

Eine Verschlüsselungsmethode aus dem antiken Sparta

Der griechische Historiograph Plutarch (um 45 - um 125 n. Chr.) beschreibt in der Parallelbiographie «Lysander und Sulla» (ab 96 n. Chr.) eine antike Methode zur Verschlüsselung von Botschaften.¹ Das Beispiel stammt aus dem Stadtstaat Sparta im fünften Jahrhundert v. Chr. (Plut. Lysandros 19-20)

«19. [...] Doch schenkten die Lakedaimonier den sonstigen gegen Lysander² einlaufenden Beschwerden wenig Beachtung. Als aber Pharnabazos, den er gekränkt hatte, indem er sein Land verwüstete und ausplünderte, nach Sparta Ankläger schickte, gerieten die Ephoren³ in grossen Zorn, liessen einen seiner Freunde und Mitfeldherren, Thorax, den sie im privaten Besitz von Geld antrafen, hinrichten und schickten ihm einen Stock mit dem Befehl zurückzukehren.

Mit diesem Stock hat es folgende Bewandnis. Wenn die Ephoren einen Befehlshaber zur See oder zu Lande aussenden, so lassen sie zwei Rundhölzer vollkommen gleich an Länge und Dicke herstellen, so dass sie mit den Schnittflächen genau aufeinanderpassen. Das eine behalten sie, das andere geben sie dem, der ausgesandt wird. Ein solches Holz nennen sie _____. Wenn sie nun eine geheime, wichtige Mitteilung zu machen haben, so lassen sie einen langen, schmalen Streifen aus Papyrus (oder Leder) zurechtmachen wie einen Riemen und wickeln ihn um den bei ihnen befindlichen Stock, ohne einen Zwischenraum zu lassen, sondern so, dass die Oberfläche rundherum überall von dem Streifen bedeckt wird. Ist das geschehen, so schreiben sie, was sie mitteilen wollen, auf den Streifen, so wie er um den Stock gewickelt ist. Haben sie es geschrieben, so nehmen sie den Streifen ab und schicken ihn ohne das Holz an den Feldherrn. Hat er ihn bekommen, so kann er zunächst nichts entziffern, weil die Buchstaben keinen Zusammenhang haben, sondern auseinandergerissen sind. Er nimmt also den bei ihm befindlichen Stock und wickelt den Briefstreifen um sie, so dass, wenn nun die Wickelung in die gleiche Lage kommt wie zuvor, das zweite an das erste schliesst, das Auge im Kreise herumführt und es den Zusammenhang auffinden lässt. Der Brief wird mit demselben Worte wie das Holz genannt, so wie man auch sonst das Gemessene nach dem Messenden nennt.

20. Als dieser Brief zu Lysander nach dem Hellespont⁴ kam, war er höchst bestürzt, und da er insbesondere die Anklagen von Seiten des Pharnabazos fürchtete, so bemühte er sich um eine Zusammenkunft mit ihm, um ihren Streit beizulegen. [...] »

Aufgaben:

1. Wie funktioniert die hier beschriebene antike Verschlüsselungsmethode? Ahmen Sie diese nach!
2. Nennen Sie Vorteile und Nachteile der Methode.
3. Machen Sie Verbesserungsvorschläge, die es einem Unbefugten schwieriger machen, an den Inhalt der Mitteilung heranzukommen.
4. Finden Sie heraus, wie die Spartaner ihre Verschlüsselungsmethode nannten. Der griechische wie der deutsche Begriff bestehen aus sieben Buchstaben (siehe Lücke im Quellentext).
5. Zusatzaufgabe: Wenden Sie die folgenden Grundbegriffe der Kryptologie auf diese Methode an: Code, Schlüssel, Steganographie und Klartext.

¹ Art. «Kryptographie», in: Der neue Pauly. Enzyklopädie der Antike. Stuttgart 2003/2012, Band 6, Spalten 873-874 sowie Band 11, Spalten 643-644.

² Der Staatsmann Lysander (gestorben 395 v. Chr.) gilt als einer der grössten spartanischen Feldherren. Er machte sich im Peloponnesischen Krieg wie im Korinthischen Krieg einen Namen, wurde allerdings wegen seines Ehrgeizes und Hochmuts stark angefeindet.

³ Ephoren waren staatliche Aufsichtsbeamte, die im antiken Sparta jährlich wiedergewählt werden mussten.

⁴ Mit Hellespont bezeichnete die griechische Antike die Meerenge der Dardanellen, der Übergang vom Marmarameer in die Ägäis (Mittelmeer)