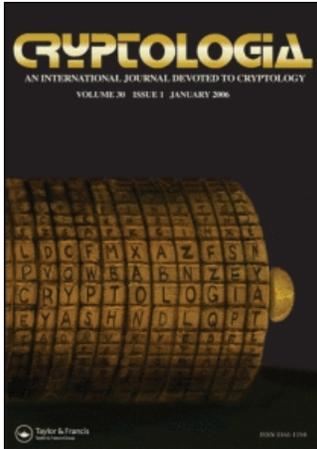


This article was downloaded by:[Winkel, Brian]
On: 14 March 2008
Access Details: [subscription number 769884566]
Publisher: Taylor & Francis
Informa Ltd Registered in England and Wales Registered Number: 1072954
Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



Cryptologia

Publication details, including instructions for authors and subscription information:
<http://www.informaworld.com/smpp/title~content=t725304178>

CASANOVA AND THE BEAUFORT CIPHER

Brian J. Winkel

Online Publication Date: 01 April 1978

To cite this Article: Winkel, Brian J. (1978) 'CASANOVA AND THE BEAUFORT CIPHER', Cryptologia, 2:2, 161 - 163

To link to this article: DOI: 10.1080/0161-117891852947

URL: <http://dx.doi.org/10.1080/0161-117891852947>

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: <http://www.informaworld.com/terms-and-conditions-of-access.pdf>

This article maybe used for research, teaching and private study purposes. Any substantial or systematic reproduction, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.

CASANOVA AND THE BEAUFORT CIPHER

Brian J. Winkel

Jacques Casanova de Seingalt (1725-1798), the Italian adventurer (!), in addition to his famed salacious and concupiscent skills, was a bit of a cryptologist in his spare time.

In the words of William F. Friedman [2, p.1] —

"That Casanova, gifted as he was, should have had more than a passing knowledge of the esoteric subject of cryptology, along with magic and the occult, should come as no surprise. We do not need to take his (Casanova's) own word for it; we possess at least three separate testimonies in substantiation: (1) an enciphered signature to one of his many published pamphlets; (2) a fairly long discussion in the *Memoirs* of his decipherment of an enciphered manuscript belonging to the famous Mme d'Urfé; and (3) a letter to an unidentified correspondent, dated about 1791, partly enciphered and published as letter no. 82 in *Patrizi e Avventurieri* (Milano, 1930, p. 399-400)."

Let us examine the third testimony cited by Friedman. The cryptic, fragmented message, upside-down on the bottom of letter No. 82 in *Patrizi e Avventurieri* appeared as follows:

```

x d z e e t t m e y n i n b m t k z o e
n s t c u r b q a u b u f r f p e i k
                                     n a b u c
m x k e u x k z t g i g n a i n
o d o n o s o r n a b u c o d o
m a e x m e r i
n o s o r n a b
                                     f o i s
                                     [l. p.11]

```

After much effort, both Friedman [2] and Bowers [1] determined from both examination of the original document and eventual decipherment that the text in *Patrizi e Avventurieri* contained certain errors. While there may be still some doubt as to the accuracy of the corrections, it is believed that the corrected text is as follows:

```

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

```

Friedman [2] and Bowers [1] in their discussions of this cipher believed that the repeated use of the word NABUCODONOSOR (the Italian spelling, without the H, of Nebuchadnezzar) served as a key-word for a Vigènere type system. Further, the final four sets of letters in the text provided a wedge leading to the recovery of the manner in which the Vigènere system was used by Casanova. With Bowers [1] pointing out that Casanova's alphabet contained 23 letters (the letter I was used also as a J, the letter U served also as a V, and there was no letter W) plus the ampersand (&), we see that the Beaufort Tableau which equivalently may be used to encipher and decipher the message of Casanova appears as follows:

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

Thus, using the above Tableau it is seen that that final four sets of letters in the (corrected) text show accurate Beaufort encipherment:

Ciphertext: M & R I
 Key: R N A B
 Plaintext: F O I S

At this point it is left to the reader to decipher the complete cryptogram of Casanova. But it should be noted that in employing the key-word NABUCODONOSOR, Casanova was not perfect (!) for at one point in the text he dropped two letters of key. Incidentally, the letters in the text "fre" probably represent the word "chiffre". As for the translation of Casanova's

Downloaded By: [Winkel, Brian] At: 02:53 14 March 2008

cryptogram, we can only say that the plaintext is somewhat confusing and we offer this cryptic conclusion from the pen of William Maxwell Bowers [1. p. 16]:

"After reading and re-reading it, *le tout trois fois*, it still does not make much sense and, *peut-être en aise fait*, it is not intended to. However, it is *ici corrigé et revu* and *aussi au moins* these scrawled *chiffre* characters have been systematically converted into true French words."

BON CHANCE!

REFERENCES

1. William Maxwell Bowers, Decipherment of the Casanova Cryptogram, *Casanova Gleanings*, v.14, 1971, 11-16.
2. William F. Friedman, Jacques Casanova de Seingalt, *Cryptologist*, *Casanova Gleanings*, v.14, 1961, 1-13.