

Deciphering a Letter to Louis XIV from his Ambassador to the Dutch Republic, le Comte d’Avaux, 1684

George Lasry

The CrypTool Team

george.lasry@cryptool.org

Abstract

The Dutch Royal Archives (Koninklijk Huisarchief - KHA) at The Hague holds a number of enciphered letters written by French diplomats in Holland in the 17th and 18th centuries, including a letter, from January 9, 1684, from Jean-Antoine de Mesmes (1640 – 1709), Comte d’Avaux, the French ambassador at The Hague from 1678 to 1689, to Louis XIV, King of France from 1643 to 1715.

In this article, we show how we deciphered the letter, and identified the historical plaintext as a letter intercepted and deciphered by the Spanish authorities in the Southern Netherlands. The letter was also published by the Prince of Orange, to expose d’Avaux secret contacts with deputies of the city of Amsterdam. D’Avaux claimed that the decryption was intentionally modified to harm France’s image, but the modern decipherment demonstrates that the historical decryption was in fact fully accurate.

1 The Document

The document is held in the Dutch Royal Archives, Koninklijk Huisarchief (KHA), under reference Prins Willem III, inv.nr. XIII-I (d’Avaux, 1684b). The first page is shown in Figure 1. The document contains a mix of cleartext and encoded parts. The cleartext indicates that it is dated January 9, 1684, and that it was sent by the Comte d’Avaux to Louis XIV (“Votre Majeste”). The digit codes are separated by spaces, although the separation is not always clear. There are some punctuation marks, like a comma. On the top of some digits, an accent appears, or a Tilda sign. Their meaning could be identified only after deciphering most parts of

the ciphertext. The codes contain either two digits (e.g., 34, 14) or three digits (e.g., 295, 505).

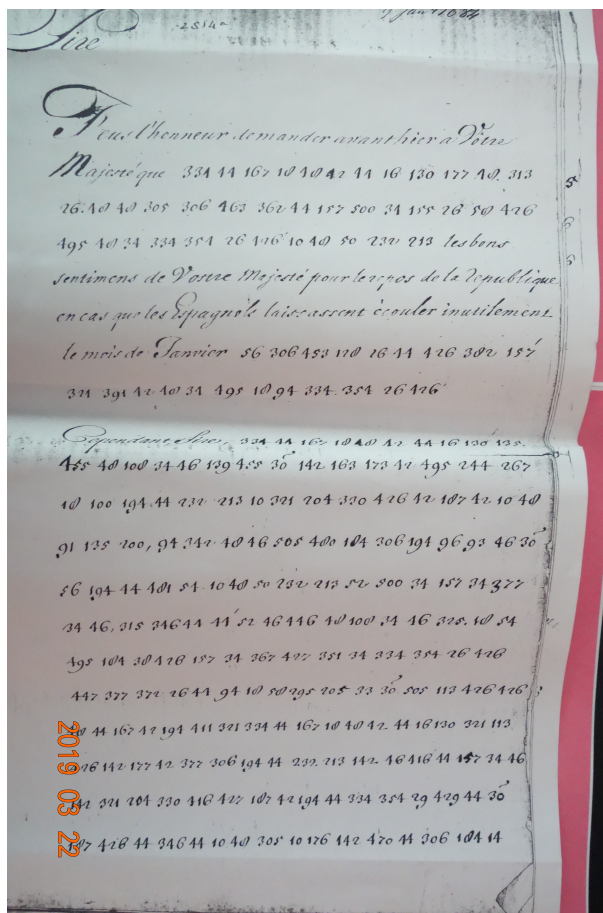


Figure 1: First Page of the Encrypted Letter (d’Avaux, 1684b)

2 Deciphering the Letter

Initially, an attempt was made to decipher the codes using computerized techniques for homophonic ciphers, described in (Lasry et al., 2020). The main challenge was that there were too many distinct codes, and the automated algorithms did not produce any valid solution.

Next, it was hypothesized that the two-digit

codes might represent single letters, while the three-digit codes represent full words, names, or places. Since there are only short continuous subsequences that contain only two-digit codes, the computerized algorithm could not produce anything useful.

Next, an attempt was made to find the original key used to encipher the text, in archives. The DE-CODE Database contains hundreds of such original keys, but very few of them are from France, and no original key could be found that decipher the letter (Megyesi et al., 2020).

The solution came from another direction. A year before, the author of this article had been contacted by a scholar who was studying other letters from the Comte d’Avaux, sent in 1688, also from Holland. Some of the encoded letters from 1688 had plaintext inscribed near the codes and help was requested to recover the key. The author was able to recover the key from those plaintext segments. It turned out to be the key for another French diplomatic document, recovered historically via codebreaking by John Wallis, the famous British mathematician and codebreaker (1616-1703). Wallis published his decipherment and the key in *Opera Mathematica* (Wallis, 1972). The author was able to recover additional codes. As shown in Figure 3, the two-digit codes mainly represent single letters. It can be seen that this is a monoalphabetic code (no homophones), with a nomenclature, and that the two-digit codes for the letters are in alphabetical order. For example, A = 20, B = 22, C = 24. Other two-digit codes represent common propositions (CE = 23, DANS = 33). The three-digits codes, shown in Figure 4, are not in an alphabetical order, but it can be seen that there is some order when looking at individual columns. For example, the syllables TA, TE, TI, TO, and TA are encoded as 322, 332, 342, 352, and 362, respectively. This pattern must have been useful to Wallis, when he broke the code.

First, the author tried to decipher the letter from Comte d’Avaux’s from 1684, using this code from 1688, without success.

Then, the author made a hypothesis that turned out to be correct. Since the code for the 1688 letter is quite simple, with ordered patterns, the code for the 1684 letter might also be a similar simple code, or even simpler, as it predates the 1688 code. One possibility considered was that instead of A, B, C, being 20, 22, 24 as in the 1688 code, the letters of the alphabet start from 10, that is, A = 10, B = 12,

C = 14, as shown in Figure 5. Under this hypothesis, fragments of the ciphertext which consist of subsequences of two-digit codes were deciphered, and produced meaningful fragments of plaintext, validating the hypothesis.

Next, the author took advantage of those already-decrypted segments and of the fact that syllables in the 1684 code were also likely to be ordered in columns, to recover several syllables. Next, he was able to recover the codes for all the syllables, and for a number of words, places, and names, as shown in Figure 6, and as a result, to decipher almost all the original ciphertext.

With a partial plaintext at hand, the author conducted a search for the historical context, and hopefully, the original plaintext, in other sources. With some effort the author identified the letter as a famous letter from the Comte d’Avaux, from January 9, 1684 (d’Avaux, 1684c). Based on the full plaintext, additional code entries could be recovered. The Tilda signs turned out to indicate digits to be deleted.

A sample of deciphered letter is shown in Figure 2.

```

Janv 1684

Sire

J'eus l'honneur de demander avant hier à Votre Majesté que

334 44 167 18 48 42 44 16 130      177 48 313
ME S SI E U R S D AMSTERDAM SO U HA

26 46 46 305      306 463 362 44 157 500 34 155 26 58 426
I T T OIENT QUE JE FI S SE CO N NO I ST RE

495 48 34 334 354 26 426 10 48 50 232      213
PAR U N ME MO I RE A U X ETATZ GENERAUX

les bons sentiments de Votre Majesté pour le repos de la République
en cas que les Espagnols laissassent écouler inutilement
le mois de Janvier

56 306 453 128 26 44 426 382 157
ET QUE JA VO I S RE FU SE

321 391      42 48 34 495 18 94 334 354 26 426
DE DONNE R U N PAR E IL ME MO I RE

Cependant Sire,

334 44 167 18 48 42 44 16 130      135
ME S SI E U R S D AMSTERDAM NE

455 48 108 34 46
PE U VE N T

```

Figure 2: Sample Decryption – Codes, Decrypted Plaintext, and Cleartext

FROM	TO	0	1	2	3	4	5	6	7	8	9
0	9										
10	19										
20	29	A	CA	B	CE	C		D	CO	E	
30	39	F	DE	G	DANS	H	EN	I	EST	J	FAI
40	49	L	R	M	S	N	JE	O	IL	P	LE
50	59	Q	LUI	R		S		T		UV	
60	69	X	NE	Y		Z		ET		ST	
70	79	NT		NS		ER					
80	89								T		
90	99						CA				LAISS

Figure 3: Similar Code Recovered by John Wallis and used by d’Avaux in 1688 – 20 to 99

FROM	TO	0	1	2	3	4	5	6	7	8	9
100	109		PUIS	SI	VA		CE		FAI		MA
110	119			SO	VE	AVOIR	CI				ME
120	129		ON	PARTICULIER	SU	VI	AVEC	CO	FACIL		MI
130	139		OIT		SANS	VO	AUTRE	CU		HONGROIS	MO
140	149		OBLIG			VU	AUSSI		DEMANDE	HONNEUR	MU
150	159										MAJESTE
160	169										MAISTRE
170	179		ORDINAIRE			AUTRICHE	CETTE		FRANCE	HEUR	
180	189			POLOGNE		AU					MENT
190	199		ORDRE	QUA						JA	
FROM	TO	0	1	2	3	4	5	6	7	8	9
200	209		QUE	SECRET	VOIR			ENTRE		JE	
210	219		QUI		VOUS		CONTRAIRE	EUX		JI	
220	229		QUO	SERVICE	VOSTRE					JO	MINISTRE
230	239		QUU	SEUL		ARGENT		EN	FOR	JU	MAIS
240	249		ORANGE	QUAND				EST			MOYEN
250	259							ESPAGNOL		JAMAIS	
260	269			QUELLE							MM
270	279			QUELQUE		ALLEMAN		ELECTION		IL	MR
280	289		PA	QUIL			COUR		GA	JOUR	MADAME
290	299		PE			XA		ENGAGE	GE	INTEREST	MAISON
FROM	TO	0	1	2	3	4	5	6	7	8	9
300	309		PI	QUOIQUE					GI		
310	319		PO	RA					GO		
320	329		PU	RE	TA		BA	COMME		GU	INTENTION
330	339		PERSONNE	RI	TE		BE	CARDINAL			NA
340	349			RO	TI	ZELL	BI		ENVOY	GENER	LA
350	359			RU	TO		BO	DA	EMPEREUR	GOVERN	LE
360	369			ROI/ROY	TU	ZI	BU	DE			LI
370	379		PAR				BEAUCOUP	DI		GRAND	LO
380	389				TANT			DO			LU
390	399		POINT		TION		BETHUNE	DU		LETTRE	NONCE
FROM	TO	0	1	2	3	4	5	6	7	8	9
400	409					BON	DANS				NEANTMOINS
410	419		PAPE			BIEN			GENS		
420	429		POUR			KI		FA			
430	439		PLUS					FE	HA	LUY	
440	449		PENSIONNAIRE		TOUT			FI	HE		NOUS
450	459		PRENDRE	REINE			DONNE	FO	HI	LEUR	
460	469			SA	TEMPS			FU	HO	LONG	
470	479		PENDANT	SE					HU		

Figure 4: Similar Code Recovered by John Wallis and used by d’Avaux in 1688 – 100 to 479

FROM	TO	0	1	2	3	4	5	6	7	8
10	19	A		B		C		D		E
20	29	F		G		H		I		J
30	39	L		M		N		O		P
40	49	Q		R		S		T		U
50	59	X		Y		Z		ET		ST
60	69									
70	79									
80	89									
90	99	AVANTAGE	CU		FAGEL	IL		PENSIONNAIRE		VA

Figure 5: Code used by d’Avaux in 1684 and Recovered by the Author – 10 to 98

FROM	TO	0	1	2	3	4	5	6	7	8
100	109	AUTHORITE						PERSONNE		VE
110	119				FAI			PROPOSITION		VI
120	129	ANCE					NA	PRINCE		VO
130	139	AMSTERDAM		EST	FIN	JOUR	NE			VU
140	149	ARGENT		EN		INFORM	NI	POUVOIR	SA	VAISSEAU
150	159	ASSEMBLEE		ELLE	FRISE		NO		SE	VILLE
160	169			EUX	GA		NU		SI	VOSTRE
170	179		CONTRAIRE	ENTRE	GE			PRENDRE	SO	
180	189		CETTE		GI	LA		1	SU	
190	199	ASSUR			GO	LE		PENDANT	SANS	
FROM	TO	0	1	2	3	4	5	6	7	8
200	209	AFFAIRE			GU	LI		PAYS		
210	219				GENERAUX	LO	NOUVEAU	PUIS		
220	229					LU	NOUVELLE	PLUS	SECOURS	
230	239			ETATZ		LUI	NOUS			
240	249	ACCORD	CONFER			LEUR				
250	259		COMME							
260	269			ESPAGNE					SEUL	
270	279	AUTRE		ESPAGNOL				PROVINCE		
280	289	AVEC			GRAND	LORS	ON			XA
290	299		COUR		1		OIT	QUA		XE
FROM	TO	0	1	2	3	4	5	6	7	8
300	309	AVOIR	CONCLU		GRONINGHE			OIENT	QUE	XI
310	319		DA		HA			OU	QUI	XO
320	329	BA	DE		HE	MA		OBLIG	QUO	XU
330	339	BE	DI		HI	ME			QUU	
340	349	BI	DO	FA	HO	MI			QUIL	VAN
350	359	BO	DU	FE	HU	MO	ORANGE		QUEL	
360	369	BU	DANS	FI	HOLLANDE	MU	OFFERT	QUELQUE	TA	
370	379	BEAUCOUP		FO	HOLLANDAIS	MAJESTE		QUAND	TE	
380	389			FU		MATIE	OFFRES		TI	
390	399		DONNE	FRANCE		MONSIEUR			TO	
FROM	TO	0	1	2	3	4	5	6	7	8
400	409	AMI			HEUR				TU	
410	419	BIEN	DESSEIN	FAVORABLE				RA		
420	429							RE	TION	
430	439				HONNEUR			RI	TANT	
440	449			FOURNI		MENT	PA	RO	TOUT	
450	459				JA		PE	RU	TROUPPES	
460	469				JE		PI	ROY	TOT	
470	479	CA			JJ	MEME	PO	REGENCE		
480	489	CE	DEPUTE		JO		PU		TEMOIN	
490	499	CI		FORT	JU	MINISTRE	PAR		TEMPS	
FROM	TO	0	1	2	3	4	5	6	7	8
500	509	CO				MAIS	POUR			

Figure 6: Code used by d’Avaux in 1684 and Recovered by the Author – 100 to 508

3 The Historical Context and the Contents of the Letter

After it was captured and deciphered in 1684, the letter was published in various pamphlets in several languages. An initial version - with the original French text - is shown in Figure 7 (d'Avaux, 1684c). It can be seen that the decryption is incomplete. An English version was also published in England (d'Avaux, 1684a).

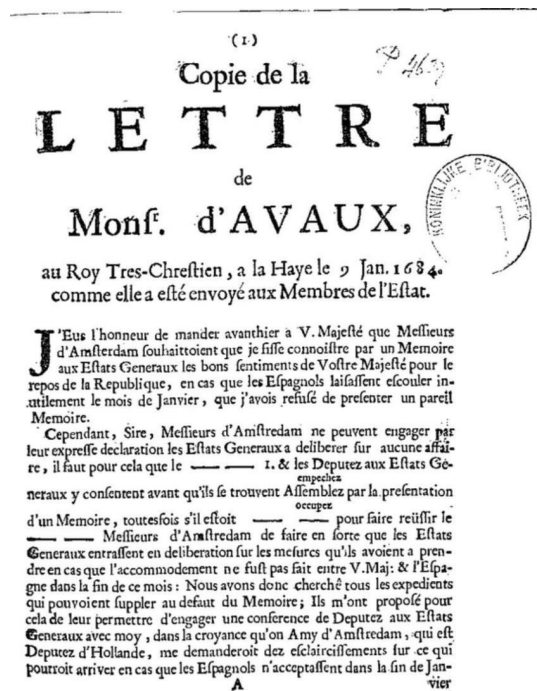


Figure 7: First Version of the Deciphering of the Intercepted Letter (d'Avaux, 1684c)

Before describing the contents of the letter, an overview of the historical context is given here. The diplomatic aspects of French intervention in Holland in the 17th century are described in detail in (Jones, 1989) and in (Kurtz, 1928). D'Avaux recorded his own version of the events in (d'Avaux, 1754). A background on Dutch cryptography is given in (De Leeuw, 1999).

The Dutch system of government at the end of the 17th century was complex, offering opportunities that the French ambassador was eager to exploit. Spain and France had just concluded a war in which Spain lost several territories in the Southern Netherlands. To counter French influence, the Prince of Orange wanted to raise new taxes, expand the army, and form new alliances. To oppose those efforts, d'Avaux established working

relationships with Williams' most consistent and influential opponents, the Regents of city governments. He openly engaged delegates from the provincial States to the States-General, to block William's initiatives, that were supported by Gaspar Fagel, the Pensionary of Holland in title but Williams' loyal ally. In 1683-84, d'Avaux and his allies were able to block William's attempt to raise any new levies of men for the army and prevented him from moving forces to the Spanish Netherlands, which were about to be invaded by a French Army.

D'Avaux's most important contacts were those whom he called Messieurs d'Amsterdam, the oligarchy of burgomasters and magistrates who controlled city governments as well as banking services providing the Dutch government with loans. D'Avaux also harnessed support from members of the Frisian and Utrecht delegations to the States-General.

In September 1683, William proposed measures to the States-General to deter Louis from making an attack on Luxemburg and to bolster Spanish resistance to an attack there. William had already moved 8000 men into defensive positions in the Spanish Netherlands but he needed to increase the army to 16000 soldiers overall. Louis conducted a policy that applied military pressure on Spain, with diplomatic intervention by d'Avaux. With the delegates from Amsterdam, Friesland and Groningen, Louis XIV wanted to counter William's attempts to come to the assistance of Spain. The deputies argued that war (with France) would ruin trade and that it was not worth risking fishing trade for the sake of assisting the Spanish Netherlands. They attached impossible conditions to the voting of extra money. Even a personal appearance by William in the States failed to persuade the Amsterdam deputies to agree to extra men and money, and left him humiliated.

In this context, on January 9, 1684 d'Avaux wrote the letter to Louis XIV describing his contacts with the Messieurs d'Amsterdam in extensive detail, but without naming them. It emerges from the letter that the republican parties are trying to get concrete assurances from Louis XIV, but d'Avaux is only providing vague ones.

The courier carrying the letter was robbed of his letters just outside Maastricht, a fortified city on the border, by men wearing the uniform of the Dutch garrison. The Marquis de Grana, the gov-

error of the Spanish Netherlands, handed over a decrypted version to William, who read it to the States of Holland on February 16. Achieving a sensational effect, he denounced two delegates from Amsterdam, who claimed that they were only trying to protect the city's trading interests.

D'Avaux responded by claiming that the Spanish had deliberately distorted the text for propaganda purposes, with a letter to the States General (shown in Figure 8), with his own version of some of the key sentences in question (d'Avaux, 1684d).

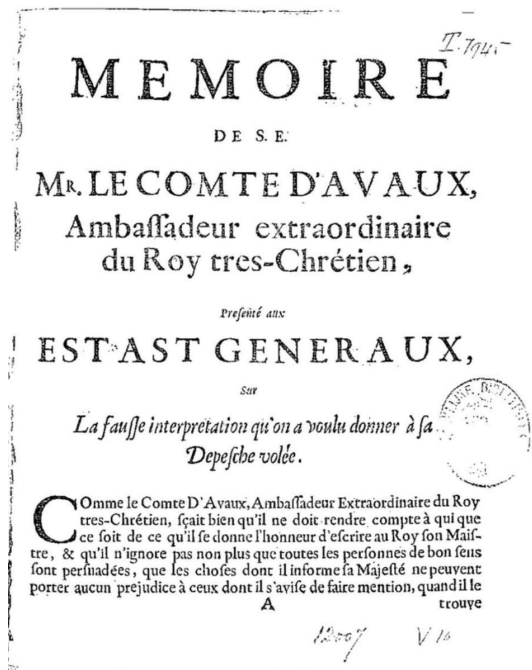


Figure 8: D'Avaux Letter to the States General in Response to the Publication of the Intercepted Letter (d'Avaux, 1684d)

An updated, more complete decryption (d'Avaux, 1684c), shown in Figure 9, further supported the claims of William. The author has compared this version to his own decipherment of the letter. They match almost entirely, refuting d'Avaux's claims that William and the Spanish had intentionally distorted his original text.

In the longer term, the incident had little effect. William was unable to support Spain, who had to accept France's terms for peace. However, attempts by d'Avaux to obtain the dismissal of the Pensionary of Holland failed, and with the expulsion of the Huguenots from France a few years later, d'Avaux's influence had significantly diminished.

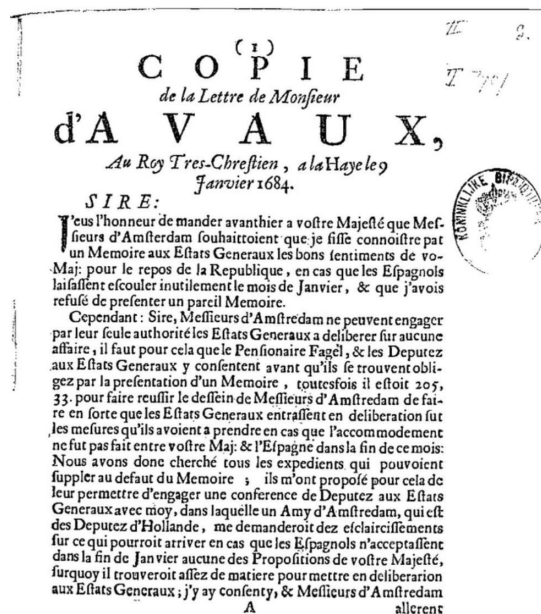


Figure 9: Second Version of the Deciphering of the Intercepted Letter (d'Avaux, 1684c)

4 Conclusion

The modern (re)decipherment of d'Avaux's letter provides some insights on the nature of the French diplomatic codes in the late 17th century. It seems that not only the same code was used in different places, but that the code used by d'Avaux in 1688 was only a minor variation of the code he had been using in 1684. Both codes have a fair amount of structure and alphabetical order, and they are highly insecure. They are even more insecure if they are used over a long period of time. It is even more striking given the fact that the 1684 code was known to be compromised, and a stronger code would have been advisable, rather than another one with minor changes. This finding is surprising, as by this time, the French cryptographers including the famous Rossignol had already introduced much more secure codes such as two-part unordered nomenclators (Kahn, 1996, p. 161).

This letter also exemplified the taking advantage of the capture and decipherment of a diplomatic coded dispatch, for propaganda purposes, despite letting the adversary know that their messages can be deciphered. Unlike another cryptographic propaganda coup, the famous Zimmermann Telegram, the capture and publication of the letter from the Comte d'Avaux did not have a major impact on diplomatic and military events.

Acknowledgments

This work has been supported by the Swedish Research Council, Grant 2018-06074, DECRYPT – Decryption of historical manuscripts.

References

- Jean Antoine Comte d’Avaux. 1684a. *An exact copy of a letter from the Count d’Avaux, His Most Christian Majesties ambassador at the Hague dated the 9th of January 1684 and directed to the King his master which was intercepted by the Marquess de Grana governour of the Spanish Netherlands : as also the copies of other three letters relating to the same affair.* Hague, London: Printed by Jacobus Sikeltus, Re-printed for Randall Taylor; Retrieved: Text Creation Partnership, <http://name.umdl.umich.edu/A04486.0001.001>.
- Jean Antoine Comte d’Avaux. 1684b. *Collection: Willem III, inv.nr. XIII-1.* Dutch Royal Archives, Koninklijk Huisarchief.
- Jean Antoine Comte d’Avaux. 1684c. *Copie de la lettre de monsieur d’Avaux, au roy tres-chrestien, a la Haye le 9 janvier 1684.* Koninklijke Bibliotheek, pfl 11962, retrieved from Brill Online - <https://primarysources.brillonline.com/browse/dutch-pamphlets-online/copie-de-la-lettre-de-monsieur-davaux-au-roy-treschrestien-a-la-haye-le-9-janvier-1684;dutchpamphletskb1kb14034>.
- Jean Antoine Comte d’Avaux. 1684d. *Memoire de S.E. Mr. le comte d’Avaux, ambassadeur extraordinaire du roy tres-chrétien, présenté aux Estats Generaux, sur la fausse interpretation qu’on a voulu donner a sa depesche volée.* Koninklijke Bibliotheek, pfl 12007, retrieved from Brill Online - <https://primarysources.brillonline.com/browse/dutch-pamphlets-online/memoire-de-se-msuprsup-le-comte-davaux-ambassadeur-extraordinaire-du-roy-treschretien-presente-aux-estats-generaux-sur-la-fausse-interpretation-quon-a-voulu-donner-a-sa-depesche-volee;dutchpamphletskb1kb14080>.
- Jean Antoine Comte d’Avaux. 1754. *Negociations du comte d’Avaux en Hollande depuis 1679 jusqu’en 1688 (publies par Edme Mallet.)*, volume 2. Durand.
- Karl De Leeuw. 1999. The Black Chamber in the Dutch Republic during the War of the Spanish Succession and its aftermath, 1707-1715. *Historical Journal*, pages 133–156.
- James Jones. 1989. ‘French intervention in English and Dutch politics, 1677–88’, in *Black Jeremy (ed.), Knights Errant and True Englishmen: British Foreign Policy, 1660–1800*. Edinburgh, John Donald Publishers.
- David Kahn. 1996. *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*. Simon and Schuster.
- Gerdina Hendrika Kurtz. 1928. *Willem III en Amsterdam, 1683-1685*. Utrecht, Kemink en zoon.
- George Lasry, Beáta Megyesi, and Nils Kopal. 2020. Deciphering papal ciphers from the 16th to the 18th Century. *Cryptologia*, pages 1–62.
- Beáta Megyesi, Bernhard Esslinger, Alicia Fornés, Nils Kopal, Benedek Láng, George Lasry, Karl de Leeuw, Eva Pettersson, Arno Wacker, and Michelle Waldispühl. 2020. Decryption of historical manuscripts: the DECRYPT project. *Cryptologia*, 44(6):545–559.
- John Wallis. 1972. *Johannis Wallis Opera Mathematica*, volume 3. E Theatro Sheldoniani.