

## 3 Projektbeschreibung

Nun beginnt in der dritten Phase die eigentliche Projektarbeit. Jedes Team teilt sich in drei Arbeitsgruppen, die sich jeweils mit folgenden Aufgaben vertraut machen:

1. Verschlüsselung nach Viginere
2. Verschlüsselung nach RSA
3. Gestaltung der grafischen Benutzeroberfläche

In den weiteren Kapiteln werden die beiden Verschlüsselungsverfahren grob vorgestellt. Es ist auf jeden Fall sinnvoll, diese Verschlüsselungstechniken zuerst formell mit Papier und Bleistift durchzuspielen.

### 3.1 Verschlüsselung nach Viginere

Blaise de Vigenère lebte von 1523 bis 1596 in Frankreich und war nach dem Studium bei verschiedenen Herren im diplomatischen Dienst eingestellt. Bei einer diplomatischen Mission in Rom entdeckte er in einem Archiv die Arbeiten von Alberti und anderer Kryptologen. Schnell wurde aus dem anfangs nur praktischen Interesse ein Lebensziel: diese Schriften alle zu studieren und ein neues, mächtigeres Chiffriersystem zu entwickeln. 1570 gab er den Dienst auf und widmete sich seinen Interessen. 1580 veröffentlichte es sein Werk *Traictè de Chiffres*. Das Buch gibt einen genauen Stand der Kryptographie seiner Zeit wieder und enthält außerdem Goldmacherrezepte, Alchemie und japanische Ideogramme.



Abbildung 3.1: Blaise de Viginere

Als Grundlage der Viginere-Verschlüsselung dient die so genannte Viginere-tabelle. In der ersten Zeile steht das Klartextalphabet, darunter die Geheimtextalphabete jeweils um einen Buchstaben versetzt. Mit Hilfe dieser Tabelle konnte man im 15. Jahrhundert Botschaften folgendermaßen verschlüsseln.

Klar	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
1	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	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	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
26	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

**Abbildung 3.2:** Viginere-Quadrat mit hervorgehobenen Zeilen, die durch das Schlüsselwort LICHT betsimmt sind.

Die Abbildung 3.3 zeigt die Verschlüsselung des Klartexts „truppenabzugnachosten“

Schlüsselwort	L I C H T L I C H T L I C H T L I C H T L
Klartext	t r u p p e n a b z u g n a c h o s t e n
Geheimtext	E Z W W I P V C I S F O P H V S W U A X Y

**Abbildung 3.3:** Verschlüsselung mit Hilfe des Schlüsselworts LICHT

Man benötigt ein Schlüsselwort, hier z.B. LICHT und schreibt dieses über die zu verschlüsselnde Botschaft, hier Klartext genannt. Um also den ersten Buchstaben "t" der Botschaft "truppenabzugnachosten" zu codieren, findet man in der Zeile "L" (von LICHT) und in der Spalte "t" (von truppen...) den entsprechenden Geheimbuchstaben "E". Um den 2. Buchstaben "r" zu verschlüsseln, findet man in der Zeile "I" und in der Spalte "r" den Geheimbuchstaben "Z". Und so geht es weiter. Jeder kann die Vigenere-Tabelle besitzen, aber um den Geheimtext zu entschlüsseln, braucht man auf jeden Fall das Schlüsselwort "Licht". Über 300 Jahre, bis 1853, dauerte es, bis Babbage ein Verfahren fand, diese Verschlüsselung zu knacken ohne Kenntnis des Schlüsselworts mit Hilfe einer Häufigkeitsanalyse von Buchstaben.

### 3.2 Verschlüsselung nach RSA

Die drei Mathematiker Rivest, Shamir und Adleman entwickelten 1977 das nach ihnen benannte RSA-Verfahren. Es basiert auf der Idee, dass die Faktorisierung einer großen Zahl, also ihre Zerlegung in (mindestens zwei) Faktoren, eine sehr aufwändige Angelegenheit ist, während das Erzeugen einer Zahl durch Multiplikation zweier Primzahlen trivial ist.



**Abbildung 3.4:** Ronald Rivest (in der Mitte), Adi Shamir (links) und Leonard Adleman (rechts),

Ich will nun das RSA-Verfahren an einem Beispiel verdeutlichen. An Alice sollen verschlüsselte Botschaften versendet werden. Dazu stellt Alice einen

öffentlich bekannten Schlüssel (public key) zur Verfügung. Jeder kann diesen Schlüssel verwenden, um seine Botschaften an Alice zu kodieren. Bob verwendet nun diesen Schlüssel, um eine verschlüsselte Nachricht an Alice zu senden. Nach der Verschlüsselung ist es nur noch Alice möglich, diese Nachricht zu dekodieren, da nur sie die "Zusammensetzung" (private key) des von ihr erzeugten (öffentlichen) Schlüssels kennt.

#### Bemerkung:

Zuerst müssen die Buchstaben in Zahlen verwandelt werden. Dazu eignet sich natürlich der ASCII-Code. Dadurch entstehen bei den Großbuchstaben Zahlen zwischen 65 und 90. Um nun ein Beispiel mit Hilfe des Taschenrechners durchzuspielen, benötige ich möglichst kleine Zahlen. Beim RSA-Verfahren müssen nämlich zwei Primzahlen gewählt werden, deren Produkt größer ist als die größte Zahl, die die Buchstaben darstellen. Deshalb nummeriere ich die Buchstaben von 1 bis 26 (ASCII – 65). Somit können im folgenden Beispiel kleinere Primzahlen gewählt werden.

### 3.2.1 Öffentlicher Schlüssel (public key)

Alice muss also zuerst einen öffentlichen Schlüssel erzeugen. Sie wählt zwei riesige Primzahlen  $p$  und  $q$ . Die Primzahlen sollten sehr groß sein, doch der Einfachheit halber nehmen wir an, dass Alice  $p = 5$  und  $q = 11$  wählt. Diese Zahlen muss sie geheim halten.

Alice multipliziert diese beiden Primzahlen miteinander und erhält die Zahl  $N$ , in diesem Fall ist  $N = 55$ .

Nun errechnet Alice eine Hilfszahl

$$Z = (p-1) \cdot (q-1) = (5 - 1) \cdot (11 - 1) = 40.$$

Sie wählt jetzt eine weitere Zahl  $E$ , die prim ist und zugleich kein Teiler von dieser Hilfszahl  $Z$  ist, in diesem Fall z.B.  $E = 7$ .

Jetzt kann Alice diese beiden Zahlen  $E$  und  $N$  in einem öffentlichen Verzeichnis ablegen, so dass jeder Zugang zu diesen beiden Zahlen hat. Diese stellen also den öffentlichen Schlüssel (public key) dar, also  $N = 55$  und  $E = 7$ .

### 3.2.2 Verschlüsselung

Bob will nun Alice eine Mitteilung machen. Er muss also die Buchstaben des Klartextes zuerst in Zahlen umwandeln. Dazu nummeriert er das Alphabet durch:  $A = 0$ ,  $B = 1$ ,  $C = 2$ , ...,  $Z = 25$ . Nun sucht er den öffentlichen Schlüssel

von Alice heraus, also  $N = 55$  und  $E = 7$ . Damit kann er jeden Klartextbuchstaben  $K$  in den Geheimbuchstaben  $G$  umrechnen nach folgender Formel

$$G = K^E \bmod N \quad [K = \text{Klartextbuchstabe}, G = \text{Geheimbuchstabe}]$$

Nehmen wir nun an, Bob will an Alice den Klartextbuchstaben „M“ verschlüsselt senden.

$$\text{„M“} = 12$$

$$G = 12^7 \bmod 55 = 35831808 \bmod 55$$

Bei großen Primzahlen wird diese Berechnung schwierig werden. Hierzu kann deshalb die Kongruenzarithmetik verwendet werden, indem  $12^7$  (bezüglich des Modulus 55) schrittweise durch eine dazu kongruente kleinere Zahl ersetzt wird.

$$G = \{[12 \bmod 55 \cdot 12] \bmod 55 \cdot 12\} \bmod 55 \dots\dots\dots$$

$$G = 23$$

Aus dem Klartext  $K = 12$  (entspricht dem Buchstaben „M“) ist somit der Geheimtext  $G = 23$  geworden. Jetzt schickt Bob den Geheimtext „23“ an Alice.

### 3.2.3 Geheimer Schlüssel (private key)

Da die Modul-Arithmetik eine Einwegfunktion ist, ist es sehr schwer, bei sehr großen Zahlen sogar unmöglich, von  $G = 23$  den Weg zurückzugehen und auf die ursprünglich Botschaft zu schließen.

Alice jedoch kann die Botschaft entschlüsseln, weil nur sie eine bestimmte Information hat, nämlich die beiden Primzahlen  $p$  und  $q$ . Daraus berechnet sie eine besondere Zahl  $D$ , den privaten Schlüssel (private key). Diese Zahl  $D$  wird nach folgender Formel berechnet:

$$E \cdot D = 1 \bmod ((p-1) \cdot (q-1))$$

also

$$E \cdot D = 1 \bmod 40 = \{1, 41, 81, 121, \mathbf{161}, 201, 241, 281, 321, 361, 401, \mathbf{441}, \dots\}$$

Aus all diesen Zahlen sucht man nun eine, die  $E$  (hier 7) als Teiler haben, z.B.

$$D = 161 : 7 = 23 \quad \text{oder auch}$$

$$D = 441 : 7 = 63$$

Somit besitzt nun Alice den geheimen Schlüssel (private key), also  $N = 55$  und  $D = 23$ .

### 3.2.4 Entschlüsselung

Um die Mitteilung von Bob nun zu entschlüsseln, benutzt Alice einfach folgende Formel:

$$K = G^D \pmod{N} \quad [K = \text{Klartextbuchstabe}, G = \text{Geheimtextbuchstabe}]$$

$$\begin{aligned} K &= 23^{23} \pmod{55} \\ &= \{[23 \pmod{55}] \cdot 23\} \pmod{55} \cdot 23 \pmod{55} \dots \dots \dots \\ &= 12 \end{aligned}$$

also  $K = 12 = \text{„M“}$ .

Alice kann also die von Bob verschlüsselte Nachricht lesen.

Ein weiteres Beispiel zum Probieren:

$$\begin{aligned} \text{„H“} &= 72 - 65 = 7 \\ G &= 7^7 \pmod{55} = 28 \\ K &= 28^{23} \pmod{55} = 7 = \text{„H“} \end{aligned}$$

Verwende nun folgenden Schlüssel:

$$\begin{array}{lll} p = 47 & N = 2773 & D = 157 \\ q = 59 & E = 17 & \end{array}$$

Auf den folgenden Webseiten findest du weitere Informationen über das RSA-Verfahren:

<http://www-lehre.informatik.uni-osnabrueck.de/~dbs/2001/skript/node144.html>

<http://www.matheprisma.uni-wuppertal.de/Module/RSA/index.htm>

## 3.3 Die grafische Benutzungsoberfläche

Die Abbildungen 3.5 bzw. 3.6 zeigen als Beispiel, wie die grafische Benutzungsoberfläche gestaltet werden könnte. Diese Oberfläche ähnelt den Benutzungsschnittstellen aus den Kapiteln 1. bzw. 2. Mit Hilfe der Reiter lassen sich verschiedene Verschlüsselungstechniken auswählen. Dementsprechend

verändert sich die Oberfläche in einigen Details. Jedoch lässt Java-Swing viele weitere Gestaltungsmöglichkeiten zu.



**Abbildung 3.5:** Ein Klarwort wird nach Caesar codiert



**Abbildung 3.6:** Ein Geheimwort wird nach Viginere decodiert