prinzipien bleiben die gleichen. Kryptographisches Codebuch aus dem amerikanischen Bürgerkrieg

[1] Von William Warby from London, England - Enigma, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=46848023
[2] Von Benutzer:Stern - Datei:Verschlüsselung (symmetrisches Kryptosystem).png, Gemeinfrei, https://commons.wikimedia.org/w/index.php?curid=16045036

Eine besondere und relativ einfache Art der Verschlüsselung ist die Codierung (auch: Kodierung). Hierbei werden in der Regel nicht einzelne Klartextzeichen oder kurze Zeichenkombinationen verschlüsselt, sondern ganze Worte, Satzteile oder ganze Sätze. Beispielsweise können wichtige Befehle wie „Angriff im Morgengrauen!“ oder „Rückzug von den Hügeln!“ bestimmten Codewörtern oder unverständlichen Zeichenkombinationen aus Buchstaben, Ziffern oder anderen Geheimzeichen zugeordnet werden. Dies geschieht zumeist als tabellarische Liste, beispielsweise in Form von Codebüchern. Zur Steigerung der kryptographischen Sicherheit von Codes werden die damit erhaltenen Geheimtexte oft einem zweiten Verschlüsselungsschritt unterworfen. Dies wird als Überschlüsselung (auch: Überverschlüsselung) bezeichnet. Außer geheimen Codes gibt es auch offene Codes, wie den Morsecode und ASCII, die nicht kryptographischen Zwecken dienen und keine Verschlüsselung darstellen.

Der Schlüssel

Der entscheidend wichtige Parameter bei der Verschlüsselung ist der „Schlüssel“. Die gute Wahl eines Schlüssels und sein sicherer Schutz vor unbefugtem Zugriff sind wichtige Voraussetzungen zur Wahrung des verschlüsselten Geheimnisses. Im Fall der Codierung stellt das Codebuch den Schlüssel dar. Im Fall der meisten klassischen und auch einiger moderner Methoden zur Verschlüsselung ist es ein Passwort (auch: Kennwort, Schlüsselwort, Codewort oder Kodewort, Losung, Losungswort oder Parole von italienisch la parola „das Wort“; englisch: password). Bei vielen modernen Verschlüsselungen, beispielsweise bei der E-Mail-Verschlüsselung, wird dem Benutzer inzwischen die (Qual der) Wahl eines Schlüssels abgenommen. Der Schlüssel wird automatisch generiert, ohne dass er es bemerkt. Hierdurch wird auch der „menschliche Faktor“ eliminiert, nämlich die nicht selten zu sorglose Wahl eines unsicheren, weil zu kurzen und leicht zu erratenden, Passworts.

Das Entschlüsseln

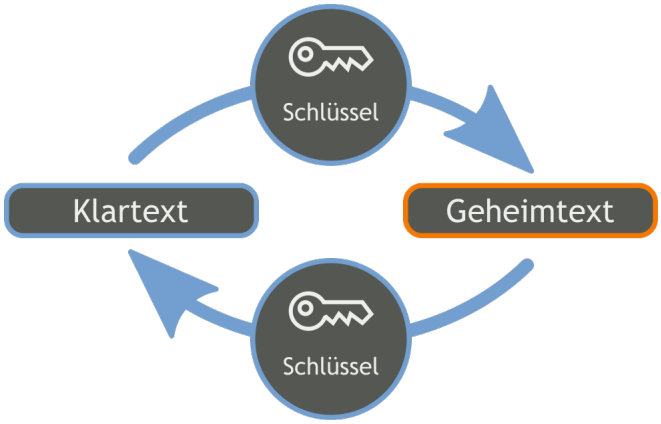
Der zur Verschlüsselung umgekehrte Schritt ist die Entschlüsselung. Zum Entschlüsseln wird der geheime Schlüssel benötigt, mit dessen Hilfe der befugte Empfänger den Geheimtext wieder in den Klartext zurückverwandeln kann. Geht der Schlüssel verloren, dann lässt sich der Geheimtext nicht mehr entschlüsseln. Gerät der Schlüssel in fremde Hände, dann können auch Dritte den Geheimtext lesen, das Geheimnis ist also nicht länger gewahrt.

Symmetrische Verschlüsselung

Symmetrische Verschlüsselungsverfahren verwenden zur Ver- und Entschlüsselung den gleichen Schlüssel. Bei historischen Verfahren lassen sich zwei Verschlüsselungsklassen unterscheiden. Bei der ersten werden, wie bei der im Beispiel benutzen Caesar-Verschlüsselung, die Buchstaben des Klartextes einzeln durch andere Buchstaben ersetzt. Mit dem lateinischen Wort substituere (deutsch: „ersetzen“) werden sie als Substitutionsverfahren bezeichnet. Im Gegensatz dazu bleibt bei der zweiten Verschlüsselungsklasse, genannt Transposition (von lateinisch: transponere; deutsch: „versetzen“), jeder Buchstabe wie er ist, aber nicht wo er ist. Sein Platz im Text wird verändert, die einzelnen Buchstaben des Textes werden sozusagen durcheinandergewürfelt. Eine besonders einfache Form einer Transpositions-Verschlüsselung ist die bei Kindern beliebte „Revertierung“ (von lateinisch: reverse; deutsch: „umkehren“) eines Textes. So entsteht beispielsweise aus dem Klartext „Geheimnis“ der Geheimtext SINMIEHEG.

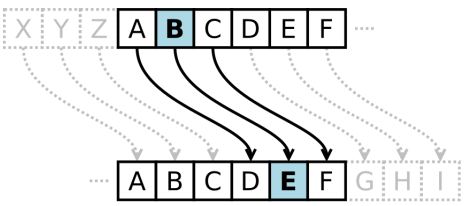
Bei modernen symmetrischen Verfahren werden Stromverschlüsselung und auf einer Blockverschlüsselung basierende Verfahren unterschieden. Bei der Stromverschlüsselung werden die Zeichen des Klartextes jeweils einzeln und nacheinander verschlüsselt. Bei einer Blockverschlüsselung hingegen wird der Klartext vorab in Blöcke einer bestimmten Größe aufgeteilt. Wie dann die Blöcke verschlüsselt werden, bestimmt der Betriebsmodus der Verschlüsselungsmethode.

Interessanterweise beruhen selbst moderne Blockchiffren, wie beispielsweise das über mehrere Jahrzehnte gegen Ende des 20. Jahrhunderts zum Standard erhobene Verschlüsselungsverfahren DES (Data Encryption Standard) auf den beiden klassischen Methoden Substitution und Transposition. Sie verwenden diese beiden Grundprinzipien in Kombination und beziehen ihre Stärke ganz maßgeblich durch die mehrfache wiederholte Anwendung von solchen Kombinationen nicht selten in Dutzenden von „Runden“. So wird, vergleichbar zum wiederholten Kneten von Teig, der Klartext immer stärker verschlüsselt. Die Stärke der Verschlüsselung steigt zumeist mit der Anzahl der verwendeten Runden.[3]



Monoalphabetische Substitution
Verfahren der Kryptographie, bei denen nur ein einziges (festes) Alphabet zur Verschlüsselung, also zur Umwandlung des Klartextes in den Geheimtext, verwendet wird.

Die Caesar-Verschlüsselung
ist ein einfaches symmetrisches Verschlüsselungsverfahren, das auf der monoalphabetischen Substitution basiert. Als eines der einfachsten und unsichersten Verfahren dient es heute hauptsächlich dazu, Grundprinzipien der Kryptologie anschaulich darzustellen.



Aufgabe 1:

[3] https://de.wikipedia.org/wiki/Verschl%C3%BCsselung; 17.05.2017

Entwerfen Sie einen Algorithmus, der nach Eingabe des Klartextes und der Verschiebung den Geheimtext ausgibt.

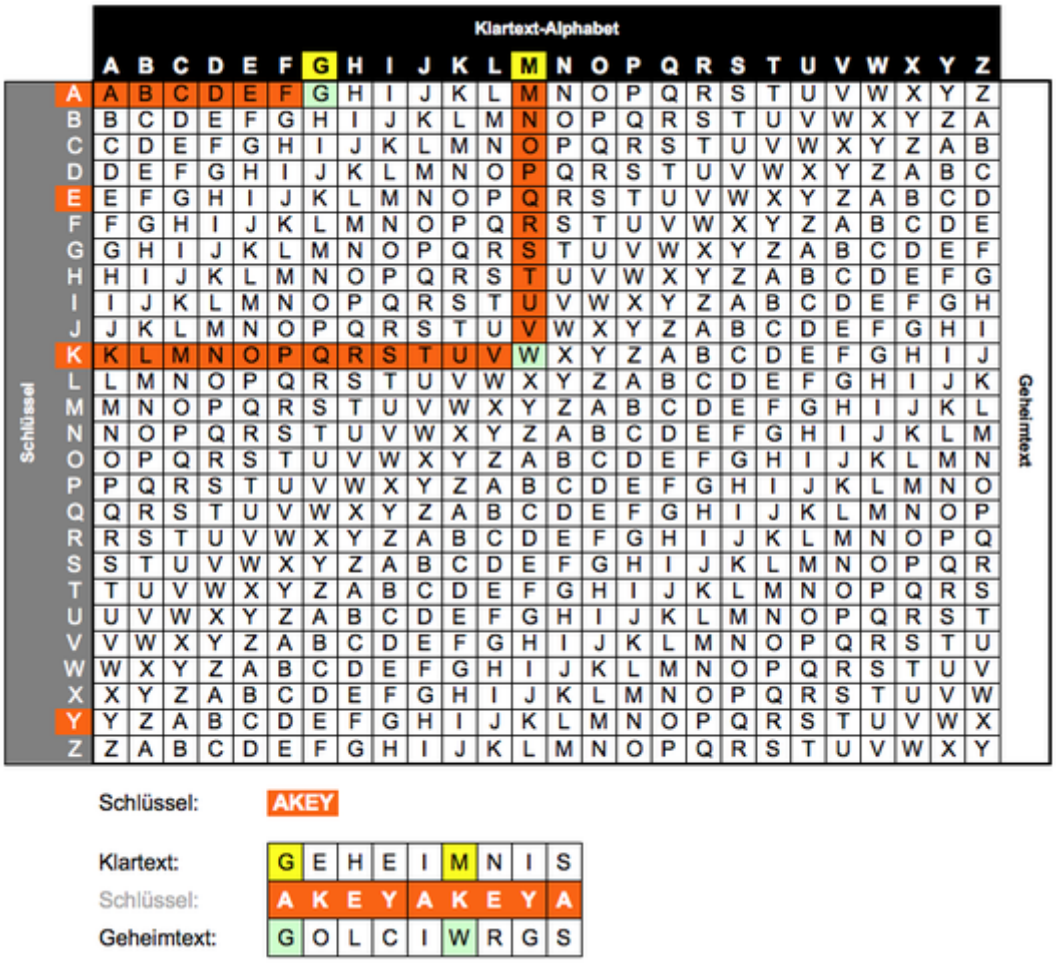
Hinweise:

- Die Texte werden ohne Leerzeichen ein- und ausgegeben.
- Der Klartext wird in Kleinbuchstaben eingegeben.
- Der Geheimtext wird in Großbuchstaben ausgegeben.

Implementieren Sie das Programm.

Polyalphabetische Substitution
bezeichnet in der Kryptographie Formen der Textverschlüsselung, bei der einem Buchstaben/Zeichen jeweils ein anderer Buchstabe/Zeichen zugeordnet wird. Im Gegensatz zur monoalphabetischen Substitution werden für die Zeichen des Klartextes mehrere Geheimtextalphabete verwendet.

Vigenère-Verschlüsselung
Die im 16. Jahrhundert entstandene Vigenère-Verschlüsselung (nach Blaise de Vigenère) galt lange als sicherer Chiffrieralgorithmus („Le Chiffre indéchiffrable“, deutsch: „Die unentzifferbare Verschlüsselung“). Ein Schlüsselwort bestimmt, wie viele und welche Alphabete genutzt werden. Die Alphabete leiten sich aus der Caesar-Substitution ab.



Aufgabe 2:

Entwerfen Sie einen Algorithmus, der nach Eingabe des Klartextes und des Schlüssels den Geheimtext (Vigenère-Verschlüsselung) ausgibt.

Hinweise:

- Die Texte werden ohne Leerzeichen ein- und ausgegeben.
- Der Klartext wird in Kleinbuchstaben eingegeben.
- Der Geheimtext wird in Großbuchstaben ausgegeben.

Implementieren Sie das Programm.

Asymmetrische Verschlüsselung

Über Jahrhunderte hinweg war man der Meinung, dass es keine Alternative zur symmetrischen Verschlüsselung und dem damit verknüpften Schlüsselverteilungsproblem gäbe. Erst vor wenigen Jahrzehnten wurde die asymmetrische Verschlüsselung (engl.: Public-key cryptography) erfunden. Kennzeichen der asymmetrischen Verschlüsselung ist, dass zur Verschlüsselung ein völlig anderer Schlüssel als zur Entschlüsselung benutzt wird. Man unterscheidet hier zwischen dem „öffentlichen Schlüssel“, der zum Verschlüsseln benutzt wird, und dem „privaten Schlüssel“ zum Entschlüsseln des Geheimtextes.

Da asymmetrische Verfahren algorithmisch aufwändiger sind als symmetrische und daher in der Ausführung langsamer, werden in der Praxis zumeist Kombinationen aus beiden, sogenannte Hybrid-Verfahren genutzt. Dabei wird beispielsweise zuerst ein zufällig generierter individueller Sitzungsschlüssel mithilfe eines asymmetrischen Verfahrens ausgetauscht, und dieser anschließend gemeinsam als Schlüssel für ein symmetrisches Verschlüsselungsverfahren benutzt, wodurch die eigentlich zu kommunizierende Information verschlüsselt wird.