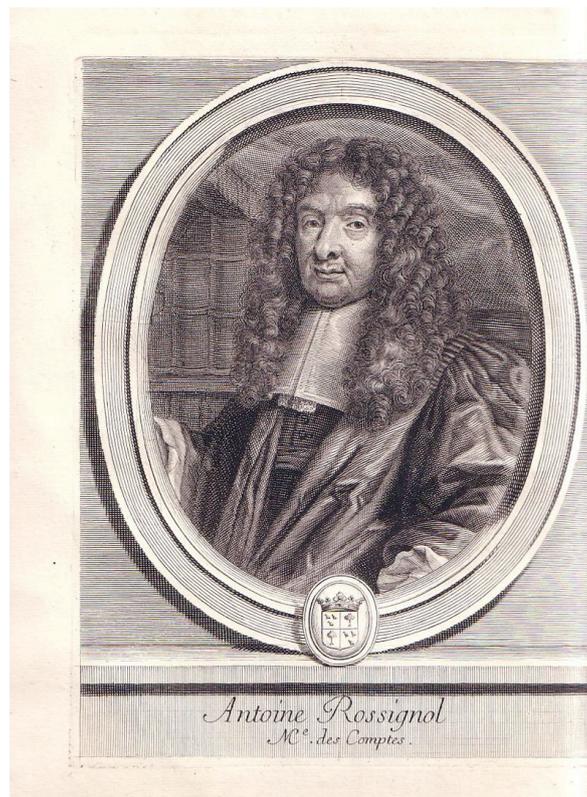


## Réalmont : une victoire obtenue par la seule arme du chiffre

Le décryptement d'un seul message peut décider du sort d'une bataille ou d'une négociation. Ce fut le cas en 1626 quand les troupes du prince de Condé assiégeant Réalmont interceptèrent un messenger sortant de la ville, porteur d'un message incompréhensible. **Condé fit venir un jeune professeur de mathématiques de la région, Antoine Rossignol des Roches, qui en trouva le sens.**

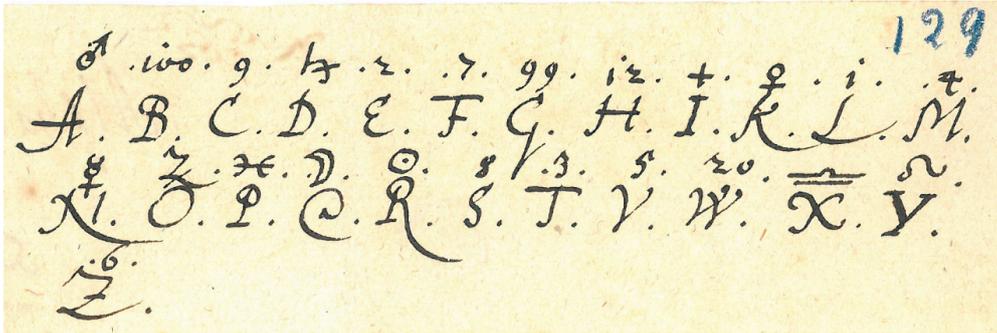


Le message annonçait que la ville était à cours de munition. Condé fit porter le message décrypté à la ville, qui se rendit. La bataille fut gagnée grâce à la seule arme du Chiffre !

### Chiffrement par alphabet chiffré

Ce message avait vraisemblablement été chiffré au moyen d'un alphabet chiffré, où chaque lettre est remplacée par un symbole, très en vogue à l'époque. Le décryptement repose à la fois sur les mathématiques et sur la linguistique. Les mathématiques par la méthode des fréquences qui permet au moins de trouver le symbole représentant la lettre « e ». La linguistique par la méthode du mot probable qui permet de deviner des mots du message selon le contexte.

Par exemple, dans un message sortant d'une ville assiégée, on peut s'attendre à des mots comme « vivres » ou « munitions ».



Un alphabet chiffré de 1626. Chaque lettre doit être remplacée par le symbole inscrit au dessus.

## Chiffrement par dictionnaire chiffré

La faiblesse des alphabets chiffrés, même améliorés en chiffrant de plusieurs façons différentes les lettres fréquentes et en ajoutant des nulles, c'est-à-dire des symboles ne signifiant rien, amena Rossignol à créer des dictionnaires chiffrés c'est-à-dire des dictionnaires bilingues dont l'une des langues est le français et la seconde, des nombres. Ainsi, on chiffre non seulement des lettres (et ce de plusieurs manières), comme auparavant, mais aussi des syllabes et des mots.

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	Y	Z	8	7	6	5	4	3	2	1	
41	41	51	61	71	81	91	101	111	121	131	141	151	161	171	181	191	201	211	221	231	241	251	261	271	281	291					
8	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96	101	106	111	116	121	126	131	136	141	146	151	156	
an	23	de	24	general	25	so	26	Manage	27	pe	28	Regale	29	Sous	30	Nulle															
au	32	de	33	guerre	34	de	35	Honneur	36	pi	37	Rome	38	Morce	39	21. 22. 301															
auec	40	de	41	Ma	42	leur	43	Ngr	44	po	45	Republique	46	an	47	Annulans															
ainsy	49	de	50	be	51	luy	52	Madame	53	pu	54	la	55	voir	56	311. 321. 331															
auray	58	Dans	59	bi	60	de	61	Ministre	62	pour	63	le	64	vr	65	Annulans															
alliance	67	de	68	so	69	le Roy	70	Mantoue	71	paix	72	le	73	vr	74	Annulans															
auec	76	en	77	hu	78	de la Cour ou	79	Modene	80	pas	81	le	82	vr	83	Annulans															
ambassade	85	elle	86	homme	87	de la Cour ou	88	Madrid	89	Prince	90	le	91	vr	92	Annulans															
allemands	93	en	94	honneur	95	elles de la Cour	96	Milan	97	prince	98	le	99	vr	100	Annulans															
auvray	102	auec	103	holande	104	le Redivion	105	Via	106	personne	107	le	108	vr	109	Annulans															
Allemagne	110	ans	111	hongrie	112	le pape	113	ne	114	particulier	115	le	116	vr	117	Annulans															
		enc	120	Ja	121	le pape	122	ne	123	particulier	124	le	125	vr	126	Annulans															