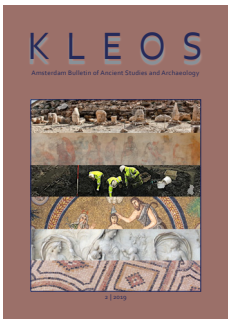
KLEOS

AMSTERDAM BULLETIN OF ANCIENT STUDIES AND ARCHAEOLOGY

Issue 2, 2019



CONTACT

▶bulletin.kleos@gmail.com
▶www.kleos-bulletin.nl

INFORMATION ON PUBLICATION

Full Title: From Fire Signals to ADFGX. A case study in the adaptation of ancient methods of secret communication
Author: Martine Diepenbroek
Published: KLEOS Amsterdam Bulletin of Ancient Studies and Archaeology / Issue 02 / April 2019
Pages: 63 - 76
ISSN: 2468-1555
Link to these articles: www.kleos-bulletin.nl

Recommended citation:
Diepenbroek, M., 2019: From Fire Signals to ADFGX. A case study in the adaptation of ancient methods of secret communication. *Kleos- Amsterdam Bulletin of Ancient Studies and Archaeology* 2, 63-76.

KLEOS - Amsterdam Bulletin of Ancient Studies and Archaeology
is a peer-reviewed, open access academic online journal, launched in 2014, which publishes current research and review articles by graduate and PhD students, as well as starting independent researchers, from the fields of archaeology and ancient studies (i.e. classics and ancient History). *Kleos* also provides reviews of recent books, conferences and exhibitions. The journal mainly aspires to serve as a platform for starting academic careers, and help students and starting researchers to share their research, gain experience in publishing, and improve their scientific skills. At the same time the journal aims to provide an overview of the research being conducted within the fields of archaeology, ancient history and classics, and support the interdisciplinary dialogue between these adjacent academic disciplines.

SUBMISSIONS

The editors invite submissions of original research on any topic related to ancient history, classics and archaeology. Information on the editorial policy, the submission process, as well as guidelines for authors and other matters that concern potential contributors, is to be found on our website. For further information, authors and readers are referred to:
▶www.kleos-bulletin.nl
▶vu-nl.academia.edu/KLEOSBulletin

DISCLAIMER

The editors cannot be held responsible for errors or any consequences arising from the use of information contained in this publication. The opinions expressed in the articles and reviews published in *Kleos* are those of the authors and not of the editors, nor of the Amsterdam Centre for Ancient Studies and Archaeology (ACASA). The publication of advertisements in *Kleos* or on the website does not constitute any endorsement by the editors of the products or institutions advertised.

COPYRIGHT AND PHOTOCOPYING

Authorisation to photocopy items for academic, educational and personal use is granted. Check for information about the terms and conditions of use: www.kleos-bulletin.nl

From Fire Signals to ADFGX. A case study in the adaptation of ancient methods of secret communication

Martine Diepenbroek

Abstract

Very early-on in Greek history mountaintops were already used as watch-towers and signalling stations from which messages could be sent over long distances by fire signals. In these earliest examples it was only possible to send one prearranged message, something that was often not sufficient in case communicating parties needed to communicate on urgent matters. The fourth-century BC military author Aeneas Tacticus accordingly invented a method for fire signalling, whereby a series of messages could be sent related to events that often occur in warfare. The system might have been used as a cryptographic device. Due to errors in Aeneas' system, Polybius improved another system based on the same principles, which in turn formed the basis for the modern 'Polybius square', used by the Germans for their ADFGX- and ADFGVX-ciphers: secret cipher systems used in the First World War. There is no clear evidence linking Aeneas' fire signalling method directly to the German ciphers. However, it will be shown that Polybius used Aeneas' system in his own fire signalling method. Polybius' method in turn impacted the development of the Polybius square and its use in the ADFGX and ADFGVX ciphers. By analysing the ancient history of Polybius' method for fire signalling and the merits of applying this to the use of the square in the German ciphers, it will be shown how an ancient fire signalling method inspired modern ciphers.

Martine Diepenbroek is a Dutch PhD student at the University of Bristol (UK). In her PhD thesis she works on the role of ancient cryptography and steganography in confidential correspondence in Greco-Roman warfare. A key figure in this field was the fourth-century BC military author Aeneas Tacticus. In her thesis she thoroughly analyses Aeneas' work 'How to Survive Under Siege', and compares this to other ancient sources on cryptography and steganography.

▶Profile page

Introduction

In a lost work on military preparations, the mid-fourth-century BC strategist and military author Aeneas Tacticus discussed a method for fire signalling, as discussed by Polybius.[1] Since Aeneas' method

1 Polybius, *Histories*, 10.44.

was laborious and open to errors, Polybius improved a method based on the same principles, forming the basis for the modern 'Polybius square' which is referenced by numerous modern cryptographers.[2] However, there is a gap in the literature; none of these scholars seem to fully appreciate the Polybius squares' origins, nor do they recognise the ways in which Polybius' original method anticipated the ADFGX and ADFGVX ciphers that were used by the Germans in the First World War. The current study will show the relevance of understanding the history of Polybius' method for fire signalling, and the merits of applying this to the use of the square in the German ADFGX and ADFGVX ciphers, thus filling a lacuna in our understanding of modern ciphers.

Aeneas Tacticus' method for fire signalling

Very little is known about the life of Aeneas Tacticus.[3] In the middle of the fourth century BC, he wrote a manual for generals known as *How to Survive Under Siege*.[4] The most important theme of this work was that there was always the threat of treachery from within a city during sieges.[5] Given the significant risk of citizens within the *polis* conspiring and communicating with the enemy, it was vital for the commanding forces to be able to communicate between themselves secretly and securely. In chapter 31 of his work, Aeneas accordingly described 16 different ways in which cryptography could have played an important role in surviving sieges.[6] In another lost work on military preparations, Aeneas discussed a method for fire signalling that could also have been used in cryptography.[7] A description of this method can be found in Polybius' *Histories*.[8]

Early-on in Greek history mountaintops were already used as watch-towers and signalling stations.[9] From these 'towers'

2 Polybius, *Histories*, 10.45.6-12; Kahn 1996, 76-77, 83; Mollin 2005, 9-10; Mollin 2006, 89.

3 Aeneas Tacticus is identified as Aineias of Stymphalos, an Arcadian general from the fourth century BC, mentioned by Xenophon (*Hellenica* ,7.3.1. See also: Oldfather 1928, 7; Sheldon 1986, 39; Whitehead 1990, 4, 10; Whitehead 2018, 21.

4 Hug 1877, 28; Brownson 1918, 281; Oldfather 1928, 7; Hunter / Handford 1927, ix-x., xxii, xxiv-xxv, 264; Barends 1955, 171; Delebecque 1957, 430; Star 195, 68; Bon 1967, vii, xii; David 1986, 343; Whitehead 1990, 10-12; Bliese 1994, 108; Vela Tejada 2004, 141-142; Rawling 2007, 13; Millett 2013, 65.

5 Aeneas Tacticus, *How to Survive Under Siege*, 4.1-4, 5.1, 9.2, 10.6, 10.11, 10.25-26, 11.3-6, 18.3-6, 18.13-18.21, 22.5, 22.7, 31 (*passim*); Liddel 2018, 124.

6 There is little evidence that any of these techniques were used in Antiquity (Pretzler 2018, 98). However, several of the events discussed in the work are narrated with such detail that it seems plausible that Aeneas played a part in some of them himself (Oldfather 1928, 4; Hunter / Handford 1927, xxxviii; Sheldon 1986, *passim*).

7 Aeneas referred to this work in *How to Survive Under Siege* (7.1-4).

8 Polybius, *Histories*. 10.44. Polybius was read widely by the ancients, as is shown by quotations of his work in the works of Strabo, Athenaeus, Cicero, Diodorus Siculus, Livy, Plutarch and Arrian (*all passim*). Much of the text that survives today from the later books of the *Histories* was preserved in Byzantine anthologies.

9 Homer, *Iliad*, 4.275-276, 5.770-771; Simonides, *Elegies*, 130; Vergil, *The Eclogues*, 8, 59; *Aeneid,* 10.454, 11.526.

messages could be sent over long distances by lighting strategic fires, as is known from e.g. Homer's *Iliad* (seventh century BC), and Aeschylus' *Agamemnon* (mid-fifth century BC).[10] Yet, in these examples the lighting of the fires communicated one prearranged message, which often did not suffice in case communicating parties needed to contact each other on urgent matters.[11] Aeneas Tacticus found a solution for the problem of only being able to send prearranged messages, and invented a method for fire signalling, whereby various messages could be sent, as has been discussed in Polybius' *Histories*.[12] According to Polybius, Aeneas discussed the system in the following way:

> "[...] those who are about to communicate urgent news to each other by fire signal should procure two earthenware vessels of exactly the same width and depth, [as well as corks]. [Through] the middle of each cork [they] should pass a rod graduated in equal sections [...], each clearly marked off from the next. In each section should be written the most evident and ordinary events that occur in war [...]. [Whenever] any of the contingencies written on the rods occurs [Aeneas] tells us to raise a torch and to wait until the corresponding party raises another. When both [...] torches are [...] visible, the signaller is to lower his torch and at once allow the water to escape through the aperture. Whenever, as the corks sink, the contingency you wish to communicate reaches the mouth of the vessel [Aeneas] tells the signaller to raise his torch and the receivers of the signal are to stop the aperture at once and to note which of the messages written on the rods is at the mouth of the vessel. This will be the message delivered, if the apparatus works at the same pace in both cases."[13]

What Polybius, and therefore Aeneas, described was an inventive and laborious method for fire signalling by using water clocks and torches.[14] Two parties who wanted to communicate with each other by means of fire signals had to take two vessels, rods and corks. The rods had to be divided into equal parts by marking them with notches. On each part of the rods one had to inscribe

10 Homer's *Iliad*, 18.203-214; Aeschylus, *Agamemnon*, 281-316. See also e.g.: Herodotus, *Histories*, 7.183, 9.3; Diodorus Siculus, *Library of History,* 19.57; Julius Africanus, *Kestoi*, 77; Onasander, *The General,* 25.2; Frontinus, *Stratagems*, 3.11.5; Polyaenus, *Stratagems of War*, 6.16.2, Hyde 1915; Dvornik 1974, 31-33; Sheldon 1987, 135; Russell 1999, 145; Sheldon 2005, 127; Woolliscroft 2001, *passim* (especially Appendix 1).

11 Polybius, *Histories*, 10.43.5-6.

12 Ibid., 10.43-46.

13 Ibid,. 10.44; translation: Paton, Walbank *et. al.* 2011, 235-237.

14 Oldfather 1928, 46-47; Hunter / Handford 1927, 120, 122-123; De Agapayeff 1939, 16-17; Dvornik 1974, 42-43; Rihll 2018, 281-287.

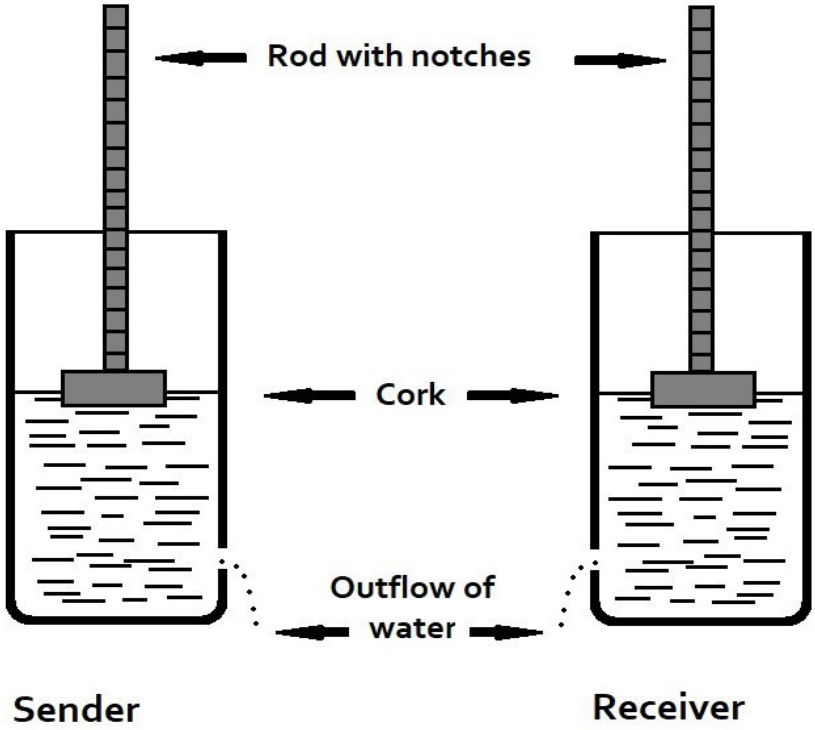


Figure 1
A possible reconstruction of Aeneas' water clock as described by Polybius (created by author, based on Aschoff 1984, 47-48).

events that often occurred in warfare. Both parties then had to set up signalling stations on a visible distance from each other. When any of the events ascribed on the rods occurred, one party had to raise a torch, and wait for the other party to respond in the same way. At this point, both parties had to pull the plugs out from the bottom of the vessels in order to let the water escape, thus causing the rod to sink into the vessel. When the right inscription reached the top of the vessel, the sending party would raise the torch again to show the receiving party that they should replace the plug and read the message that was revealed at that water level. In this way the receiving party understood the intended message (Figure 1). Since Aeneas understood the need for secrecy, because of the constant danger of treachery, it is possible, yet not provable that Aeneas' system was used for secret communication.[15] When the system was used in this way, it could have allowed communicating parties to send prearranged secret messages via the rods.

Polybius' system for fire signalling

Recent experiments in archaeology have shown Aeneas' system to be feasible.[16] Also, it is known from the second-century AD author Polyaenus that the Carthaginians used a similar method

15 Aeneas Tacticus, *How to Survive Under Siege*, 31.1.

16 Sheldon 2005, 205.

successfully.[17] However, there are two large downsides to Aeneas' method. It would have been extremely difficult to let the two water clocks run exactly parallel, and still only prearranged messages could be transferred between communicating parties.[18] Accordingly, Polybius discussed a more sophisticated system of fire signalling in his *Histories*. According to Polybius:

> "[A] recent method, [...] perfected by myself, is quite definite and capable of dispatching with accuracy every kind of urgent messages [..]. It is as follows: We take the alphabet and divide it into five parts [...] Each of the two parties [...] must [...] get ready [two sets of five torches and] five tablets and write one division of the alphabet on each tablet. [Both parties must then raise] two torches [...] for the purpose of conveying to each other that they are both at attention. [After this] the dispatcher of the message will [...] raise the first set of torches on the left side indicating which tablet is to be consulted [...]. Next, he will raise the second set on the right on the same principle to indicate what letter of the tablet [should be consulted]."[19]

Like Aeneas, Polybius still used torches, but replaced the water clocks by tablets on which the letters of the Greek alphabet were written (Figure 2).[20] The recipient had to write down all the letters that were communicated to him by means of fire signals to understand the intended message. If necessary, he could reply in the same way.

1		2		3		4		5	
α	1	ζ	1	λ	1	π	1	φ	1
β	2	η	2	μ	2	ϱ	2	χ	2
γ	3	θ	3	ν	3	σ	3	ψ	3
δ	4	ι	4	ξ	4	τ	4	ω	4
ε	5	κ	5	ο	5	υ	5		

Figure 2
Five tablets with the letters of the Ancient Greek alphabet used for fire signalling, as described by Polybius (Polybius, Histories, 10.45.6-12); (John Savard 1998/1999, The Bifid, the Trifid, and the Straddling Checkerboard, Source http://www.quadibloc.com/crypto/pp1322.htm).

Although Polybius' method was still laborious, it was clearly an improvement over Aeneas' method, since in Polybius' method no water clocks were involved that had to run parallel, and

17 Polyaenus, *Stratagems of War*, 6.16.2; Dvornik 1974, 56; Sheldon 1987, 28.

18 Polybius, *Histories*, 10.45.1-2; Hunter / Handford 1927, 120.

19 Translation: Paton, Walbank *et. al.* 2011, 239-241.

20 Polybius, *Histories*, 10.45.6-12.

every possible message could be sent, instead of only a series of prearranged messages. The fact that every possible message could be sent, makes Polybius' method easier to use in cryptography than Aeneas' method. However, once more, clear evidence for its use in secret communication remains inaccessible. Out of Polybius' method, a modern variation developed that provably has been used in cryptography: the 'Polybius square'. Among cryptographers, Polybius is often incorrectly seen as the creator of this modern cryptographic device.[21] However, the term 'Polybius square' only appears in 20th- and 21st-century cryptographic literature.[22]

	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

Figure 3
Polybius square: a 5x5 square in which a modern alphabet is placed (Salomon 2003, 29).

The Polybius Square

The Polybius square is a mathematical square – in contrast to Polybius' tablets – used in modern cryptography. A basic Polybius square consists of five rows and columns, which gives 25 cells. In these cells the 26 letters of a modern alphabet are written in their normal order from left to right, and top to bottom (Figure 3). Hereby, the letters 'I' and 'J' are usually placed in the same block.[23] All rows and columns in the square have a number. In a basic square these are the numbers one to five for both rows and columns. Every letter in the square gets a coordinate. The letter 'A', for example, can be found in the first row on the first column, which gives the coordinate 1-1, written as '11'.[24] In this way, all the letters in the square have a coordinate between '11' (A) and '55' (Z). So, in a Polybius square, first the row is indicated, and then the column. Polybius' method worked the other way around. Polybius discussed indication of the tablet first, which can be compared to the column of the Polybius square, and then the letter on the tablet, which can be compared to the row of the Polybius square.[25] A message that is sent by means of a Polybius square looks like a series of numbers. The message:

'*SEND MORE TROOPS BEFORE MIDNIGHT*',

for example, would look like the following sequence:

43 15 33 14 - 32 34 42 15 - 44 42 34 34 35 43 - 12 15 21 34 42 15 - 32 24 14 33 24 22 23 44

Since every coordinate contains two numbers – one for the row

21 Kahn 1996, 76-77, 82-83; Mollin 2005, 9-10; Mollin 2006, 89.

22 Kahn 1996, 76-77, 82-83; Mollin 2005, 9-10; Mollin 2006, 89.

23 Kahn 1996, 83; Mollin 2006, 90; Lunde 2012, 78-79.

24 Mollin 2006, 90; Kahn 1996, 83, Lunde 2012, 78-79.

25 Polybius, *Histories*, 10.4.6-12.

and one for the column – an encrypted text is created that is twice as long as the non-encrypted text.[26] To decipher the message, the recipient would take a Polybius square, look for the coordinates in the square, and check which letters correspond to these coordinates. The Polybius square has been used for cryptography in this way by the British army in the Boer War, and by the British and German armies in the First and Second World War.[27] Yet, the Polybius square could also be used as the basis for other cryptographic methods. In the last year of the First World War, for example, the German military intelligence services used the Polybius square in the ADFGX and ADFGVX ciphers.[28]

Adaptation of the Polybius square

The ADFGX and the ADFGVX ciphers were a combination of a substitution and a transposition cipher. In substitution ciphers the letters of a normal non-encrypted text, known as plaintext, are substituted into other letters, characters, or symbols.[29] In a transposition cipher, on the other hand, the normal sequence of letters of the plaintext is only rearranged. No letter is substituted into another letter or symbol.[30] The text that is formed after substitution and transposition is known as the ciphertext.[31] The ADFGX and ADFGVX ciphers are named after the only five, later six, letters that appeared in the ciphertext: the letters A, D, F, G, V, and X.[32] Messages encrypted with the ciphers were transmitted by Morse code. The six letters were chosen to minimise transmission errors, since the letters sound very different form one another in Morse code.[33] Since the ADFGX and ADFGVX ciphers were a combination of a substitution and a transposition cipher, a multistep process was used to create encrypted text with these ciphers.

In March 1918 the first of the cipher systems was introduced: the ADFGX cipher. This cipher used a Polybius square of 5x5. This square was filled with 25 of the 26 letters of the German alphabet in random order, agreed upon between sender and recipient (Figure 4).[34] The rows and columns of the Polybius square used

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

Figure 4
ADFGX cipher: Table filled with 25 of the 26 letters of the modern alphabet in a random order agreed upon between sender and recipient (created by author).

26 Mollin 2005, 1; Reba / Shier 2015, 480.

27 Mollin 2006, 90; Kahn 1996, 83; Van Tilborg, 2006, 32; Lunde 2012, 78-79.

28 Van Tilborg, 2006, 32.

29 Reinke 1962, 113; Singh 1999, 5-7; Bauer 2007, 382.

30 Ibid.

31 Mollin 2005, 1; Reba / Shier 2015, 480.

32 Childs 1919, 13; Mollin 2005, 1; Klima / Sigmon 2012, 55; Reba / Shier 2015, 480; Dooley 2016, 65.

33 Klima / Sigmon 2012, 55.

34 Ibid.

for the cipher were then labelled with the letters 'A', 'D', 'F', 'G', and 'X'. Each letter of the plaintext that had to be encrypted was then replaced by a pair of letters consisting of the letters 'A', 'D', 'F', 'G', and 'X' that could now be found in the utmost left cells of the rows, and in the top cells of the columns, hereby following the table.[35] First, the letter in the row was written, followed by the letter in the column. Therefore, the plaintext letter 'Y', was encrypted as 'XF' (Figure 5). In this way, a ciphertext was created that was twice as long as the plaintext, and that only contained the letters 'A', 'D', 'F', 'G', and 'X'.[36] The plaintext message:

'Send weapons quickly',

for example, would have been substituted into the following ciphertext:

GA DD AD FX - FG DD AA DX FF AD GA - DA DF AX GD FA FD XF

One of the characteristics of a Polybius cipher is that the length of the ciphertext is twice the length of the plaintext. The ADFGX cipher has this Polybius square characteristic. Yet, after the substitution of the message into ciphertext, the second step took place: the transposition. The origins of transposition ciphers can be traced back to the use of the Spartan *scytale*.[37] From Plutarch and Aulus Gellius we know that around a *scytale* (stick) a strip of writing material was wrapped, on which a secret message was written. Then the strip was unwrapped from the *scytale* whereby all letters changed place.[38] The principle of the changing positions of letters can also be found in the ADFGX cipher. The ciphertext that was created in the first step of the process (GA DD AD FX FG DD AA DX FF AD GA DA DF AX GD FA FD XF) was then written in a rectangular table from left to right, and from top to bottom in as many rows as necessary to write the entire message. The top row of the table was used for a 'key' (Figure 6).[39] In cryptography, the 'key' is the information that is needed to encipher and decipher a

Figure 5

ADFGX cipher table with rows and columns marked with the letters 'A', 'D', 'F', 'G', and 'X' (created by author).

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

Figure 6

ADFGX cipher table with keyword 'attack' (created by author).

A	T	T	A	C	K
G	A	D	D	A	D
F	X	F	G	D	D
A	A	D	X	F	F
A	D	G	A	D	A
D	F	A	X	G	D
F	A	F	D	X	F

35 Klima / Sigmon 2012, 56.

36 Ibid.

37 Childs 1919, 13; Dooley 2016, 65.

38 Plutarch, *Life of Lysander*, 19.5; Aulus Gellius, *Attic Nights*, 17.9.9. The two *scytalae* must have had the same diameter for the cipher to work. Otherwise, the letters would not have returned to their original place. It has been incorrectly argued by S. West and T. Kelly that *scytalae* were never used for cryptographic purposes (West 1988, 42; Kelly 1998, 246). According to these scholars, the principal meaning of the word *scytale* is 'stick' (Kelly 1985, 162; 1998, 245; West 1988, 42. See also: Strasser 2007, 278). However, these definitions in themselves do not mean that *scytalae* could never have been used for secret communication. On the contrary, the method as described by Plutarch and Gellius is so detailed and obviously useful, that it seems more than likely that *scytalae* were regularly used for this purpose in contexts where secrecy of communication was important.

39 Klima / Sigmon 2012, 34-35; Dooley 2013, 8.

message. Normally, this is a word or short sentence.[40] In Figure 6, for example, the keyword 'attack' is used.

The text in Figure 6, already once encrypted, was considered to be plaintext text again, which had to be encrypted into ciphertext.[41] This was achieved by rearranging the order of the columns in the table.[42] For this, the letters of the key were written in alphabetical order. In the case of the key '*attack*' the letters would be rearranged as A, A, C, K, T, and T. The associated columns were then rearranged in the same order, since they moved along with the letters of the key.[43] In case a letter appeared more than once in a key, like we see twice in the case of '*attack*', the leftmost column was written first.[44] So, in this case the columns were rearranged in the order 1-4-5-6-2-3 (Figure 7). Eventually, the ciphertext was taken column by column from left to right and written horizontally.[45] This provides the following sequence of letters:

GFAADF DGXAXD ADFDGX DDFADF AXADFA DFDGAF

So, this was the second time that the original message '*SEND WEAPONS QUICKLY*' was encrypted. This encrypted text was sent to the receiver who had to decrypt the text by taking all the steps in the process in reverse order.

Figure 7
ADFGX table with rearranged order of columns (1-4-5-6-2-3) (created by author).

A	A	C	K	T	T
G	D	A	D	A	D
F	G	D	D	X	F
A	X	F	F	A	D
A	A	D	A	D	G
D	X	G	D	F	A
F	D	X	F	A	F
1	**4**	**5**	**6**	**2**	**3**

The ADFGVX cipher

In June 1918, three months after the introduction of the ADFGX cipher, the Germans added an extra row and column to the Polybius square that was used for the cipher to create a 6x6 grid. Extending the grid meant that an extra letter was required to create ciphertext. The letter V was chosen for this, since this letter sounds different from the five other letters in Morse code. The newly created cipher was called the ADFGVX cipher.[46] It worked in the exact same way as its predecessor the ADFGX cipher. The ADFGX and ADFGVX ciphers were the most advanced cipher systems that the German military intelligence used during the First World War.[47] In fact, they turned out to be the toughest

40 Klima / Sigmon 2012, 34-35; Dooley 2013, 8. Aeneas Tacticus already understood the importance of a key (*How to Survive Under Siege*, 31.1).

41 Klima / Sigmon 2012, 56. This ciphertext was converted from the original plaintext '*SEND WEAPONS QUICKLY*'.

42 Klima / Sigmon 2012, 34-35; Dooley 2013, 8.

43 Klima / Sigmon 2012, 56-57.

44 Ibid.

45 Ibid.

46 Ibid., 55-57.

47 Mollin 2000, 12.

ciphers known in secret communication until the end of this war.[48]

Conclusion

The fundamental principles of fire signalling systems can be traced all the way back to Aeneas Tacticus in the fourth century BC. Clear evidence for its use in the context of secret communication remains inaccessible. Also, there is no clear evidence linking Aeneas' fire signalling method directly to the ADFGX and ADFGVX ciphers used by the Germans in the First World War. However, if we take a step back, we can see how Aeneas' system for fire signalling has inspired Polybius' system, which in turn impacted the development of the Polybius square. We do have direct evidence for the way in which the Polybius square was used in the ADFGX and ADFGVX ciphers, which turned out to be the toughest ciphers known in military secret communication until the end of the First World War. The fact that ancient core principles are still in use in modern methods for communication security demonstrates that these methods would have worked well in Antiquity – potentially and presumably conferring military and strategic advantage even though the concrete evidence for this remains inaccessible.

48 Kahn 1996, 334, 535-539; Churchhouse 2002, 45-46; Mollin 2000, 12.

Bibliography

Aschoff, V., 1984: *Geschichte der Nachrichtentechnik: Beiträge zur Geschichte der Nachrichtentechnik von ihren Anfängen bis zum Ende des 18. Jahrhunderts*, Berlin/ Heidelberg/ New York/ Tokyo.

Barends, D., 1955: *Lexicon Aeneium : a lexicon and index to Aeneas Tacticus' military manual „On the defence of fortified positions"*, Assen.

Bauer, F. L., 2007: Rotor Machines and Bombes, in K. de Leeuw/ J. Bergstra (eds.), *The History of Information Security. A Comprehensive Handbook*, Amsterdam.

Bliese, J. R. E., 1994: Rhetoric Goes to War: The Doctrine of Ancient and Medieval Military Manuals, *Rhetoric Society Quarterly*, Vol. 24 (3/4), 105-130.

Brownson, C. L., 1918: *Xenophon. Hellenica*, Volume I: Books 1-4. *Translated by Carleton L. Brownson*, Cambridge (MA) (Loeb Classical Library 88).

Burliga, B., 2008: Aeneas Tacticus Between History and Sophistry. The emergence of the military handbook, in J. Pigoń (ed.) *The children of Herodotus: Greek and Roman historiography and related genres*, Newcastle, 92-101.

Childs, J. R., 1919: *War Department Office of the Chief Signal Officer, Washington. German Military Ciphers from February to November 1918. Technical Paper of the Intelligence Section War Plans and Training Division*, Washington.

Churchhouse, R., 2002: *Codes and Ciphers*, Cambridge.

Coles, M./ R. Landrum, 2009: *Expert SQL Server 2008 Encryption*, New York.

De Agapayeff, A., 1939: *Codes and Ciphers*, Oxford/ London/ New York/ Toronto.

Dooley, J. F., 2013: *A Brief History of Cryptology and Cryptographic Algorithms*, Cham/ Heidelberg/ New York/ Dordrecht/ London.

Dooley, J. F., 2016: *Codes, Ciphers and Spies. Tales of Military Intelligence in World War I*, New York.

Dvornik, F., 1974: *Origins of Intelligence Services. The Ancient Near East, Persia, Greece, Rome, Byzantium, the Arab Muslim Empires, the Mongol Empire, China, Muscovy*, New Brunswick/ New Jersey.

Hug, A., 1877: *Aeneas von Stymphalos, ein arkadischer Schriftsteller aus klassischer Zeit. Gratulationsschrift der Universität Zürich an die Universität Tübingen zu deren vierhundertjähriger Stiftungsfeier vom VIII. - XI. August MDCCCLXXVII*, Zürich.

Hunter, L. W./ S. A. Handford, 1927: *Aeneas on Siegecraft. A Critical edition prepared by L. W. Hunter M.A. (Late Fellow of the New College, Oxford).* Revised, with some additions, by S. A. Handford, B.A. (Formerly Scholar of Balliol College, Oxford), Oxford.

Hyde, W. W., 1915: The Mountains of Greece, *The Bulletin of the Geographical Society of Philadelphia* 13, 1-16; 47-64; 110-126.

International Organization for Standardization, 2018: 'About Us' and 'What are Standards'. https://www.iso.org/about-us.html accessed on 18-03-2019.

Kahn, D., 1996: *The Codebreakers. The Comprehensive History of Secret Communication from Ancient Times to the Internet*, New York.

Kelly, T., 1998: 'The Myth of the Skytale', *Cryptologia* 22 (3), 253-260.

Klima, R. E./ N. P. Sigmon, 2012: *Cryptology. Classical and Modern with Maplets*, Boca Rotan/ London/ New York (Cryptography and Network Security Series).

Liddel, P., 2018: Writing and Other Forms of Communication in Aineias' Poliorketita, in M. Pretzler/ N. Barley (eds.), *Brill's Companion to Aineias Tacticus*, Leiden/Boston, 123-145.

Liddell H. G./ R. Scott, 1986: *A Greek-English lexicon*. Compiled by Henry George Liddell and Robert Scott, Oxford.

Lunde, P., 2012: *The Secrets of Codes. Understanding the World of Hidden Messages*, San Francisco.

Millett, P. C., 2013: Writers on War: Part 1 Greece. Winning Ways of Warfare, in B. Campbell/ L. A. Tritle (eds.), *The Oxford Handbook of Warfare in the Classical World,* Oxford/ New York/ Auckland/ Cape Town/ Dar es Salaam/ Hong Kong/ Karachi/ Kuala Lumpur/ Madrid/ Melbourne/ Mexico City/ Nairobi/ New Delhi/ Shanghai/ Taipei/ Toronto.

Mollin, R. A., 2000: *An Introduction to Cryptography*, Boca Raton/ London/ New York/ Washington.

Mollin, R. A., 2005: *Codes. The Guide to Secrecy From Ancient to Modern Times*, Boca Raton/ London/ New York/ Singapore.

Mollin, R. A., 2006: *An Introduction to Cryptography*, 2nd Edition, Boca Raton.

Montanari, F., 2015: *The Brill Dictionary of Ancient Greek*, Editors of the English edition: M. Goh/ C. Schroeder, Leiden.

Oldfather, W. A., 1928: Introduction and Notes, *Illinois Greek Club 1928, Aeneas Tacticus, Asclepiodotus, Onasander. Aeneas Tacticus, Asclepiodotus, and Onasander. Translated by Illinois Greek Club*, Cambridge, passim (Loeb Classical Library 156).

Paton, W. R./ F. W. Walbank/ C. Habicht, 2011: *Polybius. The Histo-*

ries, Volume IV: Books 9-15. *Translated by W. R. Paton. Revised by F. W. Walbank, Christian Habicht*, Cambridge (Loeb Classical Library 159).

Pretzler, M., 2018: Aineias and History. The Purpose and Context of Historical Narrative on the *Poliorketia*, in M. Pretzler/ N. Barley (eds.), *Brill's Companion to Aineias Tacticus*, Leiden/ Boston, 68-95.

Rawling, L., 2007: *The Ancient Greek at War*, Manchester/ New York.

Reba, M. A./ D. R. Shier, 2015: *Puzzles, Paradoxes, and Problem Solving: An Introduction to Mathematical Thinking*, London/ New York/ Boca Raton.

Reinke, E. C., 1962: Classical Cryptography, *The Classical Journal* 58 (3), 113-121.

Rihll, T. E., 2018: Technology in Aineias Tacticus. Simple and Complex, in M. Pretzler/ N. Barley (eds.), *Brill's Companion to Aineias Tacticus*, Leiden/Boston, 265-289.

Russell, F. S., 1999: *Information Gathering in Classical Greece*, Ann Arbor.

Salomon, D., 2003: *Data Privacy and Security: Encryption and Information Hiding*, New York.

Savard, J., 1998/1999: The Bifid, the Trifid, and the Straddling Checkerboard. John Savard's website http://www.quadibloc.com/crypto/pp1322.htm accessed on 18-03-2019.

Sheldon, R. M., 1986: Tradecraft in Ancient Greece, *Studies in Intelligence* 30 (1), 39-47.

Sheldon, R. M., 1987: *Tinker, Tailor, Caesar, Spy. Espionage in Ancient Rome*, Michigan.

Sheldon, R. M., 2005: *Intelligence Activities in Ancient Rome. Trust in the Gods, but Verify*, London/ New York.

Singh, S., 1999: *The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, London.

Starr, C. G., 1957: Reviewed Work(s): Lexicon Aeneium. A Lexicon and Index to Aeneas Tacticus' Military Manual „On the Defence of Fortified Positions" by D. Barends, *Classical Philology* 52 (1), 68.

Strasser, G. F., 2007: The Rise of Cryptology in the European Renaissance, in K. de Leeuw/ J. Bergstra (eds.), *The History of Information Security: A Comprehensive Handbook*, Amsterdam, 277-325.

Van Tilborg, H. C. A., 2006: *Fundamentals of Cryptoglogy. A Professional Reference and Interactive Tutorial by Henk C. A. van Tilborg, Eindhoven University of Technology, The Netherlands*, 2nd Edition, Boston/Dordrecht/London.

Vela Tejada, J., 2004: Warfare, History and Literature in the Archaic and Classical Periods. The Development of Greek Military Treatises, *Historia. Zeitschrift für alte Geschichte* 53 (2), 129-146.

West, S., 1998: Archilochus' message stick, *Classical Quarterly* 38, 42-48.

Whitehead, D., 1990: *Aineias the Tactician. How to Survive Under Siege*, Oxford/New York.

Whitehead, D., 2018: The Other Aineias, in M. Pretzler/ N. Barley (eds.), *Brill's Companion to Aineias Tacticus*, Leiden/ Boston, 14-32.

Williams, T. H., 1904: The Authorship of the Greek Military Manual attributed to 'Aeneas Tacticus', *American Journal of Philology* 25 (4), 390-405.

Woolliscroft, D.J., 2001: *Roman Military Signalling*, Stroud.