Kryptographische Verfahren in der griechischen und römischen Antike

Seminararbeit zum Modul Kryptographie (Claus Diem)

Tim Niehoff

12.06.2017

Inhaltsverzeichnis

1 Einleitung

Es ist bekannt, dass der Mathematik in der griechischen Antike eine große Bedeutung zugetragen wurde, wie Errungenschaften etwa von Pythagoras, Thales, Aristoteles, Euklid und Diophantos von Alexandria zeigen. Die antiken Römer bauten auf diesem mathematischen Verständnis auf, beschäftigten sich hingegen mehr mit praktischen Anwendungen etwa in den Vermessungs- und Ingenieurwesen. Das passt gut in das Bild als bedeutendste Herrschaftsmacht zu der Zeit.
Betrachtet man nun die Geschichte der Kryptographie bis in das 20. Jahrhundert, so entsteht schnell der Eindruck, dass diese mathematische Disziplin vor allem für militärische Zwecke benutzt wurde. Von diesem Standpunkt aus ist die These nicht weit hergeholt, dass das Voranbringen der Kryptographie vor allem in der römischen Antike eine große Daseinsberechtigung gehabt hat und dies mithilfe einer bedeutenden Anzahl an kryptographischen Überlieferungen leicht zu belegen ist.
Die Auseinandersetzung mit dieser These ist Gegenstand der vorliegenden Ausarbeitung. Hierbei wird der zu betrachtende Zeitraum auf die griechischen und römischen Antike von 500 v. Chr. bis 284 n. Chr. festgelegt.
Als Ausgangspunkt der Recherche werden die Geschichtskapitel bestehender kryptographischer Literatur[1] konsultiert, um anschließend selbst die aus der Antike überlieferten Quellen zu studieren. Zum Teil wurden hierfür bestehende Übersetzungen aus dem Griechischen oder Lateinischen verwendet, teilweise aber auch selbst aus lateinischen Quellen übersetzt.
Die Ergebnisse der Recherche werden im folgenden Kapitel präsentiert und an passenden Stellen mit Bemerkungen aus der Literatur ergänzt.
Das Kapitel Fazit schließt mit einer Zusammenfassung der Ergebnisse und einer Bewertung der Bedeutung der Antike für die Kryptographie ab.

[1] [Schmeh 2008, 1-3], [Kahn 1974, 70-73], [Bauer 2013, 3-6], [D'agapeyeff 2016], [Hebisch 2017], [Reinke 1962]

2 Kryptographische Verfahren

2.1 Taktikos' Vokalsubstitution

Aineias Taktikos (geboren ca. 350 v. Chr.) berichtet in seinem Werk *Poliorketika* von Handlungsanweisungen, die Bürgern dabei helfen sollen, eine Belagerung ihrer Stadt zu überstehen (vgl. [Tacticus 2017, 33]). Ein Kapitel wird der Geheimhaltung gewidmet und bietet zahlreiche, überlieferte Methoden der Steganographie. Zudem schreibt Taktikos von einem Verschlüsselungsverfahren in Form einer monoalphabetischen Substitution: Hierbei werden ausschließlich alle Vokale des Alphabets durch Punkte kodiert. Vom Standpunkt des modernen, lateinischen Schriftsystem werden so die Vokale entsprechend der Reihenfolge ihrer Vorkommen im Alphabet verschlüsselt:

A	E	I	O	U
.	:	:.	::	::.

Demzufolge entsteht aus dem Klartext mit überwiegendem Konsonanten-Anteil „H I L F E N A H T“ die Geheimschrift
„H :. L F : N . H T“.

2.2 Skytale

Die Gestalt, Verbreitung und Funktion der Skytale sind bis dato nicht eindeutig geklärt. Allgemein akzeptiert ist das Bild der Skytale als Schreibstab, um das Material gewickelt wurde und auf dem schließlich geschrieben wurde.
Apollonios von Rhodos (295 - 215 v. Chr.) könnte erstmals in seinem Werk *On Archilochus* der Skytale die Geheimhaltung von Nachrichten zugeschrieben haben. Seine Texte sind jedoch nicht überliefert; dennoch verweist Athenaeus auf ihn

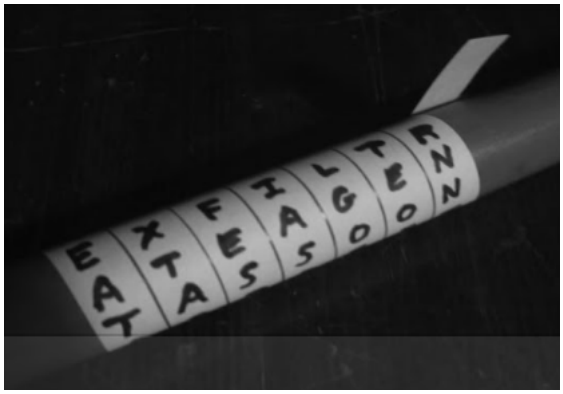

Abbildung 1: Schaubild einer Skytale. Bildquelle: (Bauer 2013, 4)

in einem Kapitel über Rätsel aus *Deipnosophistae* mehrere Jahrhunderte später: Demnach haben die Spartaner ihre Nachrichten auf einen weißen Streifen geschrieben, welches um einen Schreibstab (Skytale) gewickelt wurde. Weiterhin sei dies ausreichend von Apollonius von Rhodos in seiner Abhandlung *On Archilochus* erklärt (vgl. [Athenaeus 1854, 10.451d]).

Sowohl der Grieche Plutarch (50-120 n. Chr.) als auch der Römer Gellius (ca. 130-180 n. Chr.) liefern genauere Beschreibungen für die Skytale als kryptographisches Verfahren. Ihre Beschreibungen ähneln sich: Es ist sehr wahrscheinlich, dass Gellius entweder sich direkt auf Plutarch bezieht, oder er die gleiche(n) Quelle(n) wie Plutarch benutzte.

In *Lysander* aus den Parallelbiographien beschreibt Plutarch die Skytale wie folgt (für den folgenden Abschnitt vgl. [Plutarch 2000, LCL 80: 444f]):

Für die zwei Personen, die sich geheim unterhalten möchten, werden zwei Skytalen in Form von Holzstücken vorbereitet. Diese müssen gleich lang und dick sein. Sobald jemand eine geheime Nachricht an die andere Person schicken möchte, wickelte dieser eine lange und schmale Rolle wie etwa einen Lederriemen um die Skytale, bis diese lückenlos von der Rolle bedeckt war. Danach wird die zu überbringende Nachricht über die verschiedenen Spuren der Rolle hinweg geschrieben.

Anschließend wird die Nachricht ohne die Skytale verschickt.

Da die Zeichen der Botschaft nun transponiert sind, ist sie auch erst dann wieder lesbar, wenn der Empfänger die Geheimschrift auf seine Skytale aufrollt. Abbildung 1 veranschaulicht die Intention von Gellius.

Thomas Kelly, einstiger Professor für Griechische Geschichte an der Universität Minnesota, bezweifelt in seinem Artikel *The Myth of Skytale*, dass die Skytale zur Überbringung geheim zu haltender Nachrichten verwendet wurde (vgl. [Kelly 1998, 244-260]). Ein Hauptargument von Kelly ist, dass ihr Zweck der Geheimhaltung von Nachrichten in zu wenigen Quellen festgehalten wurde.

2.3 Polybios Chiffre

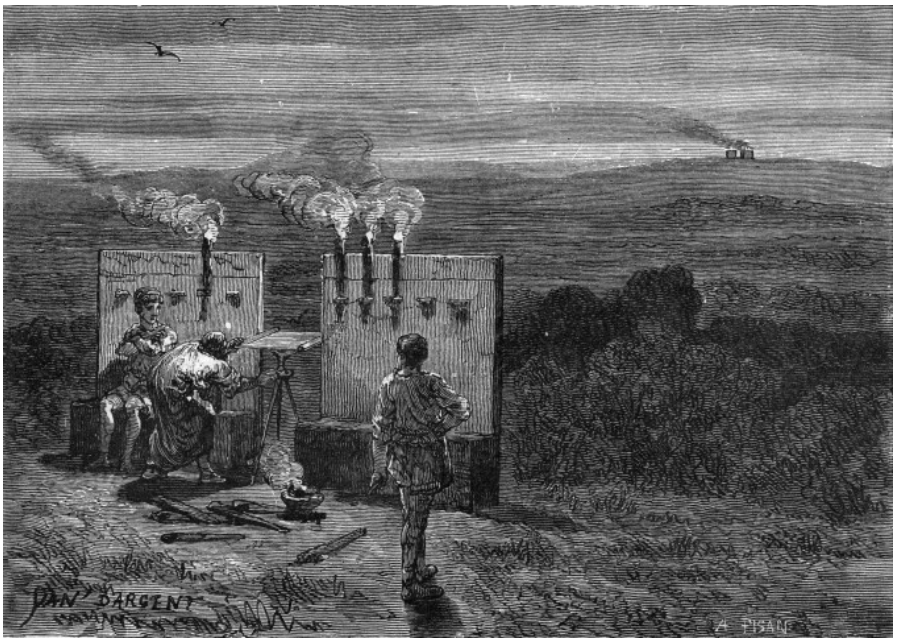

Abbildung 2: Schaubild zum ursprünglichen Zweck des Polybios-Chiffres. Bildquelle: http://newsfeed.time.com/2013/03/13/

Polybios (ca. 200 - 120 v. Chr.) beschreibt als griechischer Geschichtsschreiber in seinem Hauptwerk *Historiai* unter anderem ein optischen Telegraphieverfahren. Hierbei werden mit Feuerzeichen beliebige Mitteilungen ausgetauscht, d.h. ohne dass Sender und Empfänger sich vorher auf diese verständigt haben (vgl. [Polybius 1993, 45])[2]. Der ursprüngliche Zweck bestand also in der Kommunikation über weite Entfernungen und nicht zur Geheimhaltung von Nachrichten.
Polybios berichtet, dass das Verfahren von Cleoxenus und Democleitus entworfen wurden ist, er es jedoch verbessert habe (vgl. [Polybius 1993, 10, 45, 6]). Ihm zu

[2]Das ist erwähnenswert, weil bis dato Quellen nur überliefern, dass die Telegraphieverfahren zuvor insofern beschränkt waren, dass die zu sendenden Botschaften vor Anwendung feststehen mussten.

Ehren wird das Verfahren als *Polybios-Chiffre* bezeichnet. Es lässt sich bis in das 20. Jahrhundert hinein als Teil kryptographischer Verfahren wiederfinden, wie etwa in der *Bifif-Chiffre*, dem *ADFGVX-Chiffre* und in der *Nihilisten-Transposition* (vgl. [Kondo/Mselle 2013, 33]).

Das *Polybios-Chiffre* ist ein Substitutionsverfahren, welches für den ursprünglichen Zweck wie folgt gedacht war (vgl. [Polybius 1993, 10, 45 - 46]).

Zunächst müssen einige Vorbereitungen für jeweils beide Kommunikationsteilnehmer getroffen werden: Das Alphabet wird in fünf möglichst gleich große Teile zerlegt. Da das griechische Alphabet aus 24 Buchstaben besteht, setzt sich der fünfte Teil nur aus 4 Buchstaben zusammen. Das moderne lateinische Alphabet bietet hingegen zwei Buchstaben mehr. Deshalb müssen zwei Buchstaben durch einen zusammengefasst werden, wie etwa das I und J in der Abbildung 3. Hierbei repräsentiert eine Zeile jeweils eine Tafel und die Spalte die Position eines Buchstabens auf einer Tafel.

Nun wird auf fünf Tafeln jeweils eine der Alphabetfragmente geschrieben. Außerdem stellen die Kommunikationsteilnehmer links und rechts von sich jeweils eine Leinwand auf, die jeweils drei Meter lang und so hoch wie ein Mensch ist. Für jede Leinwand werden fünf Fackeln benötigt. Die Anzahl der Fackeln auf der linken Leinwand repräsentieren, die wievielte Tafel konsultiert werden soll und die auf der rechten Leinwand bestimmen den genauen Buchstaben der Tafel. Zwischen beiden Leinwände werden die Tafeln direkt neben einem Diopter[3] positioniert. Abbildung 2 skizziert sowohl die Vorbereitungen als auch den Ablauf.

Derjenige, der mit dem Senden einer Nachricht beginnt, hebt zwei Fackeln und wartet darauf, bis der andere das Gleiche wiederholt. Dadurch geben sie sich ge-

[3]Das fehlende Instrument mit optischer Vergrößerung wie etwa durch Linsen bei einer sehr großen Entfernung gibt Anlass zur Spekulation, dass das als Polybios Chiffre bezeichnete Verfahren aus einem anderen Jahrhundert stammt.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Abbildung 3: Polybios-Chiffre in Form einer Matrix.

genseitig zu verstehen, dass sie zur Konversation bereit sind. Möchte der Sender nun beispielsweise die Nachricht versenden, dass hundert Soldaten zu den Feinden übergelaufen sind, fasst er sie so kurz wie möglich zusammen, wie z.B. durch „Hundert Deserteure“. Nun wird Buchstabe für Buchstabe wie folgt kodiert gesendet: Der erste Buchstabe *H* steht auf der zweiten Tafel (siehe Abbildung 3). Deshalb zündet der Sender zwei Fackeln auf der linken Leinwand an. Weil *H* auf der zweiten Tafel an dritter Position steht, werden entsprechend drei Fackeln auf der rechten Leinwand angezündet. Der Empfänger kann nun mithilfe seines Teleskops zusammengefasst die Information „23“ erkennen und daraus den Buchstaben *H* folgern. Für die folgenden Buchstaben der Nachricht wird das Prozedere wiederholt.

2.4 Caesar Chiffre

Suetonius Tranquillus schreibt ca. 112 n. Chr. in *De Vita Caesarum* über zwölf Biographien römischer Alleinherrscher. In der Biographie über Caesar (100 v. Chr. - 44 v. Chr.) heißt es (vgl. [Tranquillus 1962, 56, 6], Übers. d. Verf.):

> „Sie [Briefe von Caesar] bestehen auch an Cicero, ebenfalls an Vertraute von häuslichen Angelegenheiten, bei denen er sie, falls sie irgendwie geheim zu überbringen waren, mithilfe einer Chiffre dargestellt hat, das heißt: so die Reihenfolge der Buchstaben gebaut, dass keiner imstande ist, ein Wort zu folgern. Falls jemand sie untersuchen und forschen will, so tausche er den vierten Buchstaben des Alphabets, das heißt D für A und auf die gleiche Weise die Übrigen aus."

Die Verwendung des gleichen Verfahren mit anderem Schlüssel schreibt Tranquillus dem Kaiser Augustus (63 v. Chr. - 14 n. Chr.) zu (vgl. [Tranquillus 1982, 88, 1], Übers. d. Verf.):

> „Jedes mal, wenn er jedoch mithilfe einer Chiffre schreibt, setzt er B für A, C für B, sowie die folgenden Buchstaben nacheinander auf dieselbe Art und Weise, jedoch für X ein doppeltes A."

Tranquillus' Schriften können den Eindruck erwecken, dass die Anwender der Chiffre es bei einem festen Schlüssel beließen; Caesar verwendete somit stets den Schlüssel *3* und Augustus den Schlüssel *1*.
In Gellius (ca. 130 - 180 n. Chr.) Hauptwerk *Nodes Aetticae* findet sich ein Hinweis dafür, dass Caesar auch verschiedene Schlüssel benutzt haben könnte ([Gellius 1927, 17, 9, 4], Übers. C. Diem und d. Verf.):

> „Welcher Buchstabe denn aber für einen geschrieben wird, gefiel es vorher diesen, wie ich gesagt habe, welche dieses Schreibversteck vorbereiteten."

2.5 Sprache als Chiffre

Eine Sprache als Chiffre zu benutzen, die die Angreifer vermutlich nicht sprechen und so die Nachricht geheim halten zu können, könnte bereits von Caesar überliefert worden sein (vgl. [Caesar 1859, 5,48,3 - 5,48,4]).
Im fünften Kriegsjahr (54 v. Chr.) gegen die Navier befahl er einem gallischen Reiter, eine Nachricht an den Legaten Quintus Tullius Cicero, den Bruder des berühmten Schriftstellers und Redners Marcus Tullius, zukommen zu lassen. Weiterhin heißt es (vgl. [Caesar 1859, 5,48,4], Übers. C. Diem):

> Er schickte diesen Brief mit griechischen Buchstaben, damit nicht, wenn unser Brief vom Feind abgefangen wird, der Plan bekannt werde.

Es ist ungeklärt, ob Caesar damit gemeint hat, schlicht die lateinischen Zeichen durch Griechische auszutauschen. Dies wäre jedoch nicht besonders sicher, zumal Caesar selbst davon berichtet, dass die Druiden der Gallier (vgl. [Caesar 1859, 6,6,14]) und die Helveter (vgl. [Caesar 1859, 1,1,29]) selber griechische Buchstaben verwenden. Die zweite Deutung des Zitats vom obigen Zitat ist, dass Caesar seine Botschaft in das Griechische übersetzte. Letztere Verschlüsselungsidee wurde bis ins 20. Jahrhundert verwendet, als im 2. Weltkrieg die US-Amerikaner Angehörige des Indianer-Stammes der Navajo damit beauftragten, Funksprüche mithilfe ihrer Muttersprache zu kodieren (vgl. [Kawano 1990].

3 Fazit

Taktikos' Poliorketika (vgl. [2017]) enthält viele Verfahren zum geheimen Überbringen von Nachrichten. Daher kann gefolgert werden, dass es in der Antike bereits prinzipiell ein Interesse an der Geheimhaltung von Nachrichten gab. Dennoch zählen diese Ideen fast ohne Ausnahme zur Steganographie.

Bei den wenigen Funden, die für die Geschichte der Kryptographie interessant sind, gibt es einige Einschränkungen: Zunächst bleibt es ungeklärt, ob die Skytale tatsächlich als kryptographisches Verfahren verwendet wurde. Weiterhin geht bezüglich des Polybios-Chiffres bereits aus der Überlieferung von Polybios hervor, dass sein Chiffre nicht für die Geheimhaltung, sondern zum Transport von Nachrichten gedacht war.

Lassen sich also diese Verfahren nicht zur Geschichte der Kryptographie zählen? Das hängt von der Stärke der Definition ab, wie bereits Bauer ([2013, 3], Übers. d. Verf.) passend formulierte: „Wie weit man nach den Ursprüngen der Kryptologie sucht, hängt davon ab, inwieweit man bereit ist, Definitionen zu strecken". Eine Definition von kryptographischen Verfahren könnte das notwendige Kriterium beinhalten, dass es bereits zu der Zeit seiner Entstehung für Geheimhaltungszwecke verwendet wurde. Damit fielen das Polybios-Chiffre und eventuell die Skytale als Kandidaten weg.

Selbst wenn man beide Verfahren dazu zählt, so liegt weiterhin der Schluss nahe, dass die Antike für die Entwicklung der Kryptographie unbedeutend ist. Dazu verleitet zumindest der Vergleich der Komplexität und Anzahl von Artefakten aus Kapitel 2 mit den Ergebnissen aus anderen Epochen.

So stellt sich nach dem Ziehen dieses eher ernüchternden Schlusses die Frage, warum die Kryptographie zu der antiken Zeit unbedeutend war. [Schmeh 2008, 3f] vermutet, dass die Kryptographie in dem Schatten der Steganographie stand. Zudem verweist er auf den hohen Analphabeten-Anteil an der Bevölkerung und

dem geringen Schriftverkehr.
Vielleicht wurde der damit als gering anzunehmende Bedarf an Geheimhaltungsverfahren ausreichend durch die der Steganographie gedeckt und sorgte ebenfalls dafür, dass die Chiffren aus dem Kapitel 2 als ausreichend sicher angesehen wurden.

Quellenverzeichnis

[Athenaeus 1854] Athenaeus ; Yonge, C. D. (Hrsg.) und andere, *The Deipnosophists*. Bd. 13. HG Bohn, 1854

[Caesar 1859] Caesar, G. I. ; Kraner, F. (Hrsg.), *C. Iulii Caesaris Commentarii de bello gallico*. JU Kern, 1859

[Gellius 1927] Gellius, A. ; Rolfe, J. C. (Hrsg.), *The Attic Nights*. 1927. – Original Title: Nodes Atticae

[Plutarch 2000] Plutarch ; Perrin, B. (Hrsg.), *Lives: Lysander and Sulla*. Harvard University Press, 2000

[Polybius 1993] Polybius ; Paton, W. R. (Hrsg.), *The Histories Book X*. Bd. 5. 1993

[Tacticus 2017] Tacticus, A. ; Brodersen, K. (Hrsg.), *Stadtverteidigung / Poliorketika*. De Gruyter, 2017

[Tranquillus 1962] Tranquillus, Suetonius ; Butler, H. E. (Hrsg.), *C. Svetoni Tranqvilli Divvs Ivlivs*. Clarendon Press, 1962. – Original Title: De vita Caesarum

[Tranquillus 1982] Tranquillus, Suetonius ; Carter, Betts J. H. (Hrsg.), *Suetonius Divus Augustus*. Bristol Classical Press, 1982. – Original Title: De vita Caesarum

Literaturverzeichnis

[Bauer 2013] Bauer, C. P., *Secret history: The story of cryptology.* CRC Press, 2013

[D'agapeyeff 2016] D'agapeyeff, A., *Codes and ciphers - A history of cryptography.* Read Books Ltd, 2016

[Hebisch 2017] Hebisch, U., *Verschlüsselung nach Caesar.* 2017

[Kahn 1974] Kahn, David, *The codebreakers.* Weidenfeld and Nicolson, 1974

[Kawano 1990] Kawano, Kenji, *Warriors: Navajo code talkers.* Northland Pub, 1990

[Kelly 1998] Kelly, Thomas, The myth of the skytale. In: *Cryptologia* 22 (1998), Nr. 3, S. 244–260

[Kondo/Mselle 2013] Kondo, Tabu S. , Mselle, Leonard J., An Extended Version of the Polybius Cipher. In: *International Journal of Computer Applications* 79 (2013), Nr. 13

[Reinke 1962] Reinke, Edgar C., Classical cryptography. In: *The Classical Journal* 58 (1962), Nr. 3, S. 113–121

[Schmeh 2008] Schmeh, Klaus, Codeknacker gegen Codemacher. In: *Die faszinierende Geschichte der Verschlüsselung* 2 (2008)