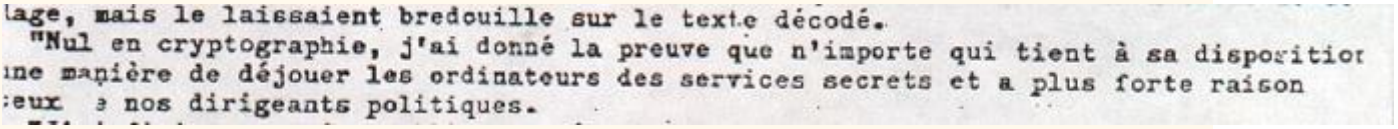
Dans son document « Pierres et Papier », Philippe de Cherisey s'évertue à essayer de nous faire croire qu'il est l'auteur du document appelé le « grand parchemin ». Je passe sur les commentaires périlleux qu'il fait pour arriver à ce résultat. Nous nous doutions qu'il mentait puisque dans le document « L'énigme de Rennes », daté du 27 juillet 1977, il se disait « nul en cryptographie. »


lage, mais le laissaient bredouille sur le texte décodé.
"Nul en cryptographie, j'ai donné la preuve que n'importe qui tient à sa disposition
une manière de déjouer les ordinateurs des services secrets et a plus forte raison
ceux de nos dirigeants politiques.

Or, pour réaliser ce cryptage, il fallait au contraire être un vrai spécialiste de cette discipline. En effet, voici qu'il nous explique comment décoder le parchemin, mais jamais il ne dit comment il a fait pour le coder. Car, malheureusement pour lui, le codage et le décodage ne sont pas symétriques. On ne peut donc employer la méthode qu'il donne pour coder le parchemin mais seulement pour le décoder !

Je vais d'abord m'attacher à expliquer le décodage qu'il indique dans son document.
Celui-ci se fait en trois étapes à partir du moment où l'on a retiré du parchemin les lettres inutiles, c'est-à-dire une lettre toutes les sept lettres.
Voici cette suite :
VCPSJQROVYMYYDLTPEFRBOXTODJLBKNJFQUEPAJYNPPBFEIELRGHIIR
VBTTCVTGD
UCCVMTEJHPNPGSVQJHGMLFTSVJLZQMTOXANPEMUPHKORPKHVJCMC
ATLVQXGGNDT
Soit deux séries de 64 lettres.

Pour simplifier la compréhension, nous allons travailler seulement sur les 64 premières. Mais il nous faut connaître le fonctionnement de deux systèmes de codage, le carré de Vigenère et la marche du cavalier.

Le décodage de Vigenère

Décodage du “F”

Il s’agit d’un système d’alphabets décalés. Là aussi, pour être simple, je ne me servirai que d’une partie de ce carré.

Prenons un mot clef simple, le mot : BAC.
Supposons que nous avons à décoder les lettres suivantes : DZAC.
Nous procédons comme à la bataille navale en nous servant des lettres du mot code dans la 1ère ligne horizontale et des lettres codées dans le côté vertical.
Pour la première lettre, le B (de BAC) en haut se croise avec un D sur le côté vertical en F.
Le A horizontal croise le Z en A.
Le C horizontal croise le A en D.
Je reprends le mot code au début : le B horizontal croise le C en E.
Le mot codé était donc l’adjectif : FADE.

Ce mode de lecture du carré de Vigenère est la « lecture directe ».

Mais pour coder le mot FADE, j'ai utilisé un procédé différent, c'est la « lecture inverse ». À partir du B de BAC, je descends verticalement jusqu'au F de FADE et je lis la lettre codée horizontalement qui est un D.

Codage du "D"

La "marche" du cavalier

C'est un deuxième système de codage appliqué par-dessus le carré de Vigenère. On place 64 lettres sur un échiquier et on les lit en suivant l'ordre de lecture donné par le parcours que peut faire un cavalier sur l'échiquier sans jamais passer deux fois sur la même case.
Voici le parcours à utiliser :

CAVALIER					3		
60	15	46	29	62	17	44	31
47	28	61	16	45	30	63	18
14	59	6	3	8	1	32	43
27	48	9	36	5	34	19	64
58	13	4	7	2	21	42	33
49	26	37	10	35	40	53	20
12	57	24	51	38	55	22	41
25	50	11	56	23	52	39	54

Cavalier

Cases échiquier						
1	2	3	4	5	6	
9	10	11	12	13	14	1
17	18	19	20	21	22	2
25	26	27	28	29	30	3
33	34	35	36	37	38	3
41	42	43	44	45	46	4
49	50	51	52	53	54	5
57	58	59	60	61	62	6

Numérotation normale

Voici comment calculer le cavalier inverse à partir du cavalier direct.
La case 1 du cavalier occupe la case 22 de la numérotation normale d'un échiquier. Je pose donc la case 22 à la première case de l'échiquier du cavalier inverse.
La case 2 est à la place de la case 37 dans la numérotation normale, donc le place la case 37 en deuxième position sur l'échiquier du cavalier inverse.
Je procéde ainsi jusqu'à remplir l'échiquier, ce qui donne la grille suivante, qui est le cavalier inverse du cavalier 3. La numérotation cavalier 1, cavalier 2, 3 ou 4 est donnée par moi tout à fait arbitrairement.

Connaissant maintenant les deux procédés nous pouvons revenir au grand parchemin.

Décodage du grand parchemin

1ère étape :
Je code toutes les lettres extraites avec comme clef l'inverse du texte de la tombe de la marquise d'Hautpoul en ajoutant : PS PRAECUM.

NTESEPTANSDECEDEELEXVIIJANVIERMDCOLXXXIREQUIESCATINPACEPS PRAECUM

Soit : **MUCEARPSPECAPNITACSEIUQERIXXXLOCDMREIVNAJIIVXELEED ECEDSNATPESETN**

J'obtiens la suite :
JYSYKJIIMDPZORUOQHZXKKOZHMHJZXDMJENJZXYZYZZYDJUJQVLKNML KCOKHPZBR

2e étape :
Je recode cette suite de lettres avec le mot MORTEPEE comme « mot-clef »

répété autant de fois qu'il le faut.
J'obtiens :
XNLSPANNASITTIATEHTRSBTEUCAEENIRXTHEENDELORSIALOELEFEDQRPEDCUSGX

3e étape :
Je place ces lettres dans l'ordre de lecture sur les 64 cases d'un échiquier et j'applique la marche du cavalier. Cela donne :
BERGEREPASDETENTATIONQUEPOUSSINTENIERSGARDENTLACLEFPAXDCLXXXIPAR

Ceci est le codage proposé par de Cherisey, mais cela est un décodage. Avec cette formule, on ne peut coder le parchemin ! Mettons-nous dans la peau de celui qui veut cacher cette dernière phrase. Il doit obtenir la suite bleue : XNLSPANNASITTIAT…
Il ne peut le faire qu'en remontant le processus et avec un codage inverse.

Codage du grand parchemin

Appliquons les trois étapes sous leur forme inverse.

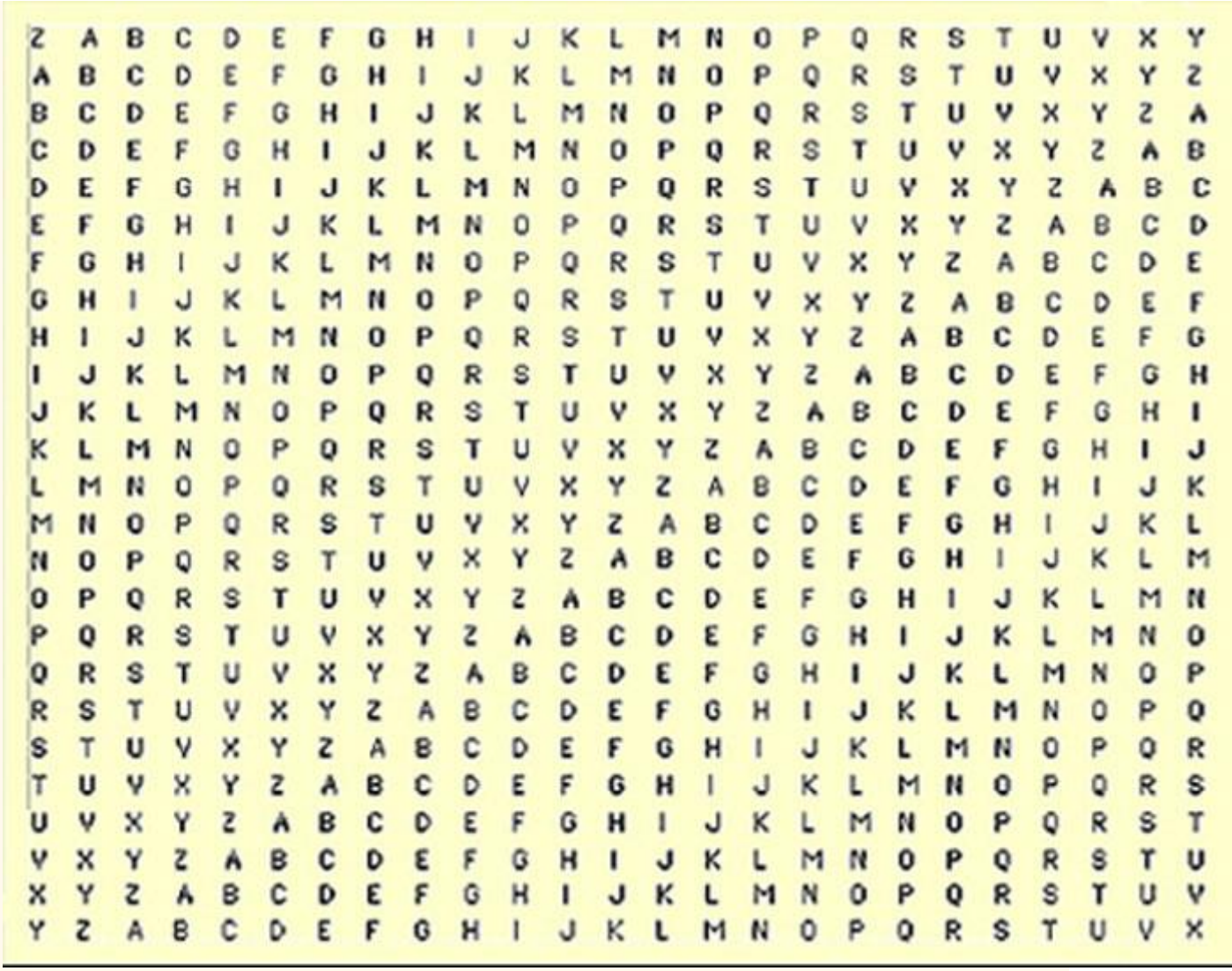
Phrase à coder :
BERGEREPASDETENTATIONQUEPOUSSINTENIERSGARDENTLACLEFPAXDCLXXXIPAR

Avec le cavalier inverse, on obtient :
XNLSPANNASITTIATEHTRSBTEUCAEENIRXTHEENDELORSIALOELEFEDQRPEDCUSGX

Le carré de Vigenère inverse avec la clef MORTEPEE nous donne :
JYSYKJIIMDPZORUOQHZXKKOZHMHJZXDMJENJZXYZYZZYDJUJQVLKNMLKCOKHPZBR

Le carré de Vigenère inverse avec la clef du texte de la tombe de la marquise à l'envers nous donne :
VCPSJQROVYMYYDLTPEFRBOXTODJLBKNJFQUEPAJYNPPBFEIELRGHIIRVBTTCVTGD
Les 64 premières lettres cachées dans le grand parchemin.

Vous pouvez vérifier que cela fonctionne en le faisant vous-mêmes et en faisant la seconde grille de 64 lettres. Mais, attention, le codeur n'a pas utilisé le même cavalier car il y a quatre cavaliers symétriques sur l'échiquier et donc quatre cavaliers inverses. Il suffit de faire un carré de Vigenère complet avec 25 lettres car, à la fin du XIXe siècle, on n'utilisait pas le W. Au passage, ceci aussi permet de dater approximativement le parchemin. Je vous donne donc ici la suite des lettres extraites de la deuxième partie du parchemin
: LUCCVMTEJHPNPGSVQJHGMLFTSVJLZQMTOXANPEMUPHKORPKHVJCMCATLVQXGGNDT



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

Conclusion

Nous pouvons déduire de cet exercice particulier que l'auteur de ce parchemin était un vrai spécialiste du cryptage et que, vu la difficulté du travail, il a été fait pour que ce document reste vraiment occulte. Que ce document a bien une valeur d'authenticité, c'est-à-dire qu'il a été fait pour transmettre quelque chose d'important qui devait rester secret.

Enfin, qu'en aucun cas, ce ne peut être Philippe de Cherisey qui ne parle jamais du codage et qui n'est pas un spécialiste de la cryptographie. D'autant que je me suis laissé dire, de source rapprochée, que lorsque les gens du « Prieuré de Sion » ont découvert ces deux parchemins, ce n'était pas les seuls, il y avait d'autres documents. En particulier il y avait un texte expliquant comment décoder ce manuscrit. Sinon personne sans aucun doute n'eut trouvé la solution, à moins d'un travail colossal de décryptage qui eût nécessité une équipe pour arriver à « casser » le mot-clef « Mortépée » puis le texte-clef de la tombe. Car, assurément, personne n'aurait pu faire le rapprochement entre ce manuscrit et le texte gravé sur cette dernière.

En conclusion, de Cherisey, comme on le sait, a voulu discréditer le livre de Gérard de Sède et a donc imaginé une histoire rocambolesque pour prouver l'improuvable, mais le manuscrit suffit à se défendre lui-même.
Rien ne prouve que c'est un de ceux que Saunière a découvert, sinon qu'il fallait se servir de la tombe du cimetière de Rennes pour comprendre. Et qu'un jour, quelqu'un lui a demandé d'effacer le texte de la tombe, donc de faire disparaître les deux clefs qui y figuraient…

14 janvier 2007, mise à jour 7 décembre 2019, Daniel Dugès ©