

Prey to a Privateer. Two Portuguese Ciphertexts from 1649

Jörgen Dinnissen

Historian,

The Netherlands

dinnissen.jorgen@gmail.com

Hugo Araújo

Federal University of Santa Maria,

Brazil

hugoaffa@hotmail.com

Abstract

The deciphered ciphertexts from the former governor-general of Brazil, António Teles da Silva, reveal two letters from him to the king of Portugal from 1649, while he was a prisoner. The letters were written in Portuguese and found on a Luso-Brazilian ship captured by a Dutch privateer, from the *Brasilse Directie Middelburg*, before the coast of Brazil. These letters were already known as plaintext letters in the National Archives, The Hague. We were able to relate the ciphertexts to the plaintexts and translations.

This paper shows that the revealed strategic military information and state secrets made no impact on the superiors of the Dutch company, the Gentlemen XIX, in The Netherlands.

It also shows that ciphers were provided from 1638 onwards in Portuguese Brazil. Based on the surviving sources, ciphertexts were used by the Portuguese mainly after the Dutch structurally threatened their communication. They became frequent in short-distance communication (on land) after the revolt of the sugar planters in 1645. In long-distance communication, over the seas, after the Dutch privateers compromised the Portuguese shipping between 1647 and 1648.

1 Introduction

The 167 ciphertext is a four manuscript pages of the Dutch West India Company (WIC) located at the National Archives, The Hague, The

Netherlands (Teles da Silva, 1649a1). The description of this manuscript reads: “Ciphercode (Dutch: *cijfercode*) from Antonio Telles da Silva, with key, 1649-3-28.”¹

The 168 ciphertext is also four manuscript pages found in the same archive (Teles da Silva, 1649b1). Its description reads: “Ciphercode from Antonio Telles da Silva, with key, 1649-12-3.”

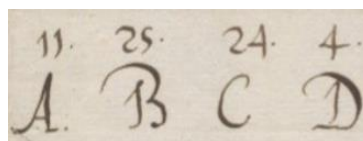


Figure 1: Part of the key from the 167 cipher.

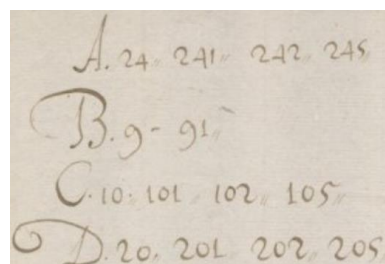


Figure 2: Part of the key from the 168 cipher.

We made a digital transcription of all pages manually. This transcription was put into the software CrypTool 2 (CT2). Using the digitized nomenclature, CT2 generated the revealed plaintext used for this paper. Table 1 shows the very first word of the two documents in ciphertext, transcription, revealed plaintext in Portuguese, and its translation into English.

¹ The dates in both manuscripts are wrong in the archival record, probably a misread by the archivist.

Month of 167 must read 5 (not 3), and month of 168 must read 6 (not 12).

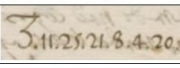
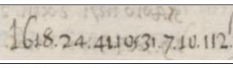
	Cipher 167	Cipher 168
Ciphertext		
Manual transcription	3.11.25.21.8.4.20.	161.8.24.41.105.31.7.10.112.
Revealed plaintext as CT2 output	Sabendo	Francisco
Translation from Portuguese into English	Knowing	Francisco

Table 1: First word of the two ciphertexts deciphered.

Next to the ciphertexts, we found the Portuguese plaintexts and translations into Dutch. We have identified information in other sources about the ship that carried these ciphertexts and the frigate that seized it. At last, we found that a person with knowledge of ciphers (Dutch: *persoon daer van kennijse hebbende*) was able to decrypt the ciphertexts through cryptanalysis and, after that, translated them. Unfortunately, the source does not mention the cryptanalyst’s name.

The ciphertexts, the revealed plaintexts, and the translations were sent in one package – together with other letters, reports, and an accompanying letterbook – by the government of Dutch Brazil, the *Hoge Raad Brasil* (*Hoge Raad*) to their company superiors, the Gentlemen XIX.

The paper will analyze these ciphertexts, their cipher, relating their decrypting and translation into Dutch to the context of the war in Brazil. We will present how the obtaining and decryption of the ciphertexts was part of the administrative practices of the WIC. In particular, we will highlight the use of Jewish scholars who acted as decrypters for the Dutch.

This paper is structured as follows: Section 2 contains a summary of the letters hidden in the ciphertexts and background information. Section 3 shows the complete trail of these letters within the Dutch administrative process. Section 4 discusses the importance of ciphertexts and how often they were used in Brazil. The technical matters of the used ciphers are discussed in Section 5. Finally, Section 6, presents five conclusions about these sources and their use.

2 Content of the Two Letters

There is a hidden letter in each of the two ciphertexts that relate to a decisive period for both the Portuguese and Dutch. At that time, they fought in the northeast of Brazil for the white gold of the 17th century: sugar.

2.1 Portuguese and Dutch Fighting for Sugar in Brazil

In 1630 the WIC conquered Recife and Olinda from the Portuguese General Government of Brazil. The Dutch occupied the northeastern region of Brazil for 24 years (1630-1654), including the heart of the sugar plantations in South America, the captaincy of Pernambuco.²

Things went rather smoothly for the Dutch until the sugar planters of Pernambuco revolted in 1645. A part of the inhabitants and the Portuguese administration followed suit. The Dutch were unable to win the battle against the “rebels” decisively, and because of that, the military offensive actions and defensive measures were costly. Next to that, the backup from The Netherlands was inadequate. The revolt of 1645 made the Dutch very suspicious of the Portuguese diplomatic movements. In 1641 both nations signed a ten years truce, which both sides ignored in the following years. In 1647, the Portuguese king authorized his ambassador in the Netherlands to negotiate two proposals: an offer to buy the territories of Dutch Brazil or, in case they refused, a proposal to pardon all the rebels, granting them a safe retreat to Bahia. The negotiations did not advance because the Portuguese and the Dutch were suspicious of each other's actions. On the one hand, the Dutch suspected the meaning behind the offer was to avoid or delay sending of military aid to Dutch Brazil. On the other hand, the Portuguese were always on alert and suspected new Dutch invasions in the Atlantic.

² The background information of Subsection 2.1 is based on Heijer den (2002), Knaap et al. (2015), and Roos (1992).



Figure 3: Map of the Atlantic ocean. Salvador, Bahia (1, Portuguese), Recife (2, Dutch), Alagoas (3) where *Nossa Senhora de Remédio* was captured. The hunting grounds of the *Directie Middelburg* is shaded (I).³

2.2 Brasile Directie Middelburg

A new company was founded next to the WIC in December 1646, the *Brasile Directie Middelburg*. The government in The Netherlands granted them the right, under strict conditions (Dutch: *provisionele conditien*), to capture enemy ships in time of war in the seas between Portugal, island Madeira, the Azores, and the coasts of Brazil and Africa. In return, the *Directie Middelburg* had to pay a share of their profits (Dutch: *recognitiegelden*) to the monopolist WIC. Article 1 of *provisionele conditien* defines that the privateers must make a report informing the name of the seized ship and its captain, a detailed list of guns, and crew of the prize ship. There is no mention of keeping and handing over letters and packing lists of the seized ships. Article 2 defines that the privateers should not attack Portuguese

³ It is unclear how far towards North America this area ran. *Provisionele Conditien* (1646) does not give a definitive answer on this. That's why question marks are put.

vessels on the anchorage of Portugal, Madeira, or the Azores. Article 7 indicates that all ships and goods seized should be delivered to the hands of the *Hoge Raad*. Three days after unloading, the *Hoge Raad* had to sell the prize ship and its cargo in cash and in public.⁴

In 1647 and 1648, the privateers (Dutch: *kaapvaarders*) captured, the vast majority by the *Directie Middelburg*, an estimated 220 Portuguese ships in the Atlantic. Half of these ships were bound for Portugal, negatively affecting the Portuguese maritime trade. Next to that, it also affected communication between the king of Portugal and the Brazilian part of his empire. As a countermeasure, from 1650 onwards, the Portuguese sugar ships sailed from Brazil in convoy and accompanied by 18 warships. The king also ordered Teles de Menezes (1647) that all relevant letters between the Crown and the general-government had to be encrypted.

The two ciphertexts taken on 1649-6-18 near Alagoas were carried by the ship *Nossa Senhora de Remédio*, who was not sailing under convoy. An accidental prey to a privateer on the watch. See Figure 3 for the location of Bahia (Portuguese), Recife (Dutch), and the hunting grounds of the *Directie Middelburg*.

2.3 Prisoner and Former Governor-General of Brazil António Teles da Silva

António Teles da Silva (1590-1650), governor-general of Brazil from 1642-1647, wrote the two ciphertexts while he was a prisoner. The king of Portugal ordered his imprisonment because he supported the revolt of Pernambuco in 1645. The king did not dare to openly support the rebels of Pernambuco because he was afraid of retaliation from the Dutch. But in secret, the Crown gave support to Teles da Silva, enforcing that officers had to follow his orders in this matter. When this became public in 1647, the king felt compelled to imprison Teles da Silva to appease

⁴ *Provisionele Conditien*, 1646.

the Dutch.⁵ A few years later, in 1650, Teles da Silva died in a shipwreck caused by a storm near the coast of Portugal, dying without receiving a Royal pardon.

2.4 The Two Ciphertexts

The ciphertexts contain two letters written in Portuguese. Teles da Silva wrote both letters from the capital of Brazil, the city of Salvador, in the captaincy of Bahia. The letters were addressed to the king of Portugal in Lisbon.⁶ See Table 2 for more details about the two letters: sender, receiver, and decrypter.

	Cipher 167 (Teles da Silva, 1649a1)	Cipher 168 (Teles da Silva, 1649b1)
Number of pages ciphertext	1.5	3
Inline cleartext	No	No
Number of pages cleartext after cipher	1.5	Only signature (3 lines)
Key	Available	Available
Date	1649-5-28 (not month 3)	1649-6-3 (not month 12)
Plaintext language	Portuguese	Portuguese
Sender name	Antonio Telles da Silvas	Antonio Telles da Silvas
Sender place	Baia, Brazil	Baia, Brazil
Receiver name	King of Portugal	King of Portugal
Receiver place	Lisbon, Portugal	Lisbon, Portugal
Encrypter	Unknown	Unknown
Decrypter	Unknown "a person with knowledge"	Unknown "a person with knowledge"
Content ciphertext	Governor-General has lack of care for defense issues	Disputes between military commanders. Threats of mutiny. Weakness of the Dutch
Content cleartext	Complaints of being arrested, being sick, and forgotten by the king	Signature

Table 2: The two ciphertexts.

We don't know who encrypted these two letters for Teles da Silva. A good candidate could be Bernardo Vieira Ravasco, who was the secretary of state of Brazil in 1649 and the right hand of the governor-general Teles de Meneses. On 1650-7-10, Teles da Silva (1650a) wrote a letter of recommendation for Ravasco to the king of Portugal. In this letter, he emphasizes the ability of Ravasco to decipher the king's ciphertexts.

2.5 Letter Dated 1649-5-28 from Teles da Silva to King

Summary of the content (Teles da Silva, 1649a1):
The new governor-general, António Teles de

⁵ In 1647 two pamphlets revealed that the king and his army supported the rebels of Pernambuco: *Kort Discours Rebelye* (1647) and *Claar Vertooch* (1647).

Meneses, stated to Teles da Silva that he would be happy if the Dutch captured him and took revenge because it would be instrumental for peace with Portugal. This letter also accused Teles de Meneses of neglecting the defenses, mismanaging the finances, and only be concerned with his private business.

In the cleartext, after the ciphertext, Teles da Silva complains to be forgotten and badly thanked by the king after being a prisoner for a year and a half, "becoming all grey and very sick".⁷ See Appendix 1, for the revealed plaintext of CT2 and Portuguese compared and a translation of the text into English.

2.6 Letter Dated 1649-6-3 from Teles da Silva to King

Summary of the content (Teles da Silva, 1649b1):
Teles da Silva informs that the soldiers were rioting and threatened to kill the Portuguese commanders Francisco de Figueiroa and Francisco Barreto because they did not receive proper rations and clothes. Pressured by the soldiers, Barreto paid the wages and provided clothes, becoming in debt to preserve the command of the troops.

Also, Teles da Silva declared to receive information about the feeble state of Dutch defenses, indicating that they could leave the forts in three months if they did not receive help from The Netherlands. He claimed to know that four hundred "useless Dutch" – injured soldiers and people coming from Angola – sailed to their homeland; he also received news that many Jews returned to The Netherlands with their wives. See Appendix 2, for the revealed plaintext of CT2 and Portuguese compared and a translation of the text into English.

⁶ Notice, that Teles da Silva writes his own name 'Telles' with 'll' and that 'Silvas' ends with 's'.

⁷ Teles da Silva (1649b2) mentions: "twenty months".

3 The Two Letters within the Administrative Process

This section shows the flow of information within the administrative process of the WIC.

3.1 Flow of Information in Dutch Brazil

On 1649-6-18, captain Bastiaen Thuijnman interrogated the skipper Pasquael Coelho and navigator Francisco Anes of the captured caravelle *Nossa Senhora de Remédio* (Thuijnman, 1649).⁸ They declared that they left from Bahia with 18 crew members (Dutch: *koppen*) with 150 crates of sugar and about 200 rolls of tobacco. They delivered all the letters they had on board to captain Thuijnman, and claimed not to be carrying letters from the governor-general to the king.

On the next day, 1649-6-19, captain Thuijnman from frigate (Dutch: *fregat*) *De Brack*, from the *Directie Middelburg*, reported to the *Hoge Raad* that he seized the *Nossa Senhora de Remédio* near Alagoas (Hoge Raad, 1649a). The *Hoge Raad* gave orders to interrogate the captured skipper and navigator and to examine and translate the letters. After that, the *Hoge Raad* ordered to dispatch these letters with the first ship sailing to The Netherlands since its content was considered worthy of attention.

On 1649-6-21, the *Hoge Raad* (1649b) registered in the daily minutes that, after reading the translations of the letters captured by Thuijnman, the content was considered relevant enough to be copied by the registry (Dutch: *griffie*) and had to send with other reports to The Netherlands in the first ship that departs.

The daily minutes of the *Hoge Raad* (1649c) registered on 1649-6-23 that they had read a translated report (Dutch: *missive*) found on the latest captured ship by captain Thuijnman. This report presented news from Angola since the Portuguese reoccupied it. This report also was

dispatched to The Netherlands, with a copy kept at the office (Dutch: *ten contoire alhier*) in Brazil.

The daily minutes of the *Hoge Raad* (1649d) registered on 1649-6-29 that the WIC bought, from the captured *Nossa Senhora de Remédio*, 20 rolls of tobacco. There is no mention of the remainder, 180 rolls of tobacco and 150 crates of sugar. Probably it was sold, together with the ship, in Middelburg, The Netherlands.

On 1649-7-23, the *Hoge Raad* (1649e) wrote to the Gentlemen XIX their periodic report (Dutch: *generale missieve*). In this report, under letter C, they listed the letters captured on the ship *Nossa Senhora de Remédio*. Some were in ciphertext (Dutch: *in cijffer geschreven*) and were deciphered (Dutch: *ontcijfferen*) by an unnamed person described as skilled in this task. The WIC officials translated the deciphered letters and the interrogation of the Portuguese prisoners into Dutch.

The Letterbook (1649) from the same day, 1649-7-23, registered under letter C, an original report found on a captured ship by captain Thuijnman and its translation. This report was written by the former governor-general Teles da Silva to the king of Portugal. The letters from Teles da Silva dated from 1649-5-28 and 1649-6-3 are in ciphertext (Dutch: *cijffer letters*). Next to these, the Portuguese revealed plaintexts, and their translations into Dutch are mentioned with their folio numbers.

We do not know whether the *Hoge Raad* themselves did anything – next to sending the reports to their superiors in The Netherlands and keeping copies of them – with the information contained in the two letters from Teles da Silva. There is no trace of this in the daily minutes nor their periodic reports. There is also no indication whether they passed on the information to Admiral Witte de With or whether it affected his military policy (With de, 1649).

⁸ Dutch spelling. ‘Pasquael’ is probably the misheard Portuguese name ‘Pascoal’. The ship has the name of

the catholic saint ‘Our Lady of Remedies’. In Portuguese it should read: *Nossa Senhora dos Remédios*.

3.2 Flow of Information between Brazil and The Netherlands

The package with letters, including ciphertexts 167 and 168, arrived in The Netherlands on 1649-9-20 (Letterbook, 1649). What did the Gentlemen XIX do with this information? Did it change their policy? We don't know if they talked about it in detail because there are no preserved (secret) minutes of this period.

On 1649-10-1, the Gentlemen XIX (1649) sent orders (Dutch: *missiven*) to the *Hoge Raad*, replying to their report of 1649-7-23. There is no mention of Teles da Silva or his ciphertexts. The Gentlemen XIX informed to be raising money from the government (Dutch: *Regeringe*) of The Netherlands to continue the conquest. They also declared the sending of ships, warships, and victuals to Brazil. There is a complete silence about the information received about the Portuguese. They must have regarded it as daily operational frictions among the Portuguese. This information had no impact on their strategy.

4 How Often Were Ciphers Used in the Portuguese Empire?

This section indicates when and where the use of ciphers occurred in the Portuguese Empire.

4.1 Use of Ciphers in Portuguese History

There is evidence of encrypted correspondences in Portuguese relations with the Ottoman Empire, dating from the 1550s.⁹

In a diplomatic context, the Portuguese ambassador in France exchanged ciphertexts with the king of Portugal between 1646 and 1649, the same period of the war in Brazil.¹⁰

Regarding the wars with the Dutch in Brazil, the governor-general Conde da Torre, who was in charge of an Armada sent to recover Pernambuco,

received in 1638 a cipher to use in transatlantic communication.¹¹

Another known example of Portuguese ciphers in this context is the report presented by Abraham de Pina (1646) to the *Hoge Raad*. De Pina explains the process he used to decipher several letters apprehended by the Dutch. João Vieira de Alagoas made the ciphertexts while he was a spy in Recife, pretending loyalty to the Dutch.¹² He ordered a "*mullato*" to deliver the ciphertexts to a rebel contact in the outskirts of Recife, but instead, he handed the letters directly over to the *Hoge Raad*. This event caused the imprisonment and torture of Vieira, who refused to deliver the key. Faced with the revealed content of the four deciphered letters, Vieira confessed that he had written the ciphers addressed to the rebels. He was tried and sentenced to the death penalty in a public execution.

4.2 Use of Ciphers in Portuguese Brazil 1645-1654

The archives of Portugal and Brazil do not have many ciphers concerning the wars in Brazil, specifically between 1645 and 1654. The only ones found so far are in the Dutch archives: De Pina's report (1646) and António Teles da Silva's (1649a1 and 1649b1) ciphertexts. See Table 3 for the ciphertexts that we found and records mentioning them. In Appendix 4, we provide more details about these sources.

Nr	Archive	Source	Sorting	Original year letter	Where
1	Portuguese	Teles da Silva, 1650b	mentions cipher	referring to 1642-1647	Seas
2	Dutch	Hoge Raad, 1646 Vieira, 1646 Kort Discours Rebelle, 1647	mentions cipher	1646	Land
3	Dutch	Pina de, 1646	ciphertext	1646	Land
4	Portuguese	Teles de Menezes, 1647	mentions cipher	1647	Seas
5	Dutch	Teles da Silva, 1649a1 Teles da Silva, 1649b1	ciphertext	1649	Seas
6	Dutch	Corea da Saa, 1649	mentions cipher	1649	Seas
7	Dutch	Dias, 1649	mentions secret communication	1649	Land
8	Dutch	Dagilaer, 1649	mentions cipher	1649	Seas
9	Portuguese	Teles da Silva, 1650a	mentions cipher	1649	Seas

Table 3: Ciphertexts in Dutch and Portuguese sources.

⁹ Couto, 2012.

¹⁰ Coelho, 1942.

¹¹ Torre, 1638.

¹² The daily minutes from 1646-5-16 (Hoge Raad, 1646) do not mention De Pina directly. They talk about

"a certain person from the jewish nation" (Dutch: *seker persoon van de joodse natie*). In future works, we will analyze the João Vieira de Alagoas' ciphertexts described in De Pina's report (1646).

We analyzed all 52 letterbooks (Dutch: *overgezonden lijste der brieven of papieren*) from the *Hoge Raad* between 1645 and 1654 to the Gentlemen XIX, chamber Zeeland, government, or simply to The Netherlands. In nineteen letterbooks (37%), we found mentions of intercepted letters, and only a couple of them mention ciphertexts. See Appendix 3 for the complete list of letterbooks and their content.

Based on the ciphertexts found and mentioned, we draw the following conclusions for Portuguese Brazil. The use of ciphers in long-distance communication became frequent after the heavy losses that Dutch privateers inflicted in 1647-1648 to the Portuguese shipping on the route from Brazil to Portugal.

The use of ciphers inside Brazil became frequent after the revolt of 1645. Luso-Brazilian spies sent ciphertexts to inform the rebel army about the state of fortresses and the WIC army. Therefore, these ciphertexts circulated in short-distance communication. In this sense, the use of cryptography by the Portuguese started after the Dutch structurally threatened their strategic military information and state secrets. On the other hand, this is also why the Dutch did not use cryptography in Brazil because they exerted control of the coastal towns and naval superiority in the South Atlantic. The Dutch control of the seas – they were king of the seas – assured the continuity of long-distance communication.

5 Ciphertexts and Keys

This section shows technical details about the used ciphertexts and their keys.

5.1 Technical Analysis

Cipher 167 is a **monoalphabetic substitution cipher**¹³ that replaces every plaintext letter with the same symbol of the ciphertext alphabet. Figure 1, in Section 1, shows the first four letters. Of the 26 letters of the Latin alphabet, the cipher used 20. The letters J, K, V, W, X, and Y are missing, with

no use of other symbols. See Table 4 for more details.

Cipher 168 is a **homophone substitution cipher**¹⁴. In this ciphertext, every plaintext letter is replaced with the same two to ten symbols of the ciphertext alphabet. Figure 2, in Section 1, shows the first four letters. Of the 26 letters of the Latin alphabet, the cipher used 21. The letters J, K, V, W, and Y are missing, with no use of other symbols. For the reconstruction of 15 codes, see Subsection 5.4.

Key symbols	Ciphertext 167. Count	Ciphertext 168. Count	Notes
Codes in key	20	71	
Code in key reconstructed	0	15	In 168 five mistakes and ten reconstructed codes.
Code symbols other not in key	0	0	
Total code symbols	20	86	
Latin letters A to Z in key	20	21	In 167 are missing: J, K, V, W, X and Y. In 168 are missing: J, K, V, W and Y.

Table 4: Symbols used in cipher 167 and 168.

Encrypting strategies not in key	Ciphertext 167. Count	Ciphertext 168. Count	Notes
Bigger numbers	Capital	Capital	
<i>U</i> can be read as ' <i>V</i> too	used	used	
<i>I</i> can be read as ' <i>J</i> too	used	used	
Punctuation marks	- (line), (dotted line), and (space)	- (line), ' (apostrophe), and (space)	
To confuse	spaces between words with(out)	spaces between words with(out)	In both ciphertexts many places where there is no space between words. This is especially clear in 168.
Hide accents	17	38	E.g. 'Nam' for 'Não'
Hide part of word	19	53	E.g. 'Gdor' for 'Governador' or 'Q' for 'Que'
Orthographical	3	22	E.g. 'Vosa' for 'Vossa' or 'Nosa' for 'Nossa'
Catchwords	not used	not used	

Table 5: Encrypting strategies not in key.

Of both ciphertexts, we have the original ciphertext (Teles da Silva, 1649a1 and 1649b1), revealed plaintext in Portuguese (Teles da Silva, 1649a2 and 1649b2) and translation into Dutch (Teles da Silva, 1649a3 and 1649b3). We compared the revealed plaintext from CT2 with the revealed plaintext in Portuguese. We also compared the Portuguese and Dutch texts with

¹³ Kopal, 2018: 30.

¹⁴ Kopal, 2019: 108.

English as their bridge language. See Appendix 1 and 2 for the details.

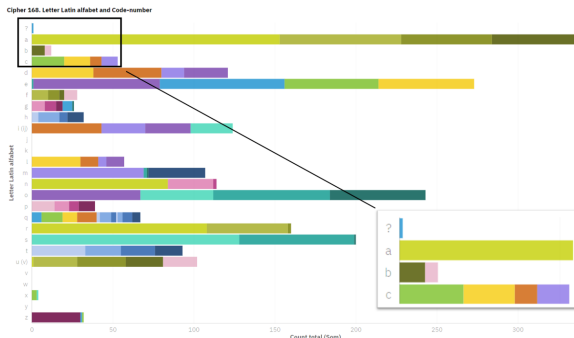


Table 6: The number-codes (in different colors) of cipher 168 are evenly distributed over the letters to make cryptanalysis harder.

Our analysis shows that the translations from Portuguese into Dutch are done correctly, with minor differences. The translator did not miss anything essential.

Our analysis also shows the use of a couple of encrypting strategies to make cryptanalysis more difficult. See the Table 5 for the complete list. For example: sometimes they deliberately do not use spaces; in general, they do not use accents and often use different spelling and abbreviations. On the other hand, one strategy made cryptanalysis easier: using bigger written numbers for capitals letters.

For making ciphertext 168, the encrypter probably used a separate piece of paper on which he kept track of how often he used codes. If we look at Table 6, we see the even distribution of the

codes (in different colors) used over the letters. This strategy made cryptanalysis harder.

Striking is that the key of cipher 168 is more complex than that of cipher 167, once they were made only six days apart. What conclusion should we draw from this?

5.2 Jewish Cryptology Specialists in Dutch Brazil

Who did the cryptanalysis and was thus able to decipher the two ciphertexts? Based on the found and mentioned ciphertexts, see Table 3, we have two suitable candidates: Moyses Raphael Dagilaer and Abraham de Pina. Both were Jews of Iberian origin who lived in Recife after the Dutch conquest and acted as rabbis. They served as cryptanalysts for the *Hoge Raad* on previous occasions. Jütte (2015) demonstrates how Jews served as cryptanalysts in Europe, especially emphasizing the role of scholars in the use of cryptography. Therefore, we suggest that these particular Jews acquired the knowledge of cryptanalysis before they came to Dutch Brazil. We haven't found out yet how these men learned how to decipher. Some factors could help us get closer to understanding this situation. The proximity they had with the Portuguese through the shared language and culture could be one of the elements. Also, the social function of secrecy¹⁵ was used by these particular Jews. They employed the knowledge of cryptography as a way to improve their relations and their business with the Dutch in Brazil.

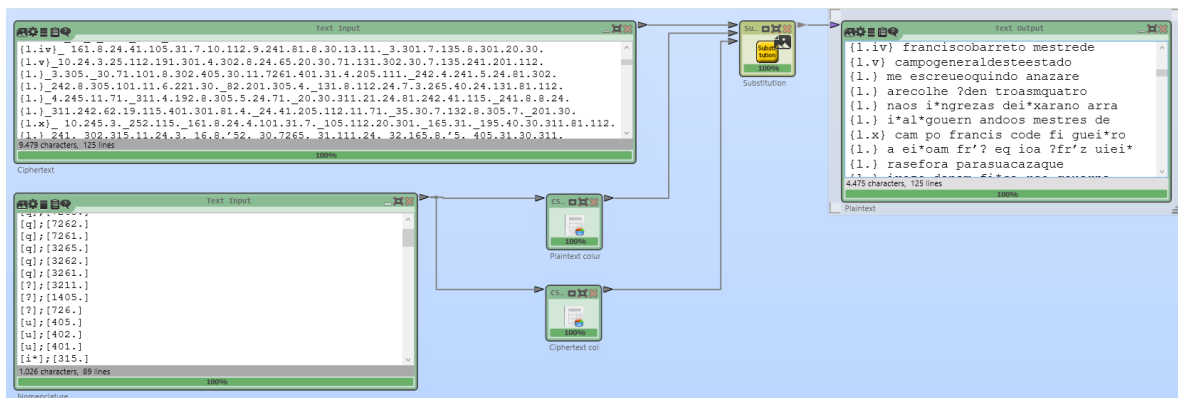


Figure 4: CT2 substitution component deciphering the 168 ciphertext using the digitized key.

¹⁵ Jütte, 2015.

5.3 Has there been a Loss of Knowledge and Skills since 1640?

Also striking is that neither the cipher 167 nor 168 contain nomenclature elements as the ones used by Conde da Torre (1638). See Figure 5.

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q
x	u	t	z	r	q	s	p	a	o	b	i	c	y	d
Sua Magestade	-----	E	Terra	-----	☞									
Governador geral do Brasil	-----	C	Mato	-----	↑									
Mestre de campo	-----	B	Engenho	-----	☞									
Sargento mor	-----	A	Canaviais	-----	⊙									
Capitão	-----	D	Açucares	-----	☐									

Figure 5: Part of the cipherkey that Torre (1638) used with nomenclature elements.

A question emerges: did the cryptographic skills diminish from Portugal since it broke with Spain in 1640? Could this be the reason why the ciphers of 167 and 168 are simpler than the ones used by Conde da Torre? Future works should develop this question about the impact of the end of the Iberian Union on Portuguese cryptography.

5.4 Generating Plaintext with CrypTool 2

We have the keys of both ciphertexts, which appears in the manuscripts, and assumed that both were substitution ciphers. Therefore, we entered the key manually into CT2. With the help of the substitution component, we were able to decipher most parts of the ciphertexts correctly. The output of cipher 167 was almost flawless from the start.

The cipher 168 was challenging since we had to reconstruct fifteen codes unaccounted in its key. Five of them were code mistakes made by the encrypter, and these mistakes were not repeated throughout the ciphertext. A mistake, for example, is the code 215 instead of 205 for letter *E*. We reconstructed ten of the codes because they fit into the used key-strategy ‘first number, +1, +2, and +5’. For example, the key of the letter *M* reads ‘3, 35’ but the reconstructed code reads ‘3, 31, 32 and 35’. The unaccounted code 32 fits into this strategy. See Appendix 2 for the complete list of unaccounted for codes of cipher 168. Based on this, we suggest that the mistakes indicate that this deciphering process was made without the original key, through cryptanalysis. After that, the

decoder was able to fill the remaining codes. This conclusion probably was drawn from the obtained Portuguese plaintext and not through the final version of the key.

CT2 provided great help with reconstruction step-by-step of a key with codes unaccounted. The software facilitated the recurrent uploading of the nomenclature and the visualization of the results in plaintext. Are all codes resolved? Are the words still meaningful? See Figure 4 for the ciphertext 168 in CT2, the nomenclature, and the revealed plaintext.

6 Conclusions

Our main findings have been:

1) The plaintexts of the deciphered ciphertexts reveal two letters that, in retrospect, were already known in the National Archives as plaintext Portuguese letters. We relate them and their translation into Dutch held in the same archive.

2) After cryptanalysis, the decrypter revealed both ciphertexts. In the case of cipher 168, the key obtained was sufficient to read enough of the plaintext. Ten codes were unaccounted for in this key. The decrypter reconstructed those codes, as is shown in the revealed plaintext but didn’t process them in the final version of the key.

3) The encryption process used the key and additional steps to make cryptanalysis harder. For example, the code sometimes does not leave spaces between words and the use of abbreviations. But there was also one element that made cryptanalysis easier: using bigger written numbers for capitals letters.

4) It’s a fact that cipherkeys were provided in Portuguese Brazil, at least from 1638 onwards, for communicating about strategic military information or state secrets. Ciphers were used by the Portuguese mainly after the Dutch structurally threatened their communication. In short-distance communication, they became frequent after the revolt of the sugar planters in 1645. The use of ciphers in long-distance communication increased after the Dutch privateers compromised the

Portuguese shipping between 1647 and 1648, notably from 1649 onwards.

5) The Gentlemen XIX did not do anything with the strategic military information and state secrets found in the two deciphered letters of Teles da Silva. The orders sent by the Gentlemen XIX after receiving the information from Dutch Brazil show that they did not use the seized information.

References

- Claar Vertooch. 1647. Anonymously, *Claar Vertooch van de Verradersche en Vyantlijcke Acten en Proceduren van Poortugal, In 't Verwecken ende Stijven van de Rebellie ende Oorloghe in Brasil*.
- Corea de Saa, 1649. 1649-7-4. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 65-171, under number 6: unfoiled. 1649-11-29. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 65-154, under letter T: unfoiled.
- Dagilaer, 1649. 1649-12-31 and 1650-1-18. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 74: unfoiled, scans 109 and 174.
- Daniel Jütte. 2015. *The Age of Secrecy. Jews, Christians, and the Economy of Secrets, 1400-1800*: 8-11, 26-27, 56-60.
- Dejanirah Couto. 2012. 'Spying in the Ottoman Empire: sixteenth-century encrypted correspondence'. *Correspondence and Cultural Exchange in Europe, 1400-1700. Cultural exchange in early modern Europe*: 274-312.
- Dias, 1649. 1649-11-28 and 1649-12-03. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 73: unfoiled, scans 1260-1262 and 1288-1291.
- Doeke Roos. 1992. *Zeeuwen en de Westindische Compagnie*: 69-77.
- Gerrit Knaap, Henk den Heijer and Michiel de Jong. 2015. *Oorloggen Overzee: Militair optreden door compagnie en staat buiten Europa 1595-1814*: 289-295.
- Henk den Heijer. 2002. *De geschiedenis van de WIC*: 65-68.
- Hoge Raad, 1646. 1646-5-16, 1646-5-19, and 1646-5-28. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 71: unfoiled, scans 420, 421, 426 and 437.
- Hoge Raad, 1649a. 1649-6-19. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 73: unfoiled, scans 680-681.
- Hoge Raad, 1649b. 1649-6-21. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 73: unfoiled, scan 681.
- Hoge Raad, 1649c. 1649-6-23. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 73: unfoiled, scans 688-689.
- Hoge Raad, 1649d. 1649-6-29. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 73: unfoiled, scans 712 and 771.
- Hoge Raad, 1649e. 1649-7-23. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 65-105: ff240-241.
- Kort Discours Rebelle. 1647. *Journael ofte kort Discours nopende de Rebelle ende verradelijcke Desseynden der Portugesen, alhier in Brasil voorgenomen, 't welck in Junio 1645 is ontdeckt*.
- Gentlemen XIX, 1649. 1649-10-1. NL-HaNA, OWIC, 1.05.01.01, kopieboeken van uitgaande stukken, 10 1646 juli 21 - 1657 okt. 10: ff64-68.
- Letterbook, 1649. 1649-7-23. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 65-107: unfoiled.
- Nils Kopal. 2018 'Solving classical ciphers with CryptTool 2'. *Proceedings of the 1st International Conference on Historical Cryptology HistoCrypt 2018*. No. 149: 29-38.
- Nils Kopal. 2019 'Cryptanalysis of homophonic substitution ciphers using simulated annealing with fixed temperature'. *Proceedings of the 2nd International Conference on Historical Cryptology HistoCrypt 2019*. No. 158: 107-116.
- Pina de, 1646. 1646-5-??. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 62-44: unfoiled.
- P.M. Laranjo Coelho. 1942. *Cartas de El-Rei D. João IV Ao Conde da Vidigueira (Marquês de Niza) Embaixador em França*.
- Provisionele Conditien, 1646. Zeeuws Archief, Middelburg (MdbZA), 1.4.10.1., 2118. Letter from 1646-12-06, unfoiled, scan 366-370.
- Teles da Silva, 1649a1. 1649-5-28. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 65-167: ff146-147.
- Teles da Silva, 1649a2. 1649-5-28. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 65-88: f140.
- Teles da Silva, 1649a3. 1649-5-28. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 65-59: f139.
- Teles da Silva, 1649b1. 1649-6-3. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 65-168: ff142-143.
- Teles da Silva, 1649b2. 1649-6-3. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 65-89: f145.
- Teles da Silva, 1649b3. 1649-6-3. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 65-90: ff141.
- Teles da Silva, 1650a. 1650-7-10. AHU_ACL_CU_005-02, Cx. 14, D. 1702.
- Teles da Silva, 1650b. 1650-7-19. Virgínia Rau. 1984. 'Fortunas Ultramarinas e a nobreza portuguesa no século XVII'. In: José Manuel Garcia. (Ed.) *Estudos sobre história econômica e social do Antigo Regime*: 36-46.
- Teles de Menezes, 1647. 1647-8-10. BNRJ-SM, 08,01,016. No 002.
- Thuijnman, 1649. 1649-6-18. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 65-97: ff154-155.
- Torre, 1638. João Paulo Salvado, Susana Münch Miranda. *Cartas do Primeiro Conde da Torre (volume II)*. 2001: 32-33.
- Vieira, 1646. 1645-05-29. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 62-43: unfoiled.
- With de, 1649. 1649-4-24 to 1649-7-31. NL-HaNA, OWIC, 1.05.01.01, inv.nr. 65-69: ff209-226.

APPENDIX 1: Ciphertext 167 from 1649-5-28

RESOLVED PLAINTEXT CT2 (CIPHERTEXT) AND PORTUGUESE PLAINTEXT COMPARED

INDEX COLORS. Grey = in ciphertext not in Portuguese; Yellow = in Portuguese not in ciphertext; Blue = differences in used letters e.g. 'i' versus 'e' (different written letters) or 'S' versus 's' (capitals).

Space is ' _ '.

{1.iii} Sabendo os Olandezes por zer selim¹⁶
{1.} que estava prizonheiro nesta prasa e o C
{1.v} onde o soltou por seu gosto contradi
{1.} zendo lho todos por quanto¹⁷ eu estava
{1.} para ir em huas naos ingrezas; se resol
{1.} ueram a uir me buscar com a sua Capi
{1.} tanta e seis naos dos estados; a esta ba
{1.x} rra, onde andam ha dias, e dizendo o ao C
{1.} onde q nam conuinha dar este capitam o
{1.} landes por muitas razois apontandolhe que
{1.} estava eu para partir, e que o iria¹⁸ dizer e
{1.} me ueriam esperar como uieram; respon
{1.xv} deo o conde que se me tomasem seria muit[o]
{1.} bom porque se uingariam os olandezes de
{1.} mim, e logo fariam pazes com portugal, o
{1.}
{1.} tomarem me nam quis deus dar esse gosto
{1.xx} ao conde, mas tememos q uenha o conde de
{1.} castel melhor dar em suas maos, epodendo ha
{1.} uer preuensois dos nauios que aqui estam
{1.} para o dito conde castel melhor ser so
{1.} corrido; o governador se lhe nam da nada, antes
{1.xxv} folgara, porque so atende a que este estado se
{1.} perca como he uender tudo, dar lic
{1.} enca a todos que se uam, leuar todos os ar
{1.} telheiros; tirar a artelharia que estava
{1.} para as fortificasois; e todo o dinhei
{1.xxx} RIJKSARCHIEF'S-GRAVENHAGE
{1.} ro que esta por uenser o gasta de maneira
{1.} que o nouo governador que uem, he forsa que tenha c
{1.} om elle grandes desauensas, por mais sof
{1.} rido que seja, acuda sua magde a isto co
{1.xxxv} mo lhe pareser melhor tomando as infor¹⁹
{1.} masois todas q lhe pareser- aarmada esta
{1.} incapas²⁰ para o que se quizer fazer delas, por²¹
{1.} que como sua magde mandou fazer pres

¹⁶ 'Zerselim' or 'Zer selim' is not a Dutch word. It's written with a Capital in the Portuguese plaintext. Probably a person's name, in this case of some prisoner of the Portuguese.

¹⁷ Ciphertext: 131. In Portuguese text: q. Hence code should have been: 13.

¹⁸ Ciphertext: 'o iria'. Portuguese: 'oiria'. Probably 'oiria' refers to a Spanish word that means 'he has heard', like Portuguese 'ouvira'.

¹⁹ Ciphertext: ? (unreadable). In Portuguese text: r.

²⁰ This sentence is not in the Portuguese plaintext. Mistake by the decrypter.

²¹ Ciphertext: ? (unreadable). In Portuguese text: r.

{1.} tes capitania e almirante, so delas²²
{1.xxxx} [f.146v]
{1.xxxxi} se trata, as mais nam dam cuida do, e so o
{1.} tem em meter muita fazenda na capi
{1.} tania de pau de facaranda misturado
{1.} com pau de brazil e outras muitas
{1.xxxxv} couzas que sam publicas se as quize
{1.} rem saber-

O Seguinte estava por letra²³

{1.} e quando não com a diser satisfaso, anno
{1.} e meio ha, que estou prezo vendo todos as dias entregar me
{1.} hum sargento a outro, com as ordens que tenho escrito e mandado
{1.1} sertidois, e quando me veio tão matratado por caia causa
{1.} estou todo branco e muy doente, não sinto meos trabalhos
{1.} senão perder sua Magde hum vasalo que tanto amava
{1.} seu serviço, e tão zeloso era dele, bem curo²⁴ que isto he lo
{1.} cura mas esta durara em mim sempre, ainda que vejja
{1.lv} quam mal se me agradece, pois vendo sua magde o estado em que
{1.} ficava tão mal o remediou, e do conde não tenho queixa,
{1.} pois obrou com forme seo ioiso, mas sua magde vendo
{1.} tão bombaria²⁵ com sem tila²⁶ he muito para a sen
{1.} tir,
{1.lx} muito tempo ha que não tenho carta vossa, vindo algu
{1.} mas en barcasen is²⁷, de presento veio, sebastião
{1.} vas, e não tive carta vossa nem de ninguem: todos nesta
{1.} ocasião me largaram, assim o em xergei²⁸ nas poucas
{1.} delinnsias²⁹ que se fizeram com sua magde e tenho eu
{1.lxv} resposta do dito señor a não tive vossa, nem de mui
{1.} tos que escrevi que sei que são chegadas, como vos
{1.} tenhais saúde, acostumado sou eu, certas for
{1.} tunas, de 11 de abril temos novas de essa sidade
{1.} e, como não avia novas da partida de castelo melhor,
{1.lxx} ficaram as naos para o anno que vem, com agla³⁰
{1.} ficarei fazendo, oi tres annos de prizam,
{1.} _147_[f.147r]
{1.lxxiii} e de estar no brazil, oito, e o mais serto he ficar nello que he,
{1.} o que os ministros pertendem, as novas maes de esta
{1.lxxv} baia, não faltara quem as de, guarde vos deos
{1.} como dezeio, baia em 28 de maio de [1]649

²² Ciphertext ‘des?’ (partly unreadable). Portuguese ‘delas’.

²³ This sentence is not in the ciphertext. Added by the decrypter. After this line the text is in Portuguese cleartext.

²⁴ Ciphertext ‘curo’ (English: I heal). Portuguese ‘veijo’ which is the orthographically incorrect form of ‘veja’ (English: ‘I see’). ‘I heal’ doesn’t make sense in this context.

²⁵ Ciphertext ‘bombaria’ (English: a batch of bombs). Portuguese ‘zombaria’ (English: mocking). ‘A batch of bombs’ doesn’t make sense in this context.

²⁶ Ciphertext ‘com sem tila’. Portuguese ‘consetila’. Both words are in English: to consent.

²⁷ Ciphertext ‘en barcasen is’. Portuguese ‘embarcaois’. Orthographically incorrect form of ‘embarcações’ (English: vessels).

²⁸ Ciphertext ‘emxergei’. Portuguese ‘enxergei’. Both words are in English: ‘I can see’.

²⁹ Ciphertext ‘delinnsias’. Portuguese ‘deligencias’ (English: proceedings or preparations for an event). Probably the encrypter made a mistake when he wrote ‘delinnsias’.

³⁰ Ciphertext ‘agla’. This could be an abbreviation for Portuguese ‘aquela’ (English: that one). Portuguese ‘que’ (English: what) makes more sense because it’s about how much time Teles da Silva already has been in Brazil.

{1.} estava assinado Antonio Telles da Silva

PORTUGUESE AND DUTCH TEXTS COMPARED WITH ENGLISH AS BRIDGE LANGUAGE

INDEX COLORS. Blue = differences in used words; Grey = in Dutch not in Portuguese; Yellow = in Portuguese not in Dutch.

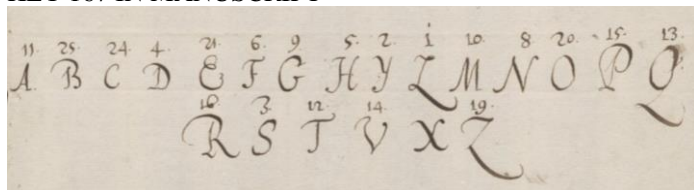
So the Dutch know by zerselim that I was a prisoner in this square (by hostage-taking and the Count released him for his pleasure contradicting everyone because I was here ready to leave with the English ships); they decided to come for me, to look for me, with his admiral and six ships of the States, to here, where they have been for days. And saying to the Count beforehand that it was not convenient to hand over me to this Dutch captain for many reasons, pointing out to him that I was about to leave, and that he himself would reveal and that they would observe my arrival just as they did; the Count replied to this that if the Dutch took me it would be very good because they would avenge the Dutch on me, and would hit peace with Portugal. But taking me, God did not want nor to give this pleasure to the Count, but we fear that the Count of Castelo Melhor will come into their hands, and there could be preventions of the ships, that are here for repair, are here to help the said Count of Castelo Melhor in case of emergency; the Count does not mention it, he rather neglect it. Because he only cares that this city loses everything, as one can perceive, like selling everything, giving permission to all who are going, taking all the constapels; take away the artillery that was for the fortifications, and all the money that is still to be due, he spends in such a way that the new Count who is being expected, is bound to have big disagreements with him, however meek he may be. Assist His Majesty in this as he see fit by taking the information for what is to be done with it after thinking carefully himself. As His Majesty ordered to make ready the admiral ship and the vice-admiral ship, he concerns only with these two, the others are not mentioned and he only takes care of by putting many goods in the admiral ship of jacaranda wood and brazilwood and many other things that are public if one wishes to know them. I comply with this

What comes next was in writing.

And when I don't say it I satisfy myself. I have been in prison for a year and a half, seeing one sergeant hand me over to another every day, with such orders that I have written and next to the sent certificates, and when I find myself so ill-treated, because of which I am all grey and very sick, anyway I feel mischief but to lose His Majesty a vassal who loved his service so much, and was so zealous of it. I clearly see that this is madness, but still the same year, it will last in me forever, even if I see how badly I am thanked. Seeing his Majesty the state in which I was, so very badly remedied it. And I have no complaint about the Count, for he acted according to his intellect, but His Majesty, seeing such a mockery³¹, consenting to it is too much is very difficult for me. It's been a long time since I've had a letters from you. As yet some ships had come, presently Sebastian Vas came, and I have had no letters from no one. All have left me on this occasion, as I have noticed seeing in the few proceedings that have been taken for me to His Majesty, and I have an answer from the aforementioned Lord and I have not had a letter from you, nor many that I have written that I know that they were received. If only you are in good health, accustomed am I, to these certain fortunes. From April 11 we have news from over there, and as there was no news of Castelo Melhor's departure, so the ships will have to stay moored until next year, and will I have to remain in prison for more years after I've been already three years of imprisonment, and of being eight in Brazil, and they think that most certain I'll stay forever, which is, what the ministers intend, the more news from Bahia, there will be no lack of those who will have written, may God preserve you as I wish.

Bahia on May 28, [1]649. It was signed Antonio Telles da Silva

KEY 167 IN MANUSCRIPT



³¹ Dutch reads 'burteneij'. Unknown word in Dutch. We follow the Portuguese translation and assume that it must signify 'mockery' (Dutch: bespotting, aanfluiting).

APPENDIX 2: Ciphertext 168 from 1649-6-3

RESOLVED PLAINTEXT CT2 (CIPHERTEXT) AND PORTUGUESE PLAINTEXT COMPARED

INDEX COLORS. Grey = in ciphertext not in Portuguese; Yellow = in Portuguese not in ciphertext; Blue = differences in used letters e.g. 'i' versus 'e' (different written letters) or 'S' versus 's' (capitals).

Letters with * are reconstructed letters.

Letters with ! are improved code errors.

Space is ' _ '.

Señor

{1.iv} francisco_barreto mestre_de
{1.v} campo_general_de_este_estado
{1.} me escreueo, que vindo a nazare,
{1.} a recolhe_r*_den_tro, as_m_quatro
{1.} naos i*ngrezas dei*xara_no arra
{1.} i*al*go_uern_ando os mestres de
{1.x} cam_po francis_co_de fi_guei*ro
{1.} a e_i*oam fr*z*, e que ioam*fr*z, uiei*
{1.} ra, se fora para sua_caza que
{1.} ixozo de_nam fi*ca r_so gouerna
{1.} ndo, e que_logo socedera, amoti*
{1.xv} narens e os soldados q!uerend_o
{1.} matar_a francisco de fig!uei*roa
{1.} e que_o_mesm!o! hauiam de_fazer ao
{1.} mestre de_campo_general, pois_l*
{1.} hes na` daua a_racam e_fardas,
{1.xx} tendo_o_i*tenta mi*!*_cruzadom e
{1.} si*nco mil* fardas, q`ue uossa magestade
{1.} nas di*tas naos i*ngrezas manda
{1.} ra, e_q`ue_nam_queriam_outro_gou
{1.} ernador sen*a` i*oam fr*z, ui*eira,
{1.xxv} o_qual de_sua_caza_tin*ha ac
{1.} odido_a_aqui*etar os sol_dad
{1.} os prometendo l*hes tudo_quan
{1.} to elles pedi*am, av!izando_a_na
{1.} zare ao_mestre_de_cam_po_genera
{1.xxx} l*_q`uez_fosse logo para_o_arraial; o
{1. RIJKSARCHIEF 'S-GRAVENHAGE
{1.} qual teue outro aui*zo ne_o_u
{1.} tras pessoas_que_na`_fosse porque o_qx
{1.} uer_i*am³² de matar no_no_cami*nho, e_por
{1.xxxv} esta_ca_uza_na` foi*, mas mando In
{1.} ao_mestr*e de_campo andre_uid
{1.} [f142v]
{1.xxxviii} al, q`ue_estau a em napare q`ue fosse a
{1.} qui*etar os_soldados l*euondo os ca
{1.xxxx} rregasoi*s do_q`ue uinha_nas naos in
{1.} grezas para_q`ue uis*em os solda_dos
{1.} q` tudo o_q`ue cuida_uam ui*nha_nas n

³² Ciphertext: qx uer iam (or without spaces: qxueriam). In Portuguese text: avião de?

{1.} aos, hera aleu^{antado} pel*os e
 {1.} mulos do di*to m^{estre} de cam*po
 {1.xxxxv} gener^{al}, mas nada bastou pa
 {1.} ra os aqui*etar, e ui*ol enta
 {1.} men*te fi*z eram com q'z se l*hes de
 {1.} sem a qu^{atro} mi*I rei*s, e oi*to ce
 {1.} ntos reis a ca^{da} solda^{do}?³³, q'ue dis
 {1.1} francisco barr^{eto} q'ue nam sabe don^{de}
 {1.} os ha de ti*rar mas i*ase³⁴ cont
 {1.} i*nuando em lhos dar, eq'ue hua'
 {1.} co^m panhi^a de i*oam fr'z uiei*r
 {1.} as q'ue estaua em naz^{ar}e, se l*eu a
 {1.lv} ntara para i*r para o^{mal}to; mas
 {1.} o m^{estre} de campo general*os a
 {1.} quietara dando l^{hes} loguo su
 {1.} as fardas, di*sm q'ue o ini*mi*go e
 {1.} sta em tal esta^{dos} q'ue namz tem
 {1.lx} com q'ue possa sahi*r fora, e q'ue pa
 {1.} ra olanda parti^{am}?³⁵ quatr
 {1.} o centos olandez^{es} i*nutei*s,
 {1.} assi* dos q'ue uieram de angola, c
 {1.} omo os q'ue estaua o estropea^d
 {1.lv} os, das sahi*das q'ue hau^{am} fe
 {1.} i*to, e q'ue foram mui*tos iudeus c
 {1.} om suas mol*heres di*zendo os r
 {1.} endi*dos q'ue sahi^{ao} q'ue hera p
 {1.} ratⁱ*ca entre os soldados q'ue
 {1.lxx} se dentro em tres mezes lhes
 {1.} nao' uier socorro de ol*anda ha
 {1.} ui*ao' de largar as for^{sas}, e q'ue
 {1.} i*ndo os ol*andezes ao si*ara por
 {1.} terem noti*sia q'ue hau^a mi*n^{as}
 {1.lxxv} de ouro, os indi*os der^{ao} nelles
 {1.} e os matarao' todos e na'o escap
 {1.} 143[f143r]
 {1.} an^{do}?³⁶ mai*s q'ue dous q'ue trouxe
 {1.} rao' as nouas e q'ue as naos dos
 {1.lxxx} estados com o poder q'ue tinh
 {1.} ao', andauam nesta barra d
 {1.} esta bahi*a esperandome a
 {1.} mi*m por noti*s i*as q'ue ti*rham q'ue
 {1.} eu hia, como tambem ao conde
 {1.lxxxv} de castel melhor- esta he
 {1.} senhor a sustansi*a da carta
 {1.} de francisco barret^o a qual* t
 {1.} anto q'ue a recebi* a mandei* por
 {1.} luis da si*lua telles, ao cond
 {1.xc} e de ui*I*a pouca, por elle nao't

³³ Code '1' in ciphertext. No letter needed in Portuguese plaintext, hence '?'.

³⁴ Ciphertext: iase. In Portuguese tekst: chase.

³⁵ Unreadable in ciphertext, hence '?'. Letter 'r' needed in Portuguese plaintext. This is code '8' or '81'.

³⁶ Ciphertext: escapando. In Portuguese tekst: escaparão.

{1.} er, notisi*as tao_mi*udas do s
 {1.} uceso, e_se para a_rezo_lus_am
 {1.} q_ue se tomasse, fosse necessario_d
 {1.} ar eu_algu_ma_info_rmasao*_ou
 {1.xcv} parecer, me!_oferesi*, por q_ue_so
 {1.} me lembrava o_ser_uiso_de_u
 {1.} ossa_magestade, e_me esquei*a
 {1.} estar prezo_ha_uinte_mezes,
 {1.} entregue_a_hu_m_sargento_de
 {1.c} mi*m_ nao*_qui*zeram saber nada,
 {1.} nem_q_ue eu_soubese a_rezolutam
 {1.} q_ue_se_tom_aaa, quei*ra_deus_q_ue
 {1.} sei*a_a_q_ue_conuem ao_serui*s_o
 {1.} de_uossa_magestade_q_ue_heso³⁷ he o_qu
 {1.cv} e_dezeio_q_ue se acerte- guarde de nosso
 {1.} Srde³⁸ a_Catolica real pessoa de_vossa_magestade como
 {1.} a_Cristandade e_Seos_vassalos avemos
 {1.} mister_baia em 3 de_uinho³⁹ de [1]649
 {1.} [Watermark: three-leaf or trefoil with letter GP or CB]
 {1.cx} Antonio Telles
 {1.} da Silvas

PORTUGUESE AND DUTCH TEXTS COMPARED WITH ENGLISH AS BRIDGE LANGUAGE

INDEX COLORS. Blue = differences in used words; Grey = in Dutch not in Portuguese; Yellow = in Portuguese not in Dutch.

Lord

Francisco Barreto, General Field Marshal of this city wrote me, that when he came to Nazare, to collect the four English ships, he left governing the in the Arrajal, the Field Marshals Francisco de Figueiroa and Joan Fernandes Vieira and that Joan Fernandes Vieira went to his house complaining that he would not be the only one governing and that soon followed by the rioting of the soldiers wanting to kill Francisco de Figueiroa and that they would do the same to the General Field Marshal, because he did not give them the rations and cloths, having eighty thousand crusados and five thousand cloths, that Your Majesty had sent in the English ships. And saying that they wanted no other governor but Joan Fernandes Vieira, who came from his house had helped to calm the soldiers by promising them everything they asked for, writing to the General Field Marshal in Nazare to go to the Arrajal; who had another warning from other people not to go because they would kill him on the way, and for this reason he didn't go but sent to the Field Marshal Andre Vidal, who was also in Nasare, to calm the soldiers by taking the delivery notes with him of that what was coming in the English ships to show, so that the soldiers could see everything that they cared about that was coming in the ships, it was only a decoration, someone-who-begrudges⁴⁰ of the General Field Marshal. But nothing was enough on the contrary and they violently made them give four thousand reis, and eight hundred reis to each soldier, which Francisco Barreto says he doesn't know where to get that money from but he still keeps on continuing to give to them. And that a company of Joao Fernandes Vieira that was in Nazare mutinied and wanted to go into the woods, but the General Field Marshal had calmed them down by giving them some cloths. They says that the enemy is in such a state that they have no power of getting out of the field. And that four hundred useless Dutchmen left for Hollanda, both those who came from Angola and those who were crippled from the exits they had made. And that many jews with their wives went, the defectors

³⁷ Ciphertext: heso. In Portuguese text: isso. Both in English: that.

³⁸ Ciphertext: Srde. In Portuguese text: S.or. Both are an abbreviation of 'Señor' (English: Lord or Sir).

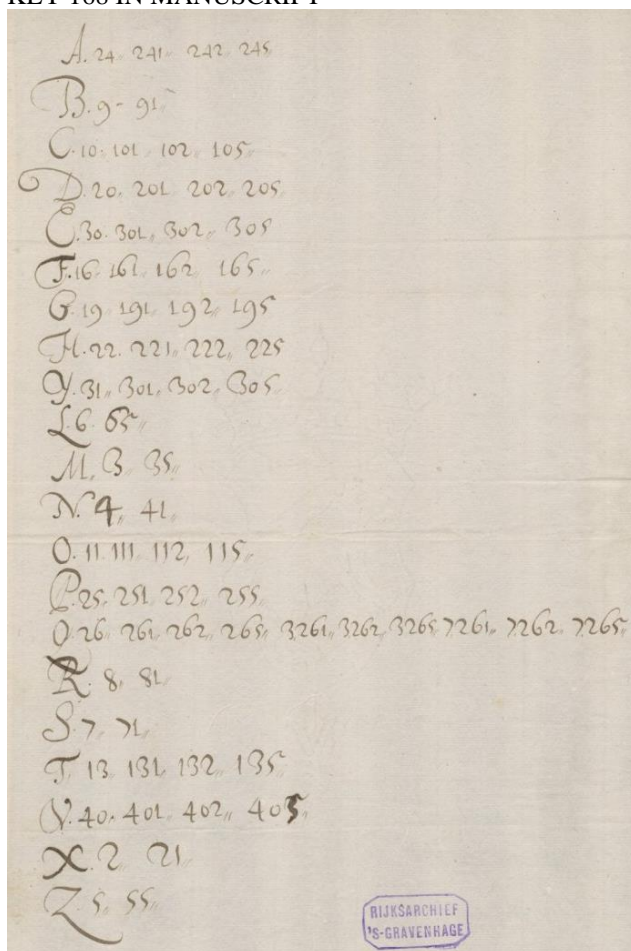
³⁹ Ciphertext: uiho. In Portuguese text: Junho. Both refer to the month 'June'.

⁴⁰ Dutch 'misgunnen'. Translation: begrudge, thinking that someone shouldn't get something. Dutch 'aemuleren' (English: emulation). A 'rival' is an 'aemulus' in Latin.

declare that among the soldiers is said that if no help came from Holland within three months, they would leave the fortresses⁴¹. And that when the Dutch came to siara because they had news that there were gold mines, the brasilians attacked them and killed them all and only two escaped, who brought the news. And that the ships of the States with the power they had were near this harbour waiting for me, for they heard the news that I was going to leave thither, as well as to the Count of Castelo Melhor. Lord this is the substance of Francisco Barreto's letter which as soon as I received it I sent (by Luis da Silva Telles) to the Count of Vila Rica, because he had no news so small of the success and if for the resolution that was taken, it was necessary for me to give some information or opinion, I offered myself, because I only remembered Your Majesty's service, and I forgot myself that I had been in prison for twenty months, in the care of a sargeant. They did not want to know anything about me, nor did they want me to know the resolution that was to be taken; may God grant that it be the one that is convenient for Your Majesty's service, for that is what I wish to be done, may God take care the royal Catholic person of Your Majesty, alike Christendom and His vassals must.

Bahia on June 3, [1]649. And it was signed Antonio Telles da Silva.

KEY 168 IN MANUSCRIPT



CODES IN CIPHER 168 NOT ACCOUNTED FOR IN ITS KEY

Nr	Code (count) mistake by crypter
1	215 (1) instead of 205 for E
2	219 (1) instead of 292 for G
3	726 (1) instead of 7261 (or 7262 or 7265) for Q
4	1405 (1) instead of 405 for V
5	3211 (1) instead of 32+11 for M+O

⁴¹ Portuguese reads 'forças' (English: forces). Dutch reads 'fortressen' (English: fortresses).

Nr	Reconstructed code (count)
1	32 (2) for M fits in used key-strategy +1, +2, and +5
2	45 (2) for N fits in used key-strategy +1, +2, and +5
3	52 (1) for Z fits in used key-strategy +1, +2, and +5
4	61 (11) for L fits in used key-strategy +1, +2, and +5
5	62 (5) for L fits in used key-strategy +1, +2, and +5
6	72 (1) for S fits in used key-strategy +1, +2, and +5
7	82 (2) for R fits in used key-strategy +1, +2, and +5
8	311 (27) for I fits in used key-strategy +1, +2, and +5
9	312 (28) for I fits in used key-strategy +1, +2, and +5
10	315 (26) for I fits in used key-strategy +1, +2, and +5

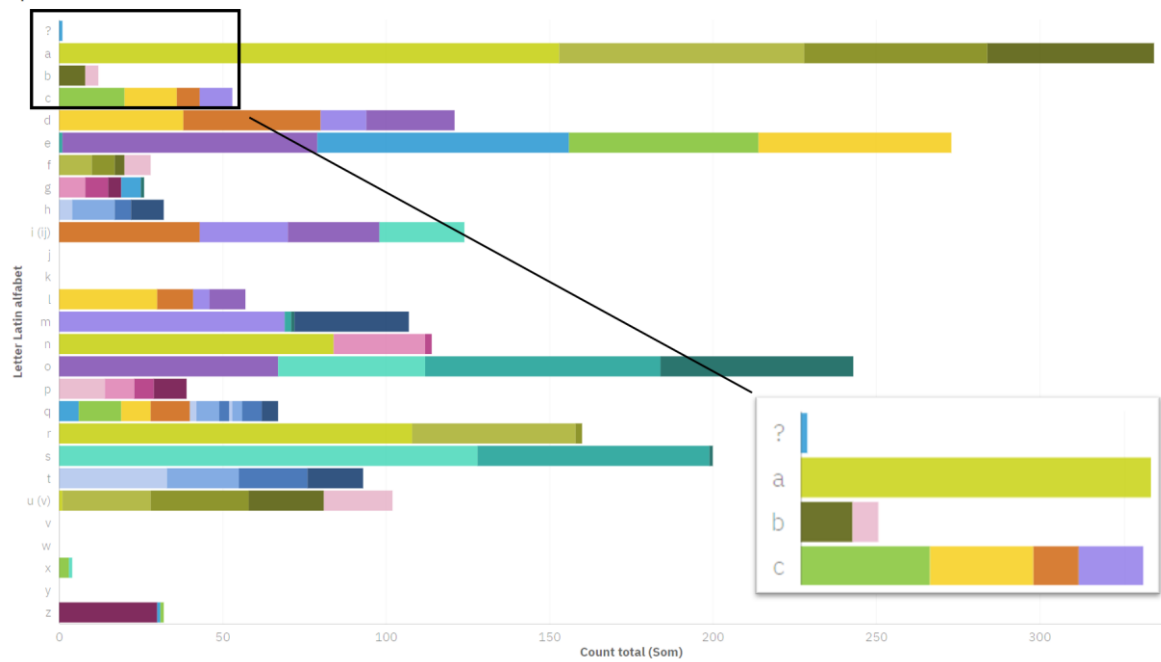
COMPLETE RECONSTRUCTED KEY OF CIPHER 168

INDEX COLORS. **Yellow** is a code that fits in used key-strategy +1, +2, and +5 but that's not used. **Green** is a reconstructed code.

Letter	Code	+1	+2	+5	Notes
a	24	241	242	245	
b	9	91	92	95	
c	10	101	102	105	
d	20	201	202	205	
e	30	301	302	305	Before reconstruction: 30, 301, 302, 305
f	16	161	162	165	
g	19	191	192	195	
h	22	221	222	225	
i (ij)	31	311	312	315	Before reconstruction: 31, 301, 302, 305
j	letter not used				
k	letter not used				
l	6	61	62	65	Before reconstruction: 6, 65
m	3	31	32	35	Before reconstruction: 3, 35
n	4	41	42	45	Before reconstruction: 4, 41
o	11	111	112	115	
p	25	251	252	255	
q	26	261	262	265	
		3261	3262	3265	
		7261	7262	7265	
r	8	81	82	85	Before reconstruction: 8, 81
s	7	71	72	75	Before reconstruction: 7, 71
t	13	131	132	135	
u (v)	40	401	402	405	
v	letter not used				
w	letter not used				
x	2	21	22	25	
y	letter not used				
z	5	51	52	55	Before reconstruction: 5, 55

NUMBER-CODES OVER LETTERS OF CIPHER 168

Cipher 168. Letter Latin alfabet and Code-number



APPENDIX 3: Letterbooks WIC between 1645-1654

List of WIC sources with letterbooks and their archive number in Nationaal Archief, Den Haag (NL-HaNA), Oude West-Indische Compagnie (OWIC), inv.nr. 1.05.01.01:

Nr	WIC archive number	Year	Month	No content (only cover page)	Nothing relevant	Examinaties prisoners or defectors	Intercepted letters	Cipher(tekst) mentioned	Letter King Portugal not in cipher
1	60-74	1645	6		1				
2	60-100	1645	6			1			
3	60-125	1645	8				1		
4	60-189	1645	8				1		
5	60-192	1645	9			1	1		
6	60-146	1645	9			1	1		
7	60-12	1645	?		1				
8	60-26	1645	?		1				
9	60-48	1645	?		1				
10	60-103	1645	?		1				
11	61-56	1646	3			1	1		1
12	62-74	1646	9		1				
13	61-60	1646	?				1		1
14	62-5	1646	?			1			
15	62-16	1646	?		1				
16	62-43a	1646	?	1					
17	62-45	1646	?			1	1	1	
18	62-89	1646	?			1	1		
19	62-111	1646	?			1	1		
20	63-38	1647	5			1			

Nr	WIC archive number	Year	Month	No content (only cover page)	Nothing relevant	Examinaties prisoners or defectors	Intercepted letters	Cipher(tekst) mentioned	Letter King Portugal not in cipher
21	63-75	1647	8				1		
22	63-101	1647	8	1					
23	63-104	1647	9	1					
24	63-99	1647	12		1				
25	63-14	1647	?		1				
26	63-67	1647	?			1			
27	63-102	1647	?	1					
28	64-30	1648	7				1		
29	64-63	1648	8			1			
30	64-76	1648	8			1			
31	64-86	1648	9		1				
32	64-103	1648	10			1	1		
33	64-104	1648	10		1				
34	64-131	1648	12			1	1		
35	64-1	1648	?				1		
36	65-40	1649	3		1				
37	65-65	1649	4			1	1		
38	65-107	1649	7				1	1	
39	65-120	1649	9			1			
40	65-154	1649	11			1	1	1	
41	65-186	1649	12			1			
42	661-1	1649	?	1					
43	661-17	1650	3			1	1		
44	661-34	1650	5			1			
45	661-59	1650	6			1			
46	661-72	1650	6		1				
47	661-57	1650	6			1			
48	661-77	1650	11			1			
49	662-1	1651	1			1			
50	662-35	1651	6			1			
51	662-34	1651	6	1					
52	662-89	1651	7				1		
53	662-59	1651	8	1					
54	662-70	1651	9		1				
55	662-80	1651	9		1				
56	662-69	1651	9	1					
57	662-79	1651	9			1			
58	662-87	1651	10	1					
59	662-94	1651	12			1			
60	662-2	1651	?		1				
61	67-1	1652	2	1					
62	67-40	1652	10	1					
63	67-60	1653	3	1					
64	67-94	1654	2		1				

Nr	WIC archive number	Year	Month	No content (only cover page)	Nothing relevant	Examinaties prisoners or defectors	Intercepted letters	Cipher(tekst) mentioned	Letter King Portugal not in cipher
Total				12	17	27	19	3	2

Summary WIC sources with letterbooks. Year and relevance:

Year	No content (only cover page). Count	Nothing relevant. Count	Examinaties prisoners or defectors. Count	Intercepted letters. Count	Cipher(tekst) mentioned. Count	Letter King Portugal not in cipher. Count
1645		5	3	4		
1646	1	2	5	5	1	2
1647	3	2	2	1		
1648		2	4	4		
1649	1	1	4	3	2	
1650		1	5	1		
1651	4	3	4	1		
1652	2					
1653	1					
1654		1				
Total	12	17	27	19	3	2

APPENDIX 4: Ciphertexts Mentioned between 1645-1654

Sources in Dutch and Portuguese archives concerning Brazil, between 1645-1654, with ciphertexts or mentioning them:

Nr	Archive	Source	Sorting	Original year letter	Where	Jewish connection	What
1	Portuguese	Teles da Silva, 1650b	mentions cipher	referring to 1642-1647	Seas	none	1650-7-19: in his testament Antonio Teles da Silva states that he had several ciphered letters that his brother had to hand over to the king of Portugal.
2	Dutch	Hoge Raad, 1646 Vieira, 1646 Kort Discours Rebelye, 1647	mentions cipher	1646	Land	deciphered by "a jew"	1646-5-8: intercepted letters in cipher from Jan Viera d'Allegro [or João Vieira de Alagoas].
3	Dutch	Pina de, 1646	ciphertext	1646	Land	decipherer De Pina is a jew	1646-5-??: letter from Abraham de Pina [or Aarão Sarfati to Dutch] with key for ciphers and explanation. Decrypted letters.
4	Portuguese	Teles de Menezes, 1647	mentions cipher	1647	Seas	none	1647-08-10: governor-general Antonio Teles de Menezes received a cipher to be used in "matters that ask for secrecy".
5	Dutch	Teles da Silva, 1649a1 Teles da Silva, 1649b1	ciphertext	1649	Seas	deciphered by "a skilled person"	1649-5-28: letter in cipher from prisoner Antonio Telles da Silvas to king Portugal. 1649-6-3: letter in cipher from prisoner Antonio Telles da Silvas to king Portugal.
6	Dutch	Corea da Saa, 1649	mentions cipher	1649	Seas	none	1649-11-29: letterbook mentions a deciphered and translated letter from admiral Salvador Correa de Saa to the king of Portugal. Other source: letter is dated 1649-7-4.
7	Dutch	Dias, 1649	mentions secret communication	1649	Land	none	1649-11-28: prisoner Steven (Stevão) Dias has to explain the characters, lines, points and words in a letter that his brother sent to him.
8	Dutch	Dagilaer, 1649	mentions cipher	1649	Seas	decipherer Dagilaer is a jew	1649-12-3 and 1650-1-18: jew Moyses Raphael Dagilaer [or Moisés Rafael de Aguilar] is promised 30 guildens for find out content of encrypted letters for governor in Angola. Found in a captured ship by captain Hartman.
9	Portuguese	Teles da Silva, 1650a	mentions cipher	1649	Seas	none	1650-7-10: Teles da Silva emphasizes the ability of Ravasco to decipher the king's ciphertexts.