Eine Unterrichtsplanung zum Thema Kryptologie

Hausarbeit von Markus Heidenreich

Kaiserslautern, im Juni 1999

Inhaltsverzeichnis

1. Fachliche Klärung des Unterrichtsgegenstandes

Während man die "Kunst des geheimen Schreibens" im speziellen Kryptographie nennt, bezeichnet Kryptologie die Lehre vom Ver- und Entschlüsseln. Die verschlüsselnde Methode der Kryptologie - die Chiffrierung - hat zum Ziel, eine Nachricht geheimzuhalten sowie sicherzustellen, daß eine Nachricht unverfälscht beim Empfänger ankommt.
Hier wird schon die Unterscheidung in die zwei möglichen Angriffsarten deutlich. Der passive Angriff erfolgt durch Mitlesen einer geheimen Nachricht durch Dritte, während der aktive Angriff durch eine Verfälschung der Nachricht auf ihrem Weg zum Empfänger charakterisiert ist.
Methoden der Chiffrierung können die Verheimlichung der Existenz einer Nachricht, die Übermittlung durch einen sicheren Kanal oder eine Verschlüsselung des Klartextes in einen Geheimtext (Chiffre) sein. Da die beiden ersten Möglichkeiten durch kurzes Nachdenken als recht unsicher bezeichnet werden können, soll die dritte Variante weiterverfolgt und zu ihr immer komplexer werdende mathematische Verfahren entwickelt werden, die einen Angriff maximal erfolgreich abwehren sollen.
Natürlich soll die Verschlüsselung eines Klartextes umkehrbar sein, d.h. der Empfänger muß in der Lage sein, aus dem Chiffre wieder den Klartext erzeugen (d.h. berechnen) zu können.

Eine historisch frühe Methode - die Skytale, die in Sparta lange vor Christus eingesetzt wurde - stellt einen Zylinder mit festem Radius dar, auf den spiralförmig ein Pergamentband gewickelt wurde. Der Absender schrieb nun längs des Zylinders auf das Band die Nachricht und wickelte das Band zum Versand ab. Der Empfänger konnte die Nachricht nur mit Hilfe eines Zylinders gleichen Radius wieder lesbar machen.
Diesen Chiffriertyp nennt man Transpositionsalgorithmus. Er beruht auf Permutation der Stellen der Buchstaben. Der Schlüssel ist hier durch den Radius der Skytale gegeben.

Ein weiteres Verfahren ist von Julius Cäsar bekannt. Hier wird das zugrundeliegende Alphabet verschoben und nimmt eine buchstabenweise Ersetzung des Klartextes gemäß der entstehenden Verschiebungstabelle vor. Identifiziert man also (nach [2]) jeden Buchstaben des Alphabets mit einer Zahl, so daß $a \cong 0$, ... , $z \cong 25$, so ist die Chiffrierung gegeben durch die Funktion

$$f(i) := (i + k) \bmod 26 .$$

Die Dechiffrierung erfolgt dann analog zur Verschlüsselung. Diesen Chiffriertyp nennt man monoalphabetischen Substitutionsalgorithmus.
Der Schlüssel ist hier die Zahl k (bei Cäsar: $k = 3$).
Weitere monoalphabetische Substitutionsalgorithmen sind denkbar, indem statt einer Verschiebung eine beliebige Permutation des Alphabets vorgenommen wird. Solche Verfahren können mit Hilfe einer statistischen Analyse leicht "geknackt" werden. Man vergleicht die Häufigkeiten der Buchstaben des Chiffre mit einer Häufigkeitsstatistik für (beispielsweise deutschsprachige) Texte. Weitergehende Vergleiche, wie Bigramm- und Trigrammanalysen, also die Untersuchung der Häufigkeit von Buchstabenpaaren und Buchstabentripeln, führen letztendlich zum Ziel.

Diese symmetrischen Verfahren wurden beispielsweise durch DES (Data Encryption Standard) verbessert, wobei der Algorithmus mit der sogenannten Produktverschlüsselung arbeitet, bei der als elementare Verschlüsselung Substitutionen und Transpositionen (Permutationen) verwendet werden. Der DES-Algorithmus wurde erstmals 1974 von der US-Regierung veröffentlicht und ist als ANSI-Standard normiert. Es handelt sich um einen Blockalgorithmus, welcher 64 Bit Klartext in 64 Bit Schlüsseltext und umgekehrt überführt. Die Schlüssellänge beträgt ebenfalls 64 Bit (56 signifikante Bit und 8 Partitätsbit). DES ist heute zwar weit verbreitet, allerdings nicht mehr zeitgemäß aufgrund der geringen Schlüsselgröße von 56 Bit. Ein erweitertes DES-Verfahren namens Triple-DES (3DES) erhöht die Sicherheit des normalen DES-Verfahrens, indem die Daten mit doppelter (112 Bit) oder dreifacher (168 Bit) Schlüssellänge verschlüsselt werden. Ein ähnliches Verfahren, das erstmals 1990 veröffentlicht wurde, wird als IDEA (International Data Encryption Algorithm) bezeichnet. Es arbeitet wie DES mit 64 Bit Blöcken, benutzt allerdings einen 128 Bit Schlüssel. (nach [8])
Alle symmetrischen Verfahren bergen den großen Nachteil, daß Sender sowie Empfänger den gleichen Schlüssel benötigen. Hieraus ergibt sich das Problem, wie dieser wiederum auf sicherem Weg übermittelt werden soll. Dieser Schwierigkeit kann mit Hilfe sogenannter asymmetrischer Verfahren begegnet werden. Hierbei ist der Schlüssel zum Chiffrieren einer Nachricht frei zugänglich (public key). Den Schlüssel, mit dem der Empfänger schließlich dechiffriert, hält dieser geheim (private key). Die mathematische Grundlage eines verbreiteten asymmetrischen Verfahrens - des RSA-Algorithmus - bietet der Satz von Euler von 1761, nach dem für $n,m,k \in IN$ gilt :

$$m^{k\cdot\varphi(n)+1} \bmod n = m \quad \text{mit} \quad \varphi(n) := \left|\{t : t \in IN, t < n, ggT(t,n) = 1\}\right| .$$

Für φ gilt : $p\ prim \rightarrow \varphi(p) = p-1$, sowie : $p,q\ prim,\ p \neq q \rightarrow \varphi(p\cdot q) = (p-1)\cdot(q-1)$.
Man wählt hier zwei hinreichend große Primzahlen p und q, so daß eine Faktorisierung deren Produkt ohne die Kenntnis einer der beiden Zahlen maximal schwierig wird. In der Praxis nimmt man mindestens 100-stellige Primzahlen.
Man berechnet

$$n := p\cdot q \text{ und } z := (p-1)\cdot(q-1), \text{ also } z = \varphi(n) .$$

Wählt man nun ein $e \in \{x : \max(p,q) < x < z, ggT(z,x) = 1\}$ und berechnet dann mit Hilfe des euklidischen Algorithmus daraus ein d durch $(e\cdot d) \bmod z = 1$.
p, q, $\varphi(n)$ und d bleiben geheim. $\{n,e\}$ wird weitergegeben und als öffentlicher Schlüssel (public key) bezeichnet, während $\{n,d\}$ den geheimen Schlüssel (private key) darstellt.
Dieses Verfahren eignet sich nicht nur zum Versenden von Nachrichten, die nur der Empfänger entschlüsseln können soll - indem der Absender zum Chiffrieren den öffentlichen Schlüssel des Empfängers benutzt - so daß ein dechiffrieren nur mit Hilfe des geheimen Schlüssels des Empfängers möglich ist. Das Verfahren eignet sich auch zum Signieren eines beliebigen Dokumentes, indem der Absender seine Unterschrift mit Hilfe seines geheimen Schlüssels chiffriert. Jeder kann nun mit Hilfe des öffentlichen Schlüssels des Absenders die Unterschrift lesen und dadurch schließen, daß die Unterschrift nur mit dem geheimen Schlüssel des Absenders chiffriert sein konnte.

Eine heute stark eingesetzte Methode zur Chiffrierung vorwiegend von Emailnachrichten nennt sich PGP (Pretty Good Privacy). Es handelt sich hier nicht um ein Kryptographieverfahren oder -algorithmus, sondern um ein Programm, welches nach einem Hybridverfahren symmetrische und asymmetrische Verschlüsselungstechniken kombiniert. PGP benutzt den RSA-Algorithmus um das Public-Key-Prinzip umzusetzen, wobei jedoch nicht die gesamte Nachricht mittels RSA verschlüsselt wird. Hierfür werden wahlweise das IDEA-, das Triple-DES- und ein weiteres ähnliches Verfahren namens CAST angeboten. Lediglich der Schlüssel des gewählten symmetrischen Verfahrens wird mittels RSA bzw. dem entsprechenden öffentlichen Schlüssel des Empfängers chiffriert. (nach [8])

2. Didaktische Analyse

2.1. Begründung des Unterrichtsvorhabens

Die Entwicklung des Zusammenlebens der Menschen geht immer mehr den Weg zur Informations- und Mediengesellschaft. Nicht zuletzt aufgrund der weltweiten Vernetzung ist es uns in minutenschnelle möglich, fast alle erdenklichen Informationen zu Hause auf den Bildschirm geliefert zu bekommen.
Durch Email, sog. "Chat"-Programme und Diskussionsforen bietet sich für viele überdies die Möglichkeit nicht nur Informationen auszutauschen, sondern auch weltweit Diskussionspartner zu finden.
Es findet sich so jeder zwar in einer gewissen schützenden Anonymität, aber dennoch einer genauso gewollten, wie erschreckenden Transparenz wieder. Jeder klassifiziert in gewisser Weise Informationen, die er preisgibt etwa in öffentliche, persönliche und vertrauliche Nachrichten.
Gerade hier müssen Techniken und Methoden bereitstehen, um in dieser anonymen Transparenz Informationen, die nur für spezielle Empfänger gedacht sind vor unbefugtem Zugriff zu schützen und nur denjenigen zugänglich zu machen, die dazu berechtigt sind.
Diesen Wunsch hat nicht nur allgemein die Gesellschaft, sondern im speziellen wird die Entwicklung auf diesem Gebiet gerade von staatlichen und militärischen Einrichtungen gefordert und gefördert.
So sind häufig eingesetzte Werkzeuge die Methoden der Kryptologie, aber solange es geheime Nachrichten gibt, wird es Angreifer geben, die versuchen, sich unberechtigten Zugang zu diesen Informationen zu verschaffen. Da die ständig wachsende Leistung von EDV-Anlagen das "Knacken" von Verschlüsselungsmethoden begünstigt, muß zu immer sichereren Chiffrierverfahren übergegangen werden. Dieser Umstand macht das Thema Kryptologie für den Moment hochaktuell und auf lange Sicht zu einem zeitlosen Forschungsgebiet der Mathematik und Informatik.

Ich halte es für sinnvoll und notwendig Schüler so früh wie möglich an dieses Thema heranzuführen, so daß für sie u.a. die Probleme des Datenschutzes und der Datensicherheit erlebbar werden. Da beispielsweise die Kommunikation via Email für die meisten Schüler nicht mehr unbekannt ist und die Geheimhaltung gewisser Nachrichten hier auch im persönlichen Interesse liegt, ist davon auszugehen, daß die private Nutzung der verbreiteten Software PGP einen positiven Einfluß auf die Erlebbarkeit des Themas hat.

2.2. Klärung der Verankerung des Themas im Lehrplan und der Abdeckung fachspezifisch-allgemeiner Lernziele

Aufgrund der ständigen Aktualität des Themas Kryptologie, kann es nach dem Lehrplanentwurf von 1993 in der letzten Phase der 12. Jahrgangsstufe, die "in besonderem Maße Freiraum zur Gestaltung eines Unterrichts, der aktuelle Themen der Informatik und ihre Wechselwirkungen mit Gesellschaft und Umwelt aufgreifen soll" ([1], S.32) passend eingeordnet werden. Wie bei den Änderungen gegenüber dem bisherigen Lehrplan beschrieben, eröffnet "die Aufnahme aktueller Entwicklungen am Ende der 12. und zu Beginn der 13. Jahrgangsstufe [...] dem Kurs inhaltliche Freiräume. Sie verpflichten ihn aber andererseits, die in den letzten Jahren stärker ins Blickfeld gerückten Beziehungen zwischen Gesellschaft, Individuum und Informationstechnik zu thematisieren" ([1], S.16).

Im Lehrplanentwurf von 1993 sind folgende fachspezifisch-allgemeine Lernziele genannt, die durch das Thema Kryptologie in dieser Form abgedeckt werden :
"Fähigkeit zur Problemlösung durch Anwendung von Methoden, Werkzeugen und Standardverfahren der Informatik" ([1], S.8),
"Fähigkeit zur [...] Beurteilung von Problemlösungen, Methoden, Werkzeugen und Standardverfahren der Informatik" ([1], S.8),
"Einsicht, daß die umfassende Anwendung der Informations- und Kommunikationstechnik vielschichtige Auswirkungen auf unser Leben hat (Umwelt, Arbeitswelt, Freizeit, Wertewandel) und daß sich daraus eine besondere Verantwortung gegenüber den Menschen, der Gesellschaft und der Natur begründet" ([1], S.8).

2.3. Auswahl und Strukturierung der Inhalte und Ziele

Als Reihenfolge des allgemeinen Zugangs zum Thema Kryptologie erscheint die historische Abfolge als sinnvoll. Es ist hier wohl eine Mischung aus synthetischen und analytischen Elementen empfehlenswert, wo der Entwurf eines zunächst symmetrischen Verfahrens, der von den Schülern selbst durchgeführt werden kann, sowie die Vorstellung des Skytale- bzw. Cäsar-Chiffre den synthetischen Teil bietet. Hier kann ein Programmierteil eingeschoben werden, in dem beispielsweise das Cäsar-Verfahren implementiert werden soll. Analytisch kann dann vorgegangen werden, um die Unsicherheit dieser Verfahren mit Hilfe der in 1. angesprochenen Häufigkeitsbetrachtungen einzusehen.
Nach einer kurzen Beleuchtung anderer symmetrischer Verfahren, die größere Sicherheit bieten, wie beispielsweise DES oder IDEA kann über das, für diese Methoden typische Problem der fast unmöglichen sicheren Übermittlung des Schlüssels mit der Idee von asymmetrischen Verfahren angeknüpft werden.
Als berühmter Stellvertreter dieser Verfahren kann der RSA-Algorithmus über seine mathematische Grundlage erschlossen werden.
Im Hinblick auf die - symmetrische und asymmetrische Verfahren kombinierende - heute zur Chiffrierung von Emailnachrichten stark eingesetzte Software PGP sollen die Grundlagen, sowie die Durchführung des RSA-Algorithmus exemplarisch geübt und vertieft werden.

2.4. Fixierung der Lernziele

Folgende Lernziele sollen erreicht werden :

- **Groblernziele :**
  Die Schüler sollten

  - die Notwendigkeit der Chiffrierung einsehen,

  - die Ideen verschiedener Chiffriermethoden verstehen,

  - die Unterschiede zwischen symmetrischen und asymmetrischen Verfahren kennen,

  - die Möglichkeiten der Kombinierung von symmetrischen und asymmetrischen Verfahren erkennen und zu nutzen wissen.

- **Feinlernziele :**
  Die Schüler sollten

  - die Zielsetzung der Chiffrierung verstehen und in die Lage versetzt werden, ohne Vorbelastung ein eigenes Verfahren zu entwickeln und dieses später grob einordnen zu können,

  - das Prinzip symmetrischer Verfahren verstehen und diese anwenden können,

  - in den Verfahren den Algorithmusbegriff erkennen und in der Lage sein, ein einfaches symmetrisches Verfahren zu implementieren,

  - die Unsicherheit der vorgestellten monoalphabetischen Substitutionsverfahren mit Hilfe der Cryptanalyse erarbeiten,

  - das gemeinsame Problem aller symmetrischer Verfahren - die meist unmögliche sichere Schlüsselübermittlung - erkennen und aufgrund dessen die Idee zur Findung asymmetrischer Verfahren nachvollziehen können,

  - die mathematischen Grundlagen des RSA-Algorithmus beherrschen und diesen auf entsprechend kleine Zahlenbeispiele anwenden können,

  - die Idee des Hybridverfahrens PGP verinnerlichen und hier den Unterschied zwischen den Möglichkeiten der Chiffrierung und der Signierung erkennen und anwenden können.

2.5. Voraussetzungen und Vorkenntnisse

Bezüglich der geforderten Voraussetzungen und Vorkenntnisse kann davon ausgegangen werden, daß aus dem Bereich der Mathematik die Eigenschaften von Primzahlen, die Primzahlzerlegung (Faktorisierung) und der Begriff "relativ prim" (als nur dem Vorhandensein des trivialen größten gemeinsamen Teilers 1 zweier Zahlen) bekannt sind.
Die beiden Operationen der Ganzzahldivision (div, mod) sind vielleicht noch nicht in dieser Form bekannt, jedoch ist das Teilen mit Rest ein geübter Vorgang, so daß die Definition der Operationen keine Probleme bereiten sollte. Das einzige Problem stellt sich beim Euklidischen Algorithmus, der so wahrscheinlich noch nicht vorkam. Daher ist es sinnvoll, diesen kurz vorzustellen und anhand einiger Beispiele einzuüben.
Von seitens der Informatik kann von einem Vorwissen im Bereich der strukturierten Programmierung, also dem Umgang mit Prozeduren und Funktionen speziell in der imperativ orientierten Standardsprache Pascal ausgegangen werden.
Sachlich wäre es sinnvoll, die Schüler vorher schon mit dem Thema Internet und Dienste in diesem Netz (insbesondere Email) bekanntgemacht zu haben, da hier ein Anwendungsschwerpunkt der Methoden der Kryptologie liegt. Es ist allerdings auch möglich die Verschlüsselung zunächst auf Dateiebene zu betreiben und später in einem Themengebiet Internet einen Rückgriff auf die Kryptologie vorzunehmen.

2.6. Lernkontexte

Als Rahmen der Kryptologie bietet sich für den Einstieg die Übermittlung schriftlicher Nachrichten in Papierform an, wobei später auf die elektronische Form der Nachrichtenübermittlung übergegangen werden kann, was bei richtiger Präsentation bei Schülern sicherlich auf reges Interesse trifft.

2.7. Literatur

Für eine 4-6-stündige Unterrichtseinheit halte ich es nicht für sinnvoll ein eigenes Buch anzuschaffen. Entweder ist das Thema Kryptologie in einem allgemeinen Buch zum Informatikunterricht, das länger benutzt werden kann vorhanden oder die Informationen werden auf anderen Wegen, wie Kopien und Tafelbilder in schriftlicher Form vorliegend und für die Schüler nachlesbar gemacht.

3. Methodische Bemerkungen

Wie schon in 2.3 beschrieben, sollen die analytische und synthetische Art des Zugangs vermischt werden. Zunächst soll die allgemeine Problemstellung der geheimen Nachrichtenübermittlung beschrieben und dadurch eine Motivation gegeben werden, so daß Schülerideen zur Realisierung von Verschlüsselungsmethoden gesammelt werden können. Es bietet sich an, zunächst ein Unterrichtsgespräch mit den Schülern über dieses Thema zu beginnen, um u.a. die Notwendigkeit kryptologischer Anwendung zu klären und später die Schüler in Gruppen je ein eigenes Chiffrierverfahren "erfinden" zu lassen.
Eine Diskussion über die gefundenen Lösungsansätze finde ich unmittelbar im Anschluß am besten platziert, da es so möglich ist, die gewonnenen, noch frischen Erkenntnisse maximal erfolgreich zu sichern.
Als Vertiefung kann zur Hausaufgabe die Verschlüsselung verschiedener (entsprechend kurzer) Textstücke mit Hilfe des eigenen Verfahrens gegeben werden.

Im nächsten Schritt wird das Arbeitsblatt eingesammelt und aufgetretene Probleme bei der Bearbeitung besprochen.
Anschließend können den Schülern in Form eines Lehrvortrags historische Verfahren, wie die Skytale, das Cäsar-Verfahren und die allgemeine Permutation mit Hilfe kurzer Vorstellung und Ausführung von Beispielen nähergebracht werden.
Nachdem sich diese Verfahren nicht sehr komplex darstellen, kann unmittelbar im Anschluß mit dem 2. Arbeitsblatt, das die Programmierung des (verallgemeinerten) Cäsarverfahrens beinhaltet zur Sicherung des Stoffs begonnen werden.
So können Probleme direkt geklärt und die begonnene Aufgabe als Vertiefung ggf. als Hausaufgabe fertiggestellt werden. Außerdem sollen sich die Schüler im Hinblick auf den nächsten Schritt überlegen, wie Substitutionsverfahren (beispielsweise Cäsar) "geknackt" werden können.

Aus der Motivation, diese symmetrischen Verfahren so sicher als möglich gegen Angriffe zu entwerfen, soll zunächst eine Ideensammlung zum "Knacken" des verallgemeinerten Cäsar-Chiffre (mit nicht notwendig $k = 3$) später der allgemeinen Substitutionsverfahren erstellt werden, um einige Ideen praktisch zu erproben. Ist dadurch die Erkenntnis der Unsicherheit dieser Verfahren erreicht, so werden symmetrische Verfahren aus der heutigen Zeit, wie DES und IDEA vorgestellt.
Zur Vertiefung und dem besseren Verständnis können unmittelbar im Anschluß diese neu eingeführten Verfahren praktisch angewandt werden.

Im nachfolgenden Schritt ist es sinnvoll zum vorläufigen Abschluß der symmetrischen Verfahren diese kurz zu wiederholen, um über das gemeinsame anwendungsorientierte Problem dieser Methoden - einen sicheren Kanal zum Austausch des Schlüssels unter den Kommunikationspartnern zu finden - zur Idee der asymmetrischen Verfahren zu gelangen.
Falls bei den Schülern der Euklidische Algorithmus noch nicht bekannt sein sollte, kann er hier ausführlich erarbeitet und geübt werden. In diesem Fall ist es möglich, den 4. Schritt auf 2 Stunden aufzuteilen. Andernfalls genügt eine Wiederholung des Algorithmus innerhalb der Vorstellung des RSA-Verfahrens.

Die Sicherung des Stoffs erfolgt durch Rechnen mehrerer Beispiele des RSA-Algorithmus (Ver- sowie Entschlüsselung) mit relativ kleinen Zahlen.
Zur vertiefenden Hausaufgabe soll das Cäsar-Verfahren nur kurz, allerdings die mathematische Grundlage und die Anwendung des RSA-Algorithmus ausführlich wiederholt werden.

Im letzten Schritt sollen Unklarheiten, die bei der Wiederholung des RSA-Verfahrens aufgetreten sind kurz besprochen werden, so daß in der anschließenden Hausaufgabenüberprüfung (siehe S.15) bezüglich Aufgabe 2 keine Überraschungen zu erwarten sind.
Um danach zum heutigen Einsatz kryptologischer Verfahren zu gelangen, soll die Möglichkeit der Kombinierung symmetrischer Verfahren und des RSA-Algorithmus herausgearbeitet werden. Hier kann das Prinzip der digitalen Unterschrift, d.h. des Signierens einer Nachricht mit Hilfe des geheimen Schlüssels des Senders eingestreut werden.
Das exemplarische Durchrechnen eines Zahlenbeispiels zu einem solchen Hybridverfahren soll die erarbeitete Idee festigen und sichern.
Vertiefend kann hier zunächst ein geführter, dann aber selbständiger Umgang mit der Software PGP die Unterrichtsreihe abschließen.

4. Skizze des Unterrichtsverlaufs

Hier soll der in 3. ausführlich beschriebene methodische Aufbau der Unterrichtseinheit in tabellarischer Form den Schritten und deren einzelnen Phasen zugeordnet werden, sowie die gewählten Sozialformen und eingesetzten Medien genannt werden.

1. Schritt :

Phase	Inhalt	Sozialform	Medien
Motivation	Allgemeine Einführung in das Thema, Motivation	UG	T
Erarbeitung	Erarbeitung eines eigenen Verschlüsselungsverfahrens	GA	
Sicherung	Besprechung der gefundenen Schülerlösungen	SV+D	T
Vertiefung	Hausaufgabe : Verschlüsselung eines kurzen Textstücks (Arbeitsblatt 1)	EA	

2. Schritt :

Phase	Inhalt	Sozialform	Medien
Wiederholung	Einsammeln von Arbeitsblatt 1 und Besprechung aufgetretener Probleme	UG	
Motivation	Kennenlernen historischer Verfahren (Skytale, Cäsar, allg. Permutationen)		
Erarbeitung	Vorstellung der historischen Verfahren Skytale, Cäsar, allg. Permutationen	LV	T/F (s.S.14)
Sicherung	Beginnen mit Arbeitsblatt 2 : Programmieren des (verallgemeinerten) Cäsar-Verfahrens	GA/EA	C
Vertiefung	Hausaufgabe : Beenden der Programmieraufgabe, Überlegungen zum "Knacken" des Cäsar-Verfahrens	EA	

3. Schritt :

Phase	Inhalt	Sozialform	Medien
Motivation	"Knacken" des Cäsar-Verfahrens mit dem Ziel des Übergangs zu sichereren Verfahren	UG	
Erarbeitung	Sammeln der Schülerideen zum Erkennen der Unsicherheit solcher Substitutionsverfahren	UG	T
Sicherung	Praktische Beispiele zum "Knacken" von einfachen Substitutionsverfahren	GA/EV	ggf. T
Erarbeitung	Vorstellung ausgewählter symmetrischer Verfahren aus der heutigen Zeit (DES, IDEA, ...)	LV	T/F
Vertiefung	Praktisches Beispiel zur Verschlüsselung mit Hilfe des DES-Verfahrens	LV/UG	T

4. Schritt :

Phase	Inhalt	Sozialform	Medien
Wiederholung	Kennengelernte symmetrische Verfahren	UG/SV	T
Motivation	Wie findet eine sichere Übermittlung des Schlüssels statt ?		F (s.S.15)
Erarbeitung	Idee der asymmetrischen Verfahren des unterschiedlichen Schlüssels für Sender und Empfänger	LV/UG	F (s.S.15)
Erarbeitung	Unterrichtung der mathematischen Grundlagen des RSA-Algorithmus (ggf. muß hier der Euklidische Algorithmus neu eingeführt werden)	LV	T/F
Sicherung	Durchrechnen einiger Beispiele des RSA-Algorithmus mit kleinen Zahlen	LV/GA/EA	T
Vertiefung	Hausaufgabe : Kurze Wiederholung des Cäsar-Verfahrens und Wiederholung der mathematischen Grundlagen und Zahlenbeispiele zum RSA-Algorithmus	EA/GA	

5. Schritt :

Phase	Inhalt	Sozialform	Medien
Wiederholung	Besprechung von Unklarheiten bzgl RSA-Algorithmus	UG	T
Wiederholung	Hausaufgabenüberprüfung (siehe S.15) mit anschießender Besprechung		
Erarbeitung	Nicht nur Möglichkeit der Verschlüsselung, sondern auch des "unterschreibens" von Nachrichten.	LV/UG	T/F (s.S.16)
Erarbeitung	Möglichkeit der Kombinierung, indem die Nachricht zunächst mit Hilfe eines symmetrischen Verfahrens chiffriert wird. Der hier benutzte Schlüssel wird mit Hilfe des RSA-Algortihmus verarbeitet und so verschlüsselt übermittelt.	LV/UG	T/F (s.S.16)
Sicherung	Exemplarisches Durchrechnen eines Beispiels zu diesem Hybridverfahren.	SV/UG	T
Vertiefung	Zunächst leicht geführter dann selbständiger Umgang mit der Software PGP	GA/EA	C

Folgende Abkürzungen wurden verwendet :

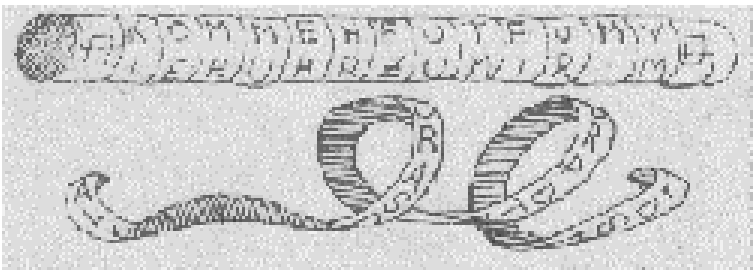
UG Unterrichtsgespräch
LV Lehrvortrag
SV Schülervortrag
GA Gruppenarbeit
EA Einzelarbeit
D Diskussion
T Tafel
F Folien
C Computer

Folie 1

2 historische Verfahren :

Die Skytale von Sparta :

- Zylinder mit festem Radius,
- spiralförmig aufgewickeltes Pergamentband,



- lesen der Nachricht fast nur möglich mit Zylinder gleichen Radius,
  $\Rightarrow$ Schüssel ist der Radius
- Typ : Transpositionsalgorithmus (Permutation der Stellen der Buchstaben).

Der (verallgemeinerte) Cäsar-Chiffre :

- das zugrundeliegende Alphabet wird um eine bestimmte Anzahl an Stellen verschoben bzw. beliebig "permutiert",
- es ist entweder die Verschiebungsanzahl bzw. eine Ersetzungstabelle anzugeben : beispielsweise

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

- der Schüssel ist die Verschiebungsanzahl bzw. die Ersetzungstabelle,
- Typ : monoalphabetischer Substitutionsalgorithmus.

Folie 2

Symmetrische und asymmetrische Verfahren :

Symmetrische Verfahren :

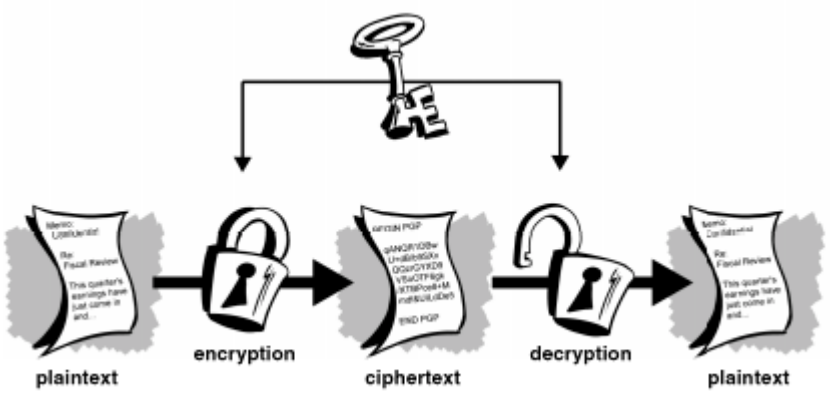


Abbildung aus [3]

- Zur Chiffrierung sowie zur Dechiffrierung wird der gleiche Schlüssel benötigt
  ⇒ Problem : Wie soll dieser Schlüssel sicher übermittelt werden ?

Asymmetrische Verfahren :

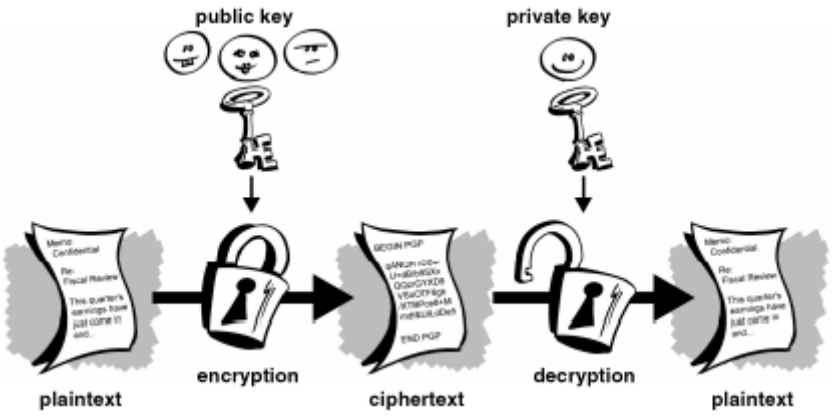


Abbildung aus [3]

- Zur Chiffrierung bzw. zur Dechiffrierung werden unterschiedliche Schlüssel verwendet.

Folie 3

PGP als Hybridverfahren :

Die Verschlüsselung :

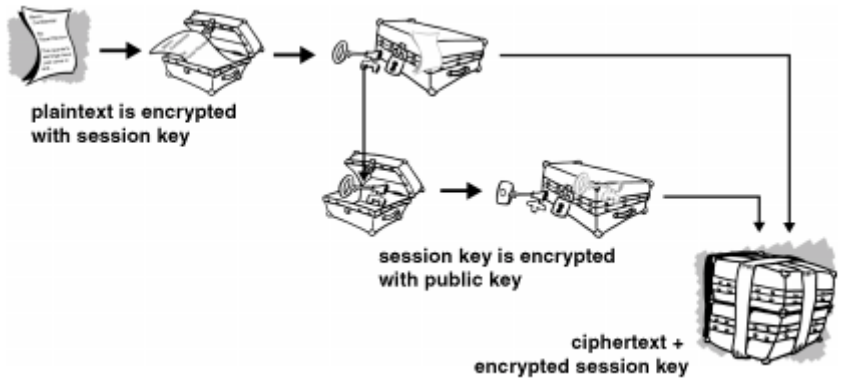


Abbildung aus [3]

Die Entschlüsselung :

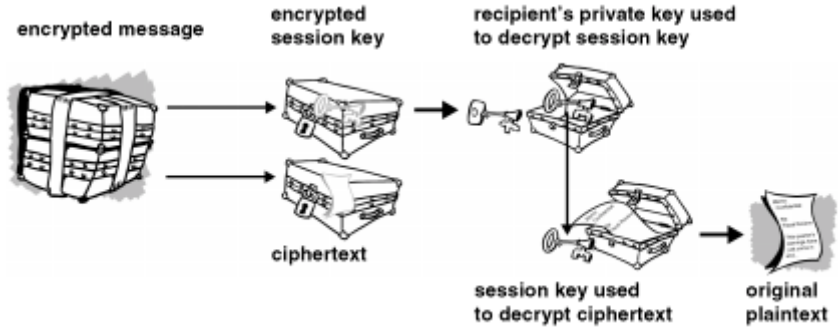


Abbildung aus [3]

Die digitale Unterschrift :

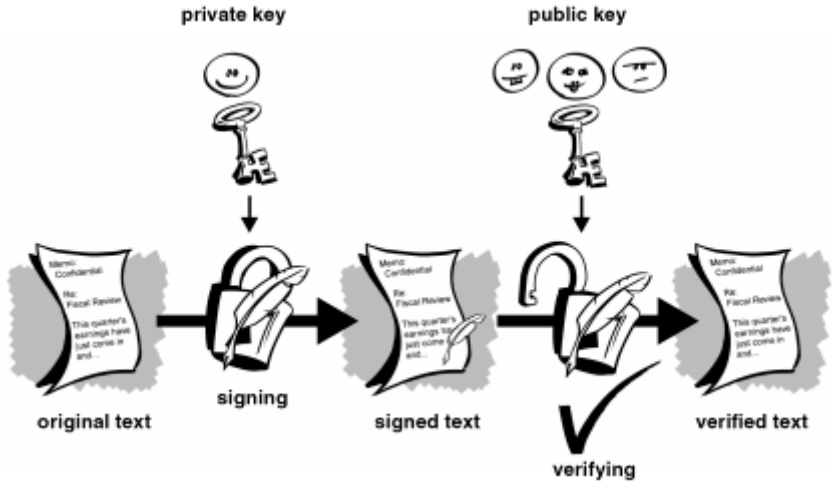


Abbildung aus [3]

Arbeitsblatt 1

Bearbeiten Sie die Aufgaben einzeln, nicht in der Gruppe ! Sprechen Sie sich bei Aufgabe 2. ab, daß jedes Textstück nur einmal pro Gruppe bearbeitet wird !

1. Beschreiben Sie das in Ihrer Gruppe entwickelte Verschlüsselungsverfahren in kurzen Worten. Geben Sie dazu jeweils den Algorithmus zur Chiffrierung sowie zur Dechiffrierung an (wenn möglich auch in "mathematischer Form").

2. Verschlüsseln Sie eines der folgenden Textstücke mit Hilfe Ihres Verfahrens. Prüfen Sie durch Entschlüsselung des entstandenen Chiffre, ob sich Ihr Verfahren zur Nachrichtenübermittlung eignet.
   (Bearbeiten Sie innerhalb einer Gruppe keine gleichen Textstücke)

   a. INFORMATIKUNTERRICHT MACHT MIR SEHR VIEL SPASS
   b. FRANZ JAGT IM KOMPLETT VERWAHRLOSTEN TAXI QUER DURCH BAYERN
   c. UNSER KATER MAX SCHLAEFT JEDE NACHT IN UNSEREM BETT
   d. DIESER TEXT WURDE CHIFFRIERT UND IST NUN WIEDER LESBAR

3. Welche der folgenden Aussagen treffen für Ihr Verfahren zu ?

   ☐ Durch alleinige Angabe des Verfahrens und des Schlüssels für die Chiffrierung ist klar, auf welche Weise entschlüsselt werden muß, um den gleichen Klartext wieder zu erhalten.

   ☐ Für Klartext und Chiffre liegt das gleiche Alphabet zugrunde.

   ☐ Bei jedem Verschlüsselungsvorgang bleibt die Anzahl der Zeichen gleich.

Arbeitsblatt 2

Vervollständigen Sie folgendes Programmfragment um die procedure chiffrieren;

```
program Caesar;
uses crt;
var  k,c       : string;  {Klartext, Chiffre}
     loop      : char;    {Nochmal ?}
     v         : integer; {Verschiebungslänge}
     knr, cnr  : integer; {Zeichennummer des Klartext- bzw.}
                          {Chiffrezeichens}

{------------------------------------------------------------------------}

procedure initialisieren;
 begin
  clrscr;
  writeln('Dieses Programm dient zur (De-)Chiffrierung eines eingegebenen');
  writeln('Textes nach dem Cäsar-Verfahren um die eingegebene');
  writeln('Verschiebungslänge.');
  writeln('Es werden nur Gross- und Kleinbuchstaben von A-Z bzw. a-z');
  writeln('(de-)chiffriert. Sonderzeichen und Umlaute werden');
  writeln('zu einem "?" verarbeitet, Leerzeichen bleiben gleich !');
  writeln('Die Art der Chiffierung nennt man');
  writeln('monoalphabetischen Substitutionsalgorithmus.');
  writeln;
 end; {initialisieren}

{------------------------------------------------------------------------}

procedure einlesen;
 begin
  write('Klartext : ');
  readln(k);
  write('Verschiebungslänge : ');
  readln(v);
  writeln;
 end; {einlesen}

{------------------------------------------------------------------------}

procedure chiffrieren;
 begin
 end; {chiffrieren}

{------------------------------------------------------------------------}

procedure ausgeben;
 begin
  writeln('Chiffre : ',c);
 end; {ausgeben}

{------------------------------------------------------------------------}

begin {main}
 repeat
  initialisieren;
  einlesen;
  chiffrieren;
  ausgeben;
  writeln;
  write('Nochmal (J/N) ? ');
  loop := readkey;
 until UpCase(loop) = 'N';
end. {main}

{------------------------------------------------------------------------}
```

Musterlösung zu Arbeitsblatt 2 :

```
1. Variante ("if") :

procedure chiffrieren;
var i : integer; {Schleifenlaufvariable}
 begin
   c := '';
   for i:=1 to length(k) do
     begin
       if ((ord(k[i]) >= 65) and (ord(k[i]) <= 90)) then
         begin
           knr := ord(k[i]) - 65;
           cnr := (knr + v) mod 26;
           c := c + chr(cnr + 65);
         end {then}
       else
         begin
           if ((ord(k[i]) >= 97) and (ord(k[i]) <= 122)) then
             begin
               knr := ord(k[i]) - 97;
               cnr := (knr + v) mod 26;
               c := c + chr(cnr + 97);
             end {then}
            else
             begin
               if (ord(k[i]) = 32) then
                 begin
                   c := c + chr(32);
                 end {then}
                else
                 begin
                   c := c + chr(63);
                 end; {else}
             end; {else}
         end; {else}
     end; {for}
 end; {chiffrieren}

{-------------------------------------------------------------------------}

2. Variante ("case") :

procedure chiffrieren;
var i : integer; {Schleifenlaufvariable}
 begin
   c := '';
   for i:=1 to length(k) do
     begin
       case ord(k[i]) of

          65..90  : begin
                      knr := ord(k[i]) - 65;
                      cnr := (knr + v) mod 26;
                      c := c + chr(cnr + 65);
                    end;

          97..122 : begin
                      knr := ord(k[i]) - 97;
                      cnr := (knr + v) mod 26;
                      c := c + chr(cnr + 97);
                    end;

          32      : c := c + chr(32);

          else      c := c + chr(63);

       end; {case}
    end; {for}
 end; {chiffrieren}

{-------------------------------------------------------------------------}
```

Hausaufgabenüberprüfung in Informatik

Zum Thema Kryptologie

1. a. Beschreiben Sie mit kurzen Worten das Chiffrierverfahren, das von Julius Cäsar verwendet wurde und durch ihn bekannt ist.

1. b. **Ent**schlüsseln Sie folgendes Textstück mit Hilfe dieses Verfahrens.
(Hinweis : Der Klartext ist ein sinnvolles Wort !)

N U B S W R J U D S K L H

1. c. Weshalb nennt man dieses Verfahren symmetrisch ?

2. a. Nennen Sie den für das RSA-Verfahren grundlegenden Satz von Euler.
Benennen Sie darüber hinaus beide Eigenschaften, welche wir für die φ-Funktion im Bezug auf Primzahlen kennengelernt haben.

2. b. Berechnen Sie zunächst für $p = 13$, $q = 17$ und $e = 5$ die Zahl d gemäß des RSA-Algorithmus und wenden Sie dann dieses Verfahren auf den Klartext $m = 5$ an. (Hinweis : Das Ergebnis ist 31, der Rechenweg ist wichtig.)

6. Quellenangaben

[1] Lehrplanentwurf Informatik, Rheinland-Pfalz von 1993.

[2] Thomas Beth, Peter Heß, Klaus Wirl. Kryptographie. B.G. Teubner. Stuttgart 1983.

[3] Network Associates, Inc. and its Affiliated Companies. An Introduction to Cryptography

[4] SSH Communications Security, Inc. (http://www.ssh.fi/tech/crypto)

[5] Deutsche Telekom AG (http://www.telekom.de/angebot/telesec)

[6] Bundesministerium für Wirtschaft und Technologie (http://www.bmwi.de)

[7] Axel Wagner, Lehrer u.a. für Informatik am Saarpfalz-Gymnasium, Homburg. (http://www.hom.saar.de/~awa)

[8] Security-Server der Universität Siegen (http://www.uni-siegen.de/security)