Inhalt

Lerntätigkeiten der AdressatInnen im Vorfeld

Das vorliegende Unterrichtskonzept mit der Lernaufgabe führt in ein neues Gebiet ein. Es werden wenige Begriffe aus der Welt der Kryptologie benötigt. Diese Begriffe werden den Studierenden in der Hinführung zur Lernaufgabe vermittelt. Es gibt keine Voraussetzungen an die Studierenden, die direkt im Vorfeld zu diesem Unterricht erfüllt werden müssten.

Es gibt allerdings eine Voraussetzung allgemeinerer Art: Der Unterricht nimmt an einigen Stellen Bezug auf das Internet und E-Mail als Kommunikationsmittel. Die Studierenden müssen die Begriffe Internet und E-Mail kennen. Konkret sollten sie wissen:

- Das **Internet** ist ein riesiges Netzwerk von TeilnehmerInnen. Alle TeilnehmerInnen können miteinander kommunizieren. Das Internet bietet immense Mengen an Information an, und der Informationsaustausch ist rege. Das Internet ist weltumspannend. Die TeilnehmerInnen am Internet sind beliebig, sie kennen sich in der Regel nicht.
- **E-Mail** oder **Electronic Mail** ist der am häufigsten benutzte Dienst zum Informationsaustausch im Internet. E-Mail funktioniert ganz analog zur normalen Post. Das heisst: Eine E-Mail wird mit der Zieladresse versehen und losgeschickt. Optimal wäre natürlich, wenn die Studierenden selbst schon E-Mails verfasst und verschickt hätten.

Unterrichtsvorbereitung

Beschreibung des Unterrichts – Sequenz

	Inhalt	*Methode*	*Dauer*
1	Der Informierende Unterrichtseinstieg liegt im Abschnitt mit demselben Namen fertig ausformuliert vor. Dazu gehören vier Folien (Abschnitt "Folienvorschau").	Vortrag der Lehrperson	4'
2	Der Vortrag der Lehrperson führt kurz in das Thema ein. Anschliessend werden die *Klassischen Methoden* vor allem anhand der CAESAR-Methode vorgestellt. Die Hintergrundinformationen für die Lehrperson befinden sich im Abschnitt "Klassische Verschlüsselungsmethoden". Der Abschnitt enthält auch Themen, die nicht unbedingt mit den StudentInnen behandelt werden müssen und je nach Bedarf in den Unterricht eingebaut werden können. So zum Beispiel der geschichtliche Exkurs.	Vortrag der Lehrperson	10'
3	An dieser Stelle folgt eine Gruppenarbeit. Dabei spielen die Studierenden das System CAESAR selber durch. Sie erkennen auch, wie einfach es zu brechen ist. Die Anleitung zur Gruppenarbeit für die Studierenden liegt fertig ausformuliert vor. Als Illustration zur Gruppenarbeit dient nochmals die erste Folie des Informierenden Unterrichtseinstiegs.	Arbeit zu dritt	18'
4	In der Lernaufgabe lernen die Studierenden die Idee hinter den *Public Key Verfahren* kennen. Für die Lernaufgabe ist ein eigenes Kapitel reserviert.	Lernaufgabe	20'
5	Die Antworten auf die Fragen der Lernaufgabe sowie einige Hintergrundinformationen und die Terminologie liegen ebenfalls schriftlich vor. Die Unterlagen werden an die StudentInnen verteilt und werden selbständig studiert. Für die Lehrperson liegt zusätzliches Material vor (Abschnitt "Public Key Kryptologie – Etwas zum Hintergrund").	Selbststudium	8'
6	Der letzte Teil ist für allfällige Fragen der Studierenden reserviert.	Klasse	5'

Informierender Unterrichtseinstieg

In dieser Lektion beschäftigen wir uns mit der Frage: Wie wird eine Nachricht verschlüsselt, ohne dass man sie gleich knacken kann? Es geht also um die folgende Situation: Alice möchte eine wichtige Nachricht an Bob schicken. Die Nachricht soll verschlüsselt werden. Hier in der Mitte befindet sich der "Feind" namens Mallet. Mallet legt alles daran, die Nachricht abzufangen und zu entschlüsseln, damit er sie lesen kann. Sie werden zwei Arten zur Verschlüsselung von Daten kennenlernen. Die *klassischen* und die *Public Key Methoden*.

In einem ersten Teil werde ich Ihnen eine sehr alte und nicht sehr wirkungsvolle Methode vorstellen. Sie heisst CAESAR. In einer kurzen Gruppenarbeit werden Sie anschliessend CAESAR genauer unter die Lupe nehmen und die Schwachstelle selber kennenlernen. CAESAR gehört zu den sogenannten *klassischen Verschlüsselungsmethoden*. Alle klassischen Methoden weisen einen grossen Nachteil auf. Dieser Nachteil wird durch eine andere Art von Verschlüsselungsmethoden behohoben. Diese besseren Verfahren heisse*n Public Key Verfahr*en. Sie werden selbständig die grundlegende Idee hinter den Public Key Verfahren erarbeiten. Zusammen mit den richtigen Antworten auf die Arbeit erhalteSie einige Hintergrundinformationen. Für das Studium dieser Unterlagen haben Sie einige Minuten Zeit.
Zum Schluss bleibt noch etwas Zeit für allfällige Fragen.

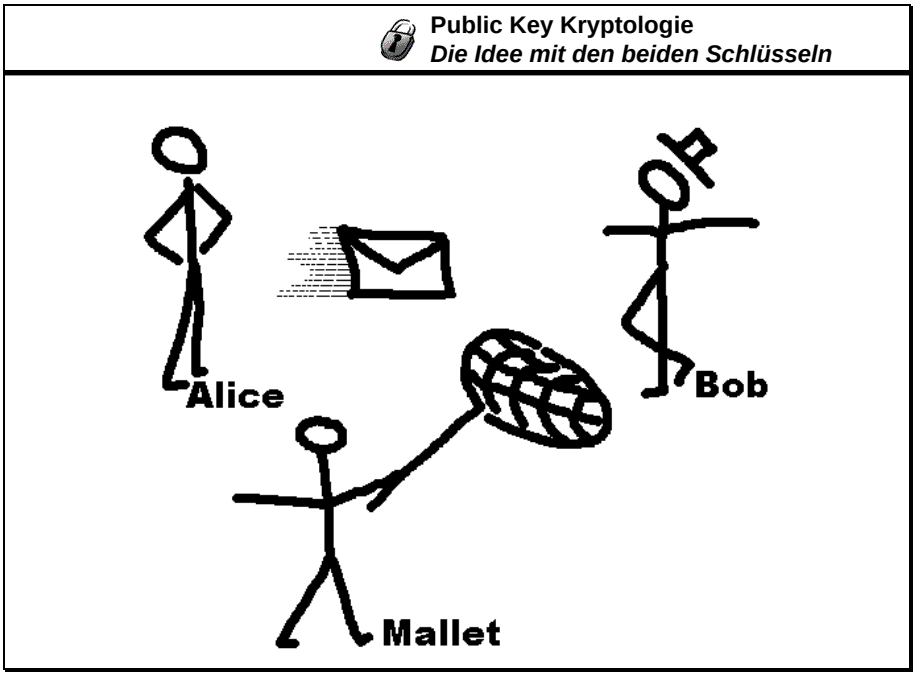
Was können Sie nach dieser Lektion?

- Sie kennen die Verschlüsselungsmethode CAESAR als Beispiel für eine klassische Methode. Das heisst: Sie können eine Nachricht mit Hilfe von CAESAR verschlüsseln und auch wieder entschlüsseln. Sie kennen die wichtigste Eigenschaft, die allen klassischen Methoden gemeinsam ist.
- Sie können umgangssprachlich erklären, welches die entscheidende Idee hinter den Public Key Verfahren ist. Zum Beispiel mit Hilfe der Analogie mit dem Schnappschloss und dem Schlüssel. Insbesondere können Sie auch erklären, warum Public Key Verfahren funktionieren. Oder worauf sich die Verfahren verlassen, damit sie sicher sind.

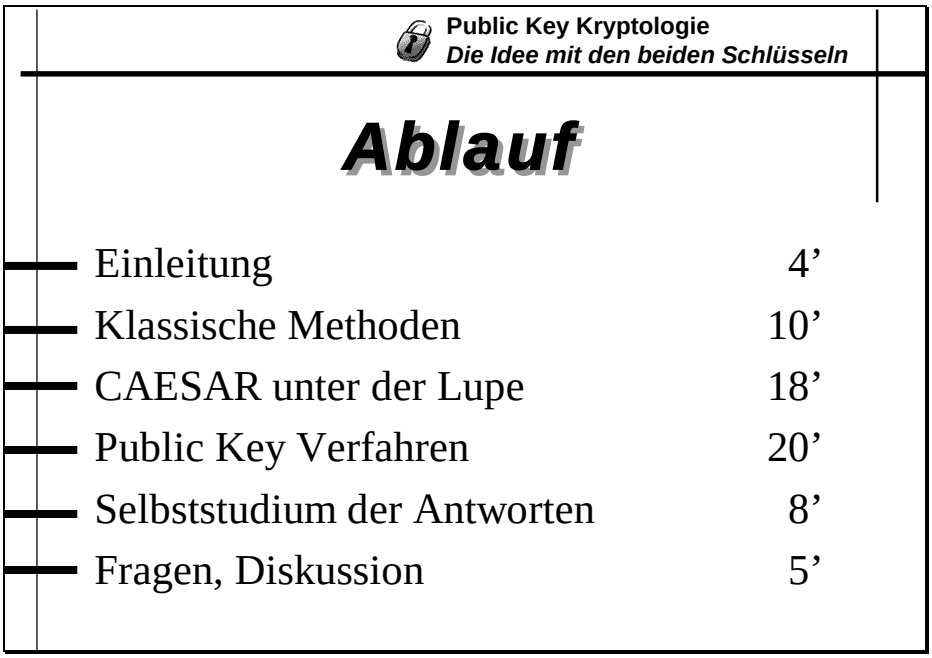
Und wozu behandeln wir das Thema? Das Gebiet der Verschlüsselung und Entschlüsselung von Daten gewinnt immer mehr an Bedeutung. Vor allem im Internet werden Public Key Verfahren häufig verwendet, weil das Internet prinzipiell nicht abhörsicher ist. Deshalb ist es wichtig, dass Sie die Grundlagen kennen. Die Betonung liegt auf dem Wort "Grundlagen". Die mathematischen Hintergründe werden wir gänzlich ausser Acht lassen. Wir konzentrieren uns auf die Ideen und Konzepte.

Übrigens: Schon zweimal haben Sie nun das Wort "Kryptologie" gesehen. Kryptologie ist der Name der Wissenschaft, die sich mit dem Ver- und Entschlüsseln von Daten befasst. "Public Key" heisst soviel wie "öffentlicher Schlüssel". Was das bedeutet, werden Sie selber herausfinden.

Folienvorschau

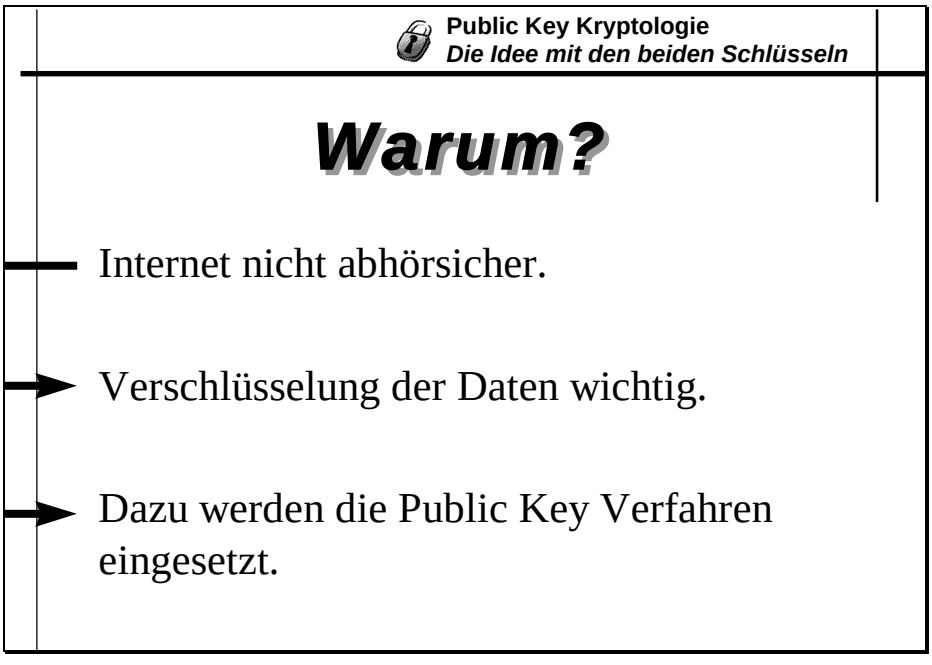


Folie 1 – Einführung in das Thema und Vorstellung der beteiligten Personen



Folie 2 – Ablauf der Lektion

Folie 3 – Ziele der Lektion



Folie 4 – Begründung

Klassische Verschlüsselungsmethoden

Alice und Bob kommunizieren miteinander (Die erste Folie aus dem Informierenden Unterrichtseinstieg dient zur Illustration). Ihre Nachrichten können sie wie im Mittelalter per Pferdekurier oder ganz modern mittels E-Mail im Internet verschicken. Das Problem bleibt immer dasselbe: Die Nachrichten können durch Unberechtigte abgefangen und gelesen werden. Hier zum Beispiel durch Mallet.
Was also können Alice und Bob tun, um Mallet einen Strich durch die Rechnung zu machen? Die Lösung liegt auf der Hand. Die beiden versuchen, ihre Botschaften geheim zu halten. Eine altbekannte Methode: Sie verwenden Zitronensaft als Tinte. Dadurch wird die Botschaft unsichtbar. Durch Erwärmung (zum Beispiel mit einem Bügeleisen) wird die Nachricht wieder sichtbar gemacht. Auf diese Weise wird die Nachricht ganz einfach versteckt.
Eine andere Methode ist CAESAR. Der Name stammt von dem berühmten römischen Feldherrn. Er hat die Technik selber angewendet. Es handelt sich hier um eine sehr simple Verschlüsselungsmethode.

Die Verschlüsselungsmethode CAESAR

CAESAR arbeitet mit *Substitutionen*: Jeder Buchstabe des Alphabets wird durch einen anderen ersetzt. Der neue Buchstabe wird erhalten, indem vom alten Buchstaben um eine bestimmte Anzahl Schritte weiter gerückt wird. Am Ende des Alphabets wird zyklisch wieder am Anfang begonnen. CAESAR hat also einen Parameter: Die Anzahl der Schritte, welche die Buchstaben voneinander trennt.

Das folgende **Beispiel** verschiebt um drei Positionen:

```
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
⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓
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
```

Die obere Zeile zeigt das alte, normale Alphabet. Die untere Zeile stellt das neue, verschobene Alphabet dar. Das neue Alphabet dient nun zur **Verschlüsselung** von Texten. Zum Beispiel wird die Nachricht GUTENTAG verschlüsselt zu JXWHQWDJ.
Entschlüsselt wird die Nachricht völlig analog. Jeder Buchstabe wird durch den drei Positionen weiter vorne liegenden ersetzt. Die benötigte Schablone sieht gleich aus wie die obige. Lediglich die Reihenfolge der Zeilen wird vertauscht:

```
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
⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓ ⇓
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
```

Genau hier liegt das grosse **Problem**: Aus der Methode zur Verschlüsselung kann problemlos und innert kürzester Zeit das Vorgehen zum Entschlüsseln hergeleitet werden. CAESAR kann also nur dann funktionieren, wenn die **Methode geheim bleibt**.

Eigenschaften klassischer Verschlüsselungsmethoden

Alle klassischen Methoden weisen dasselbe Problem auf wie CAESAR. Sobald die Verschlüsselungsmethode bekannt wird, kann daraus das Verfahren zur Entschlüsselung gewonnen werden. Natürlich geht das nicht bei jedem System so schnell wie bei CAESAR. Trotz-

dem ist es in jedem Fall innert nützlicher Frist möglich. Die Folge: Die Verschlüsselungsmethode muss unbedingt **geheim bleiben**.
Diese Eigenschaft der klassischen Verfahren ist der Grund dafür, dass diese auch als *symmetrische* oder *Einwegverfahren* bezeichnet werden.

Konsequenz: Bevor sie sensible Nachrichten austauschen, müssen sich Alice und Bob über das Verschlüsselungsverfahren einigen. Dazu benötigen sie einen geheimen, sicheren Kanal. Eine Möglichkeit: Alice und Bob treffen sich persönlich und vereinbaren das Verfahren.
Häufig ist das allerdings illusorisch. Gerade im Internet gibt es keine sicheren Kanäle. Sämtliche Leitungen können grundsätzlich abgehört werden. Und sich persönlich zu treffen ist meistens undenkbar und zu aufwendig; zum Beispiel wenn die Kommunikation zwischen Japan und Südafrika stattfindet.

Geschichtlicher Exkurs – Kryptologie im Altertum

Von Sueton wird überliefert, dass Julius Cäsar das Verfahren CAESAR selber angewendet hat. Cäsar soll dabei das Alphabet immer um drei Stellen verschoben haben. Von anderen Zahlen wird nirgends berichtet.
Aber CAESAR ist nicht das älteste System. Die vielleicht älteste bekannte Technik stammt vom griechischen Historiker Polybios, welcher 30 Jahre vor Cäsars Geburt starb. Allerdings ist nicht bekannt, ob Polybios seine Methode zur Verschlüsselung von Nachrichten benutzt hat. Er benutzte das sogenannte *Polybios Checkerboard*:

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Jedem Buchstaben entspricht demnach ein Buchstabenpaar entlang der entsprechenden Zeile und Kolonne: T, K und O werden so zu DD, BE und CD. Der Text GUTENTAG wird verschlüsselt zu BBDEDDAECCDDAABB.

Ein anderes Prinzip ist das "Verstecken der Nachricht". Oder mit dem Fremdwort: **Steganographie**. Der erwähnte Trick mit Zitronensaft und Bügeleisen fällt in diese Klasse. Es wird nichts verschlüsselt; der Text bleibt im Klartext und wird einfach versteckt.
Dazu eine kleine Anekdote von Herodot: Histaios hatte eine Abmachung mit seinem Schwiegersohn Aristagoras: Sobald er eine Nachricht bestehend aus einigen Punkten erhielt, sollte Aristagoras die Revolution gegen Persien starten. Als Histaios die Nachricht tatsächlich schicken wollte, war das Gebiet zwischen ihnen zu stark bewacht. Die Meldung hätte nicht gefahrlos übermittelt werden können. Also liess Histaios den Kopf eines Sklaven rasieren. Auf die Kopfhaut malte er die Punkte. Als das Haar nachgewachsen war, schickte er den Sklaven zu Aristagoras mit der Nachricht: "Rasiere meinen Kopf!"
Die Geschichte ist ein Beispiel für die Kombination von Verschlüsseln und Verstecken: **Krypto-Steganographie**.

CAESAR unter der Lupe

Anleitung zur Gruppenarbeit

Eigentlich haben Sie in den letzten zehn Minuten schon alles wichtige zur Verschlüsselungsmethode CAESAR erfahren. In der Gruppenarbeit geht es darum, dass Sie das Verfahren selber kurz durchspielen. Ausserdem werden Sie sehen, wie einfach CAESAR geknackt werden kann.

Arbeitsform

Sie arbeiten zu dritt. Sie verteilen die Rollen entsprechend der bekannten Situation: Alice und Bob tauschen Nachrichten aus. Mallet ist der "Spion", der die Nachrichten abfängt und zu entschlüsseln versucht. Als Hilfsmittel benötigen Sie nur Papier und Schreibzeug.
Zur Bearbeitung der Aufgaben stehen Ihnen 15 Minuten zur Verfügung. Anschliessend haben wir einige Minuten Zeit, um auf Fragen einzugehen.

Ziele

In dieser Gruppenarbeit sollen Sie CAESAR als Beispiel für *klassische Verschlüsselungsverfahren* konkret durchspielen. Dabei erfahren Sie, welches der grundlegende Nachteil von CAESAR ist: Aus dem Vorgehen für die Verschlüsselung kann problemlos die Methode zur Entschlüsselung gewonnen werden. Deshalb muss das Verfahren unbedingt geheim bleiben.
Nach der Arbeit sollten Sie in der Lage sein, CAESAR umgangssprachlich zu erklären. Ausserdem sollten Sie den eben geschilderten Nachteil kennen. Sie brauchen nichts schriftliches abzugeben, und die Arbeit wird selbstverständlich auch nicht bewertet.

Aufgabe 1 – Mallet weiss von nichts.

Spielen Sie in Ihrer Gruppe die folgenden Punkte exakt durch:

1) Alice und Bob einigen sich darüber, wie stark die Alphabete im CAESAR-System verschoben werden sollen. Beispiel: A wird zu F, B zu G, und so weiter. Diese Information bleibt geheim. Mallet erfährt nichts!

2) Bob wählt eine kurze Nachricht. Höchstens drei Worte. Er verschlüsselt den Text mit Hilfe der unter 1) getroffenen Vereinbarung. Bob schreibt den verschlüsselten Text auf ein Stück Papier und schiebt es in Richtung Alice.

3) Bevor die Nachricht Alice erreicht, fängt Mallet sie ab. Er schreibt den Text ab und schickt das Original weiter an Alice.

4) Alice und Mallet sind nun beide im Besitz der verschlüsselten Botschaft. Sofort machen sich beide an die Entschlüsselung. Wie lange hat Alice, die über die Zusatzinformation aus 1) verfügt? Schafft es auch Mallet in weniger als zwei Minuten?

Aufgabe 2 – Mallet ist informiert.

Der Ablauf ist gleich wie in Aufgabe 1. Der grosse Unterschied: Diesmal weiss auch Mallet darüber Bescheid, um wieviele Positionen die CAESAR-Alphabete verschoben werden. Spielen Sie mit dieser neuen Voraussetzung den Ablauf aus Aufgabe 1 nochmals durch. Wie lange hat Mallet nun, um die Botschaft zu entschlüsseln? Welches Fazit ziehen Sie aus dem Vergleich von Aufgabe 1 und 2?

Die Lernaufgabe

Zugehöriges Schul-/Studienbuch

Die Lernaufgabe gehört zu keinem Buch.

Das Neue

Die StudentInnen lernen das zugrundeliegende Konzept der *Public Key Verfahren* kennen: Die Verschlüsselung geht sehr einfach. Dagegen ist das Vorgehen zur Entschlüsselung zwar offensichtlich und dennoch nicht praktikabel, weil das Entschlüsseln zu lange dauern würde. Nur mit dem richtigen Hilfsmittel (Spezialausgabe des Telefonbuchs) ist die Entschlüsselung effizient möglich. Darum ist es absolut unnötig, das Verfahren geheim zu halten. Das ist der grosse Vorteil gegenüber den klassischen Verschlüsselungsmethoden.
Die beschriebene Idee wird in der Lernaufgabe anhand eines anschaulichen Beispiels illustriert. Dadurch wird die Materie für die StudentInnen verständlicher. Ausserdem dürfte sich das Beispiel besser im Gedächtnis festsetzen als etwas vergleichbares aus der Mathematik.

Bewertung der Antworten

Die richtigen Antworten sind getrennt vermerkt und dienen auch als Material für die Studierenden. An dieser Stelle soll lediglich auf ein mögliches Bewertungsschema hingewiesen werden. Grundsätzlich ist für die Lernaufgabe allerdings keine Bewertung vorgesehen.

Aufgabe 1

- Nummer suchen und Anfangsbuchstaben des Familiennamen wählen. *1 Punkt*

Aufgabe 2

- Die Nachricht kann auch mit dem normalen Telefonbuch entschlüsselt werden. *1 Punkt*
- Problem: Die Suche geht zu lange. *3 Punkte*
- Grund: Das Telefonbuch ist falsch geordnet.

Oder: Schlimmstenfalls müssen sämtliche Einträge im Telefonbuch geprüft werden. *1 Punkt*

Aufgabe 3

- Das Verfahren muss nicht geheim bleiben. *3 Punkte*
- Grund: Die Entschlüsselung ohne Spezialausgabe geht zu lange. *1 Punkt*

Maximalpunktzahl = 10 Punkte

Materialien und Dokumentation

Für die Lernaufgabe werden ausser Schreibzeug und Papier keine zusätzlichen Materialien oder Dokumentationen benötigt.

Public Key Kryptologie

Die Idee mit den beiden Schlüsseln

Arbeitsanleitung

Sie haben unterdessen einiges über *klassische Verschlüsselungsmethoden* erfahren. CAESAR ist ein Beispiel für eine klassische Methode. Sämtliche klassischen Methoden weisen ein grosses Problem auf: Das Verfahren zur Verschlüsselung und Entschlüsselung muss unbedingt geheim bleiben. Das Verfahren muss also auf einem abhörsicheren Weg festgelegt werden. Leider gibt es aber gerade im Internet keine abhörsicheren Leitungen. Deshalb lernen Sie in den folgenden Aufgaben ein Verfahren kennen, das dieses Problem löst.
Zunächst allerdings einige organisatorische Angaben.

----------Vorgehen----------

Sie bearbeiten die Aufgaben alleine. Zum Lösen der Aufgaben stehen Ihnen insgesamt 20 Minuten zur Verfügung. Hilfsmittel sind keine nötig. Höchstens Papier und Schreibzeug für Ihre Notizen. Notieren Sie Ihre Antwort bei jeder Aufgabe. Stichworte genügen, aber versuchen Sie, genau zu sein!

---------- Ziele----------

Sie sollten in der Lage sein, sämtliche Aufgaben in der Zeit zu bearbeiten und sich Ihre Gedanken dazu zu machen. Bei den meisten Aufgaben sind verschiedene Teilfragen notiert; es sollen alle beantwortet werden. Anhand der schriftlichen Unterlagen können Sie vergleichen, ob Sie die Aufgaben richtig gelöst haben. Wichtig ist, dass Sie die grundlegende Idee und Eigenschaft des Verfahrens mit dem Telefonbuch kennen. Auch im Vergleich zu CAESAR.
Nach Abschluss der Arbeit brauchen Sie nichts abzugeben, Ihre Leistung wird nicht bewertet.

---------- Verschlüsseln per Telefonbuch----------

Wir betrachten ein anderes Verfahren für die Verschlüsselung von Texten. Als Hilfsmittel benötigen Sie ein *umfangreiches* Telefonbuch. Zum Beispiel dasjenige der Stadt Zürich. Es ist wie gewohnt alphabetisch nach Familiennamen geordnet.
Wie können Sie damit die Botschaft JA verschlüsseln? Sie suchen sich zuerst eine Abonnentin, deren Familienname mit J beginnt. Zum Beispiel Christine Joly. Ihre Nummer lautet 312 23 08. Anschliessend wählen Sie einen beliebigen Abonnenten unter all jenen, die mit A beginnen. Die Nummer von Enrique Atanes lautet 363 82 67. Fertig! Die verschlüsselte Botschaft lautet: 3122308-3638267.

---------- Aufgabe 1 – Das As im Ärmel ----------

Eine Verschlüsselung macht ja nur Sinn, wenn die Botschaft wieder entschlüsselt werden kann. Dazu haben Sie sich eine *Spezialausgabe* des Zürcher Telefonbuchs erstellt. Die Spezialausgabe enthält sämtliche Einträge nach der Telefonnummer aufsteigend geordnet. Wie entschlüsseln Sie mit der Spezialausgabe die Botschaft 3122308-3638267?

--------- Aufgabe 2 – Entschlüsselung ohne Trick --------

Normalerweise besitzen Sie keine nach Nummern geordnete Spezialausgabe des Zürcher Telefonbuchs. Kann die Nachricht 3122308-3638267 auch mit dem normalen, alphabetischen Telefonbuch entschlüsselt werden? Welches Problem ergibt sich, wenn Sie so entschlüsseln?

(Wichtige Nebenbemerkung: Wir nehmen hier an, dass Sie auch keine elektronische Ausgabe des Verzeichnisses besitzen. Es ist also keine Suche mit Hilfe des Computers möglich.)

---------- Aufgabe 3 – Geheimhaltung ist alles? ----------

Folgende Situation: Sie sind der einzige Mensch, der die Spezialausgabe des Telefonbuchs besitzt. Alle anderen verfügen lediglich über die alphabetische Version. Natürlich geben Sie die Spezialausgabe an niemanden weiter.
Müssen Sie unter diesen Umständen die Verschlüsselungsmethode geheim halten? Anders gefragt: Kann zum Beispiel unser alter Bekannter Mallet etwas mit der Botschaft 3122308-3638267 anfangen, wenn er weiss, wie der ursprüngliche Text verschlüsselt wurde? Begründen Sie Ihre Meinung stichwortartig.

Public Key Kryptologie

Die Idee mit den beiden Schlüsseln

Antworten zu den Aufgaben und Weiterführung

---------- Aufgabe 1 ----------

Die erste Telefonnummer lautet: 3122308. Weil die Spezialausgabe des Telefonbuchs nach Nummern geordnet ist, kann die Nummer 3122308 problemlos und in kurzer Zeit gefunden werden. Der zugehörige Name: Christine Joly. Mit demselben Vorgehen lässt sich der Name zur zweiten Nummer, 3638267, finden: Enrique Atanes. Die Anfangsbuchstaben der Familiennamen bilden die entschlüsselte Nachricht: JA.

---------- Aufgabe 2 ----------

Natürlich kann die verschlüsselte Nachricht auch mit dem normalen, alphabetisch geordneten Telefonbuch entschlüsselt werden. Nur leider kann dann nicht systematisch vorgegangen werden. Im Gegensatz zur Spezialausgabe des Telefonbuchs muss im schlimmsten Fall jeder Eintrag danach geprüft werden, ob die zugehörige Nummer die 3122308 oder die 3638267 ist. Bei den etwa 320'000 Einträgen[1] im Telefonbuch der Stadt Zürich stellt dieses Vorgehen einen immensen Aufwand dar. Demnach ist eine Entschlüsselung auf diese Weise zwar möglich, in der Praxis aber illusorisch. Die Nachricht wäre meistens schon längst nicht mehr von Bedeutung bis sie endlich fertig entschlüsselt ist.

---------- Aufgabe 3 ----------

Die Antwort zu Aufgabe 2 zeigt: Ein Entschlüsselungsversuch macht wenig Sinn, wenn die Spezialausgabe des Telefonbuchs nicht zur Verfügung steht. Auch wenn ganz klar ist, wie man die Nachricht entschlüsseln müsste. Deshalb kann das ganze Vorgehen für Verschlüsselung und Entschlüsselung völlig gefahrlos veröffentlicht werden. Es ist egal, wer davon weiss. Sogar wer die verschlüsselte Nachricht abgefangen hat, kann nichts damit anfangen solange er oder sie nicht über die Spezialausgabe verfügt.
Damit wird klar: Das Verfahren kann öffentlich bekannt sein. Die nach Nummern geordnete Spezialausgabe des Telefonbuchs allerdings darf auf gar keinen Fall weitergegeben werden. Die Sicherheit des ganzen Systems hängt davon ab, dass die Spezialausgabe geheim bleibt!

------- Wieso der Name: *Public Key Kryptologie?*-------

In dieser Aufgabe haben Sie ein Verschlüsselungsverfahren mit einigen interessanten Eigenschaften erarbeitet:

- Das Verfahren selbst muss nicht geheim bleiben. Sie können es zum Beispiel in der Zeitung öffentlich bekannt geben.
- Die Verschlüsselung einer Botschaft ist simpel. Jedermann und jede Frau kann verschlüsseln.

[1] Diese Zahl stammt aus einer persönlichen Auskunft der Telecom Zürich vom 28. 8. 1997.

- Die Entschlüsselung ist im Grunde genommen auch simpel. Allerdings benötigt man ein weiteres Hilfsmittel. Nur so kann die Nachricht in vernünftiger Zeit entschlüsselt werden.
- Das Hilfsmittel muss unbedingt geheim bleiben. Sonst kann das ganze System nicht funktionieren.

Das Verfahren gehört zu den *Public Key Verfahren.* "Public Key" bedeutet: "Öffentlicher Schlüssel". In unserem System mit dem Telefonbuch: Jede beliebige Person kann die Botschaft mit Hilfe des Telefonbuchs verschlüsseln. Zumindest sämtliche BewohnerInnen der Stadt Zürich besitzen das richtige Telefonbuch. Alle sind in der Lage, einen Text zu verschlüsseln. Also stellt das Telefonbuch den **öffentlichen Schlüssel** dar.
Wo es etwas *Öffentliches* gibt, ist auch das Gegenteil, das *Private* zu finden. Bei allen Public Key Verfahren gibt es also zwei Schlüssel. Den **Public Key** und den **Private Key**. Wo befindet sich in unserem System der Private Key? Klar: Die Spezialausgabe des Telefonbuchs. Nur damit lässt sich die Botschaft entschlüsseln.Eine kurze Illustration. Stellen Sie sich vor: In jedem Postamt des Landes hängen Schnappschlösser von Ihnen. Alle sind identisch und mit Ihrem Namen gekennzeichnet. Eine Freundin möchte Ien einen Brief senden ohne dass ihn alle lesen können. Sie legt den Brief in ein Kästchen. Danach lässt sie sich im Postamt eines Ihrer Schlösser geben und verschliesst damit das Kästchen. Anschliessend sendet sie das Kästchen an Ihre Adresse.
Unterwegs kann nichts passieren, weil niemand den Schlüssel zum Schloss hat. Sie selbst haben natürlich einen Schlüssel. Sie können also das Kästchen öffnen und die Nachricht lesen, sobald sie eintrifft.
In diesem Szenario stellen die unzähligen Schnappschlösser den **Public Key** dar. Der einzige Schlüssel in Ihrem Besitz ist der **Private Key**.

Im Prinzip funktionieren die Public Key Verfahren in der Praxis genau gleich. Nur sind die Hintergründe dort sehr mathematisch. Die mathematische Theorie, die dahinter steckt, interessiert aber nicht so sehr. Uns geht es hier um die Idee. Deshalb zur Wiederholung nochmals die...

Eigenschaften von Public Key Verfahren

- Es gibt zwei Schlüssel: Den **Public** und den **Private Key**.
- Der **Public Key** ist öffentlich zugänglich, er muss nicht geheim bleiben. Nachrichten werden ausschliesslich mit dem Public Key verschlüsselt.
- Die verschlüsselte Nachricht kann nur mit dem **Private Key** entschlüsselt werden. Der Private Key muss unbedingt geheim bleiben.
- Die beiden Schlüssel bilden ein festes Paar. Der Private Key ist die Entsprechung zum Public Key und umgekehrt. Trotzdem ist es praktisch unmöglich, den Private Key aus dem Public Key herzuleiten. Übrigens kann auch der Public Key nicht aus dem Private Key konstruiert werden.

In der Praxis nehmen kleine Programme die ganze Arbeit ab. Sie erstellen zwei Schlüssel mit den oben genannten Eigenschaften. Es ist egal, welchen Schlüssel man zum Private Key und welchen zum Public Key macht. Verschlüsselt man mit dem einen, so macht immer der jeweils andere die Entschlüsselung möglich. Wichtig: Sobald die Wahl zwischen Private und Public Key festgelegt ist, darf nicht mehr gewechselt werden! Der Private Key muss dann geheim bleiben.

Public Key Verfahren – Etwas zum Hintergrund

Die *klassischen* oder *symmetrischen* Verfahren weisen eine negative Eigenschaft auf: Gibt man die *Ver*schlüsselungsmethode bekannt, so verrät man automatisch auch die *Ent*schlüsselungsmethode. Das muss nicht unbedingt so sein. Bei den *Public Key Verfahren* kann die Verschlüsselungsmethode problemlos weitergegeben werden. Die Idee stammt ursprünglich von Diffie und Hellman und wurde Mitte der Siebziger Jahre vorgestellt (Diffie, Hellman 1976).

Wieso funktionieren Public Key Verfahren?

Auch für alle Public Key Verfahren gilt grundsätzlich: Mit der Bekanntgabe der Verschlüsselungsmethode wird automatisch auch die Entschlüsselungsmethode verraten. Denn mathematisch gesehen sind die Funktionen zum Ver- und Entschlüsseln Umkehrfunktionen und können auseinander hergeleitet werden. Wenn aber die Herleitung des Private aus dem Public Key Hunderte von Jahren dauert, dann können wir den Public Key trotz allem gefahrlos bekannt geben.

Genau hier wird angesetzt: Es gibt sogenannte *Einwegfunktionen*. Sie verhalten sich ähnlich wie eine Einbahnstrasse. Es ist kein Problem, sie in die eine Richtung anzuwenden. Die andere Richtung allerdings ist praktisch unmöglich, weil die Berechnung einfach viel zu lange dauern würde. Es existiert jedoch eine *Hintertür* (oder englisch: *Trapdoor*). Mit Hilfe einer Zusatzinformation (der Private Key!) kann die Funktion doch in kurzer Zeit in der anderen Richtung angewendet werden.

Deshalb heissen die Public Key Verfahren auch *Einweg-* oder *asymmetrische Verfahren*.

Quellenverzeichnis

Bücher / Artikel

Diffie W., Hellman M.: New directions in cryptography. In: IEEE Transactions on Information Theory. 22 (1976), 644-654.

Salomaa A.: Public-Key Cryptography. Berlin Heidelberg 1990 (Springer).

Welsh D.: Codes and Cryptography. New York 1988 (Oxford University Press).