La cryptologie dans la littérature

Didier Müller

(didiermuller.ch)

Champéry, 10 septembre 2024

Sommaire

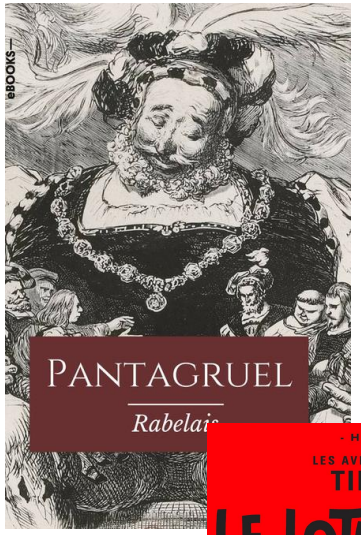
Première partie

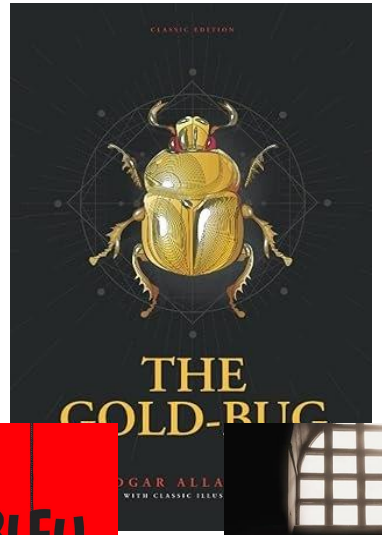
10 exemples de cryptologie dans la littérature

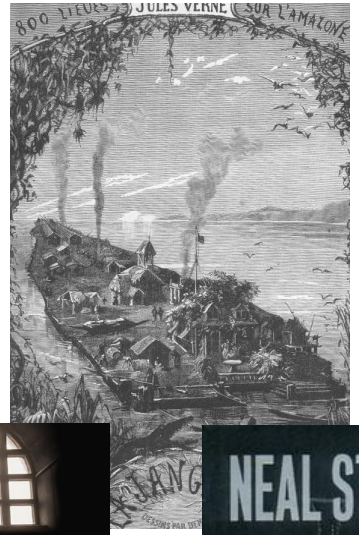
Seconde partie

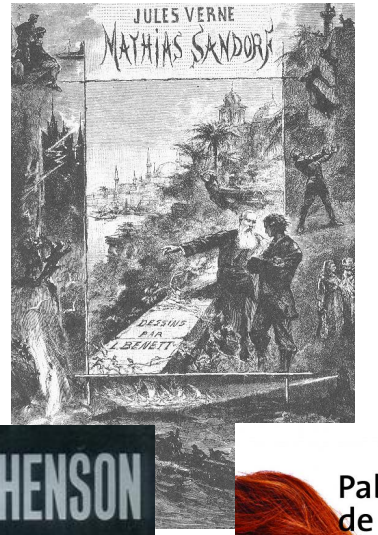
Les 9 couronnes

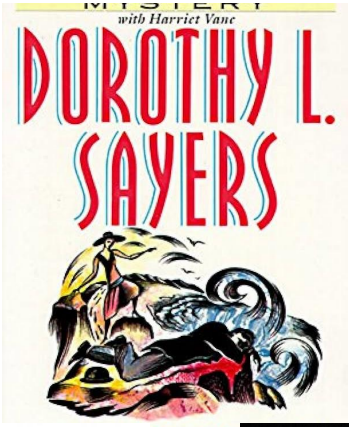
Première partie

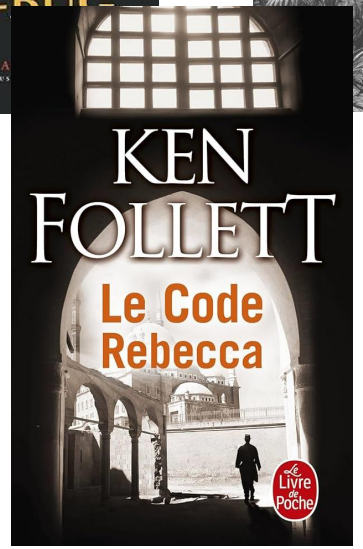


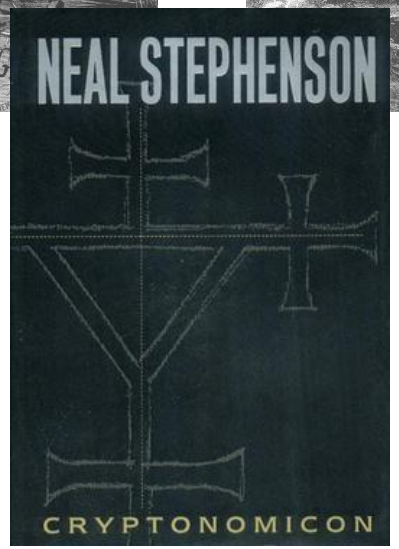


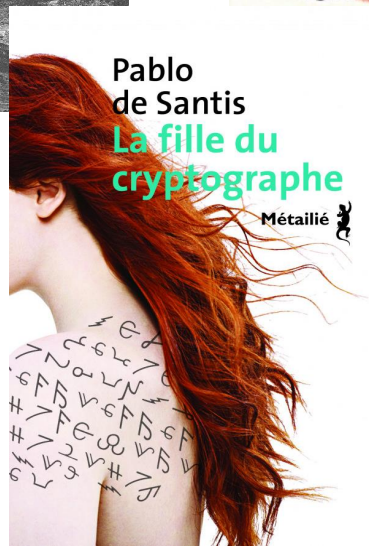


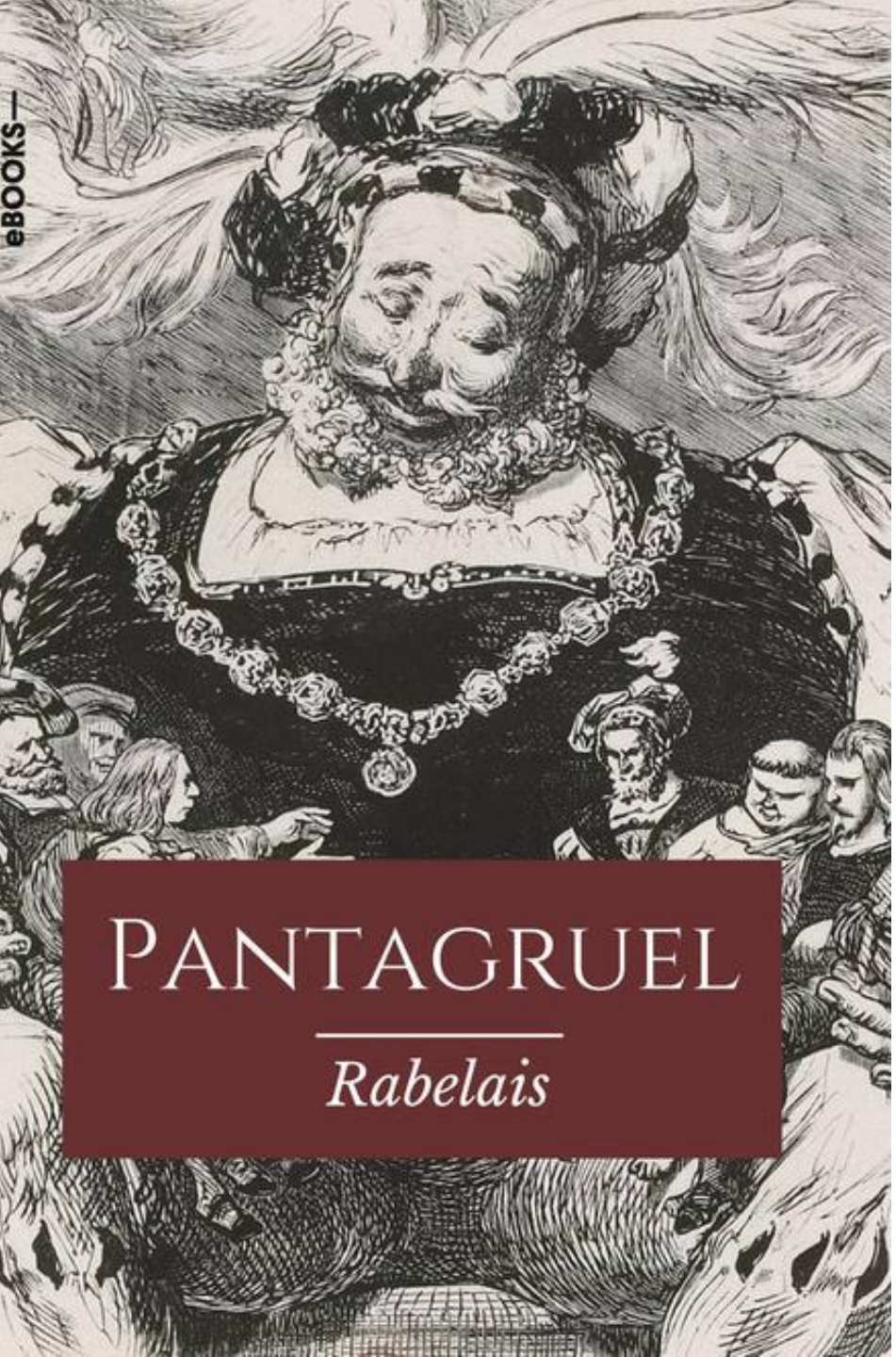












Pantagruel (1532)

François Rabelais, 1483 (ou 1494?) - 1553

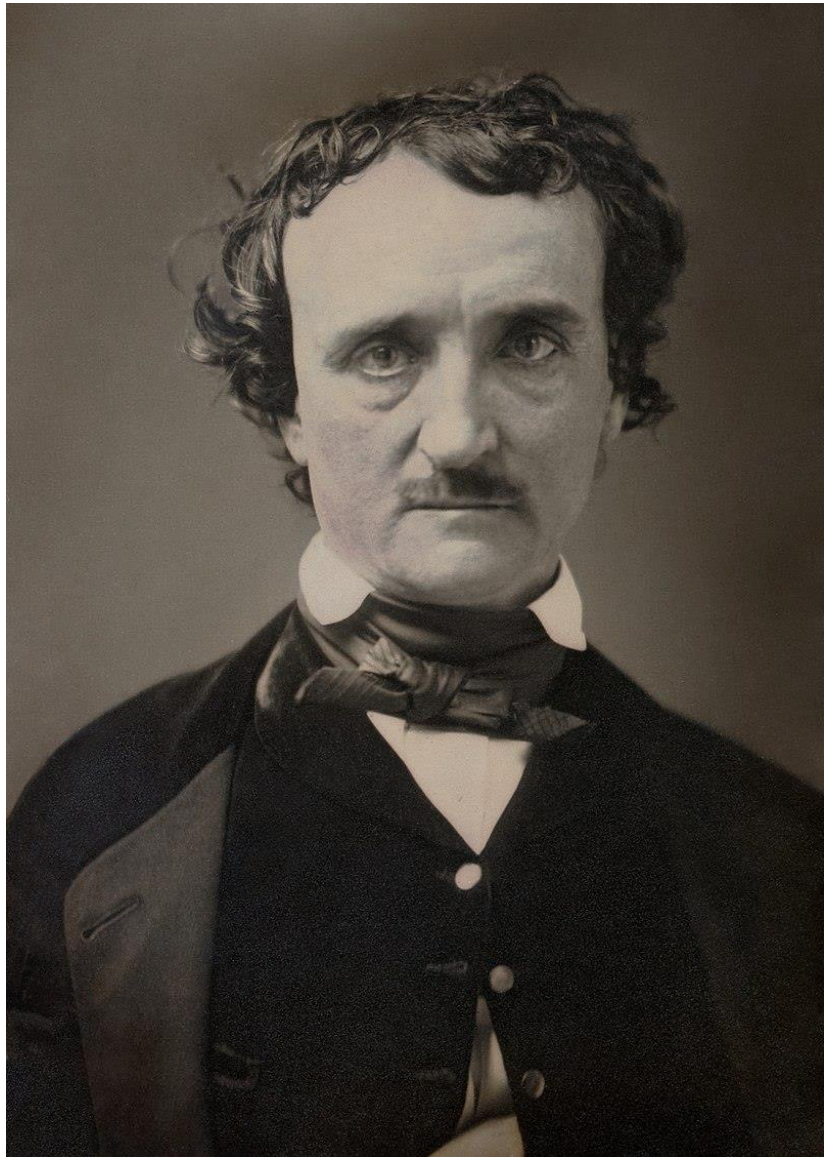
- Le chapitre 24 traite des **encres invisibles**.
- **Fun fact :** C'est sous le pseudonyme d'*Alcofribas Nasier* que François Rabelais publia *Pantagruel* et *Gargantua*.

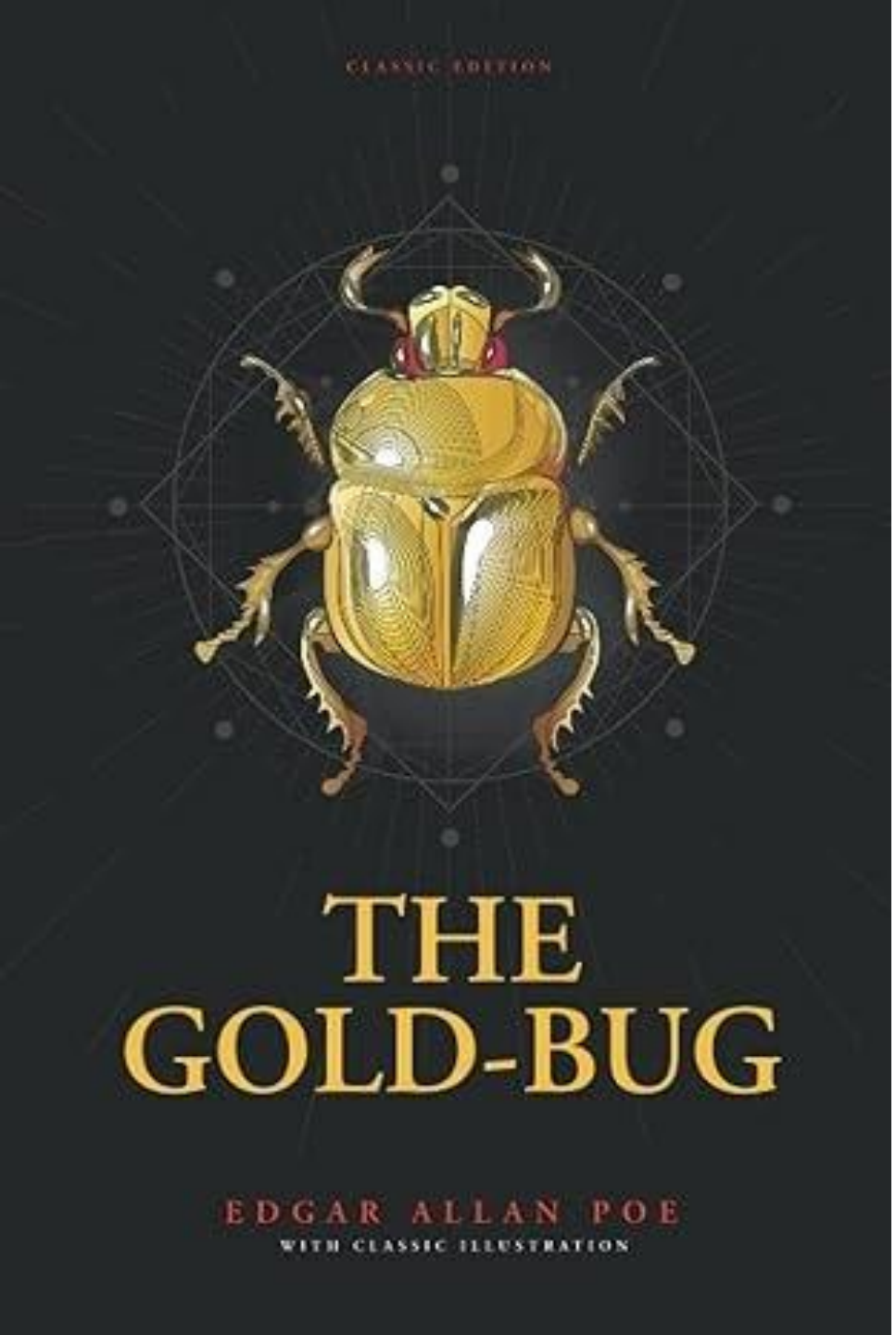
Alcofribas Nasier ?!

francois rabelais

Edgar Allan Poe (1809-1849)

- Poe était féru de cryptographie et se faisait fort de décrypter n'importe quelle **substitution simple (monoalphabétique)**.
- *Le scarabée d'or* est sa nouvelle la plus connue.
- "A Few Words on Secret Writing", Graham's Magazine, July 1841, pp. 33-38





Le scarabée d'or (1843)

Substitution monoalphabétique

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;1‡)
;:‡*8†83(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:*‡(;4
956*2(5*—4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48081;
8:8‡1;48†85;4)485†528806*81(‡9;48;(88;4(‡?34;48
)4‡;161;:188;‡?;

Le scarabée d'or

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;
e e e e e

1‡(;:‡*8†83(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:
e e ee ee e e

*‡(;4956*2(5*-4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48
e e e e e

081;8:8‡1;48†85;4)485†528806*81(‡9;48;(88
e e e e e ee e e ee

;4(‡?34;48)4‡;161;:188;‡?;
e ee

Le scarabée d'or

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;
the h h te the e e t

1‡(;:‡*8†83(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:
t e e ee th tee te the t

*‡(;4956*2(5*-4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48
th h e e th e t e h t the

081;8:8‡1;48†85;4)485†528806*81(‡9;48;(88
e te e the e th he ee e thet ee

;4(‡?34;48)4‡;161;:188;‡?;
th hthe h t t eet t

Le scarabée d'or

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;
the h h te the e e t

1‡(;:‡*8†83(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:
rt e e ree th rtee te rthe t

*‡(;4956*2(5*-4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48
rth r h e e th e t e h t r the

081;8:8‡1;48†85;4)485†528806*81(‡9;48;(88
e te e the e th he ee e r thetree

;4(‡?34;48)4‡;161;:188;‡?;
thr hthe h t t eet t

Le scarabée d'or

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;
goo g the ho ho te the e e t

1‡(;:‡*8†83(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:
ort o e egree th rtee ute orthe t

*‡(;4956*2(5*-4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48
orth r h e e th e t e hoot ro the

081;8:8‡1;48†85;4)485†528806*81(‡9;48;(88
e te eo the e th he ee e ro thetree

;4(‡?34;48)4‡;161;:188;‡?;
throughthe hot t eetout

Le scarabée d'or

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;
goodg the ho ho te thede e t

1‡(;:‡*8†83(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:
ort o edegree dth rtee ute orthe t d

*‡(;4956*2(5*-4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48
orth r h e e th e t de hoot ro the

081;8:8‡1;48†85;4)485†528806*81(‡9;48;(88
e te eo thede th he d ee e ro thetree

;4(‡?34;48)4‡;161;:188;‡?;
throughthe hot t eetout

Le scarabée d'or

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;
goodg inthe i ho ho te inthede i e t

1‡(;:‡*8†83(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:
ort onedegree ndthirteen inute northe t nd

*‡(;4956*2(5*-4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48
north in r n h e enth i e t ide hoot ro the

081;8:8‡1;48†85;4)485†528806*81(‡9;48;(88
e te eo thede th he d ee ine ro thetree

;4(‡?34;48)4‡;161;:188;‡?;
throughthe hot i t eetout

Le scarabée d'or

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;
Agoodg a inthe i ho ho te inthede i eat

1‡(;:‡*8†83(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:
 ort onedegree andthirteen inute northea tand

*‡(;4956*2(5*-4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48
north ain ran h e enth i ea t ide hoot ro the

081;8:8‡1;48†85;4)485†528806*81(‡9;48;(88
 e te eo thedeath heada ee ine ro thetree

;4(‡?34;48)4‡;161;:188;‡?;
throughthe hot i t eetout

Le scarabée d'or

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;
Agoodg assinthe isho shoste inthede i sseat

1‡(;:‡*8†83(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:
 ort onedegreesandthirteenminutesnortheastand

*‡(;4956*2(5*-4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48
northmain ran hse enth im eastsideshoot romthe

081;8:8‡1;48†85;4)485†528806*81(‡9;48;(88
 e te eo thedeathsheada ee ine romthetree

;4(‡?34;48)4‡;161;:188;‡?;
throughtheshot i t eetout

Le scarabée d'or

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;
Agoodg assinthe isho shoste inthede i sseat

1‡(;:‡*8†83(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:
fort onedegreesandthirteenminutesnortheastand

*‡(;4956*2(5*-4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48
northmain ran hse enth im eastsideshootfromthe

081;8:8‡1;48†85;4)485†528806*81(‡9;48;(88
 efte eofthedeathsheada ee inefromthetree

;4(‡?34;48)4‡;161;:188;‡?;
throughtheshotfift feetout

Le scarabée d'or

5 3‡‡† 305)) 6* ;48 26)4‡.) 4‡);80 6* ;48 †8¶60))85;
A good glass in the bishop's hostel in the devil's seat

1‡(;: ‡*8 †83(88) 5*† ;46(;88* 96*?;8) *‡(;485); 5*† 2:
forty-one degrees and thirteen minutes northeast and by

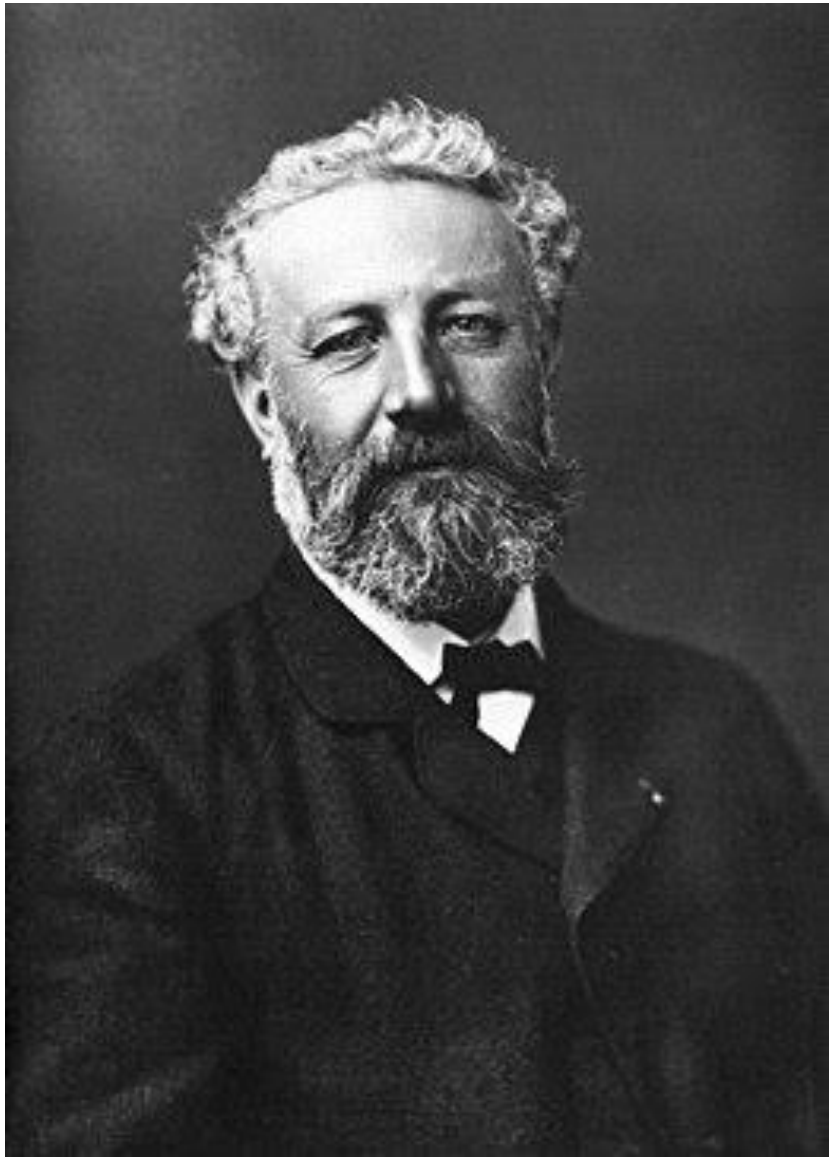
‡(;4 956 2(5*-4)8¶8*;4 0692 85);)6†8)4‡‡; 1(‡9 ;48
north main branch seventh limb east side shoot from the

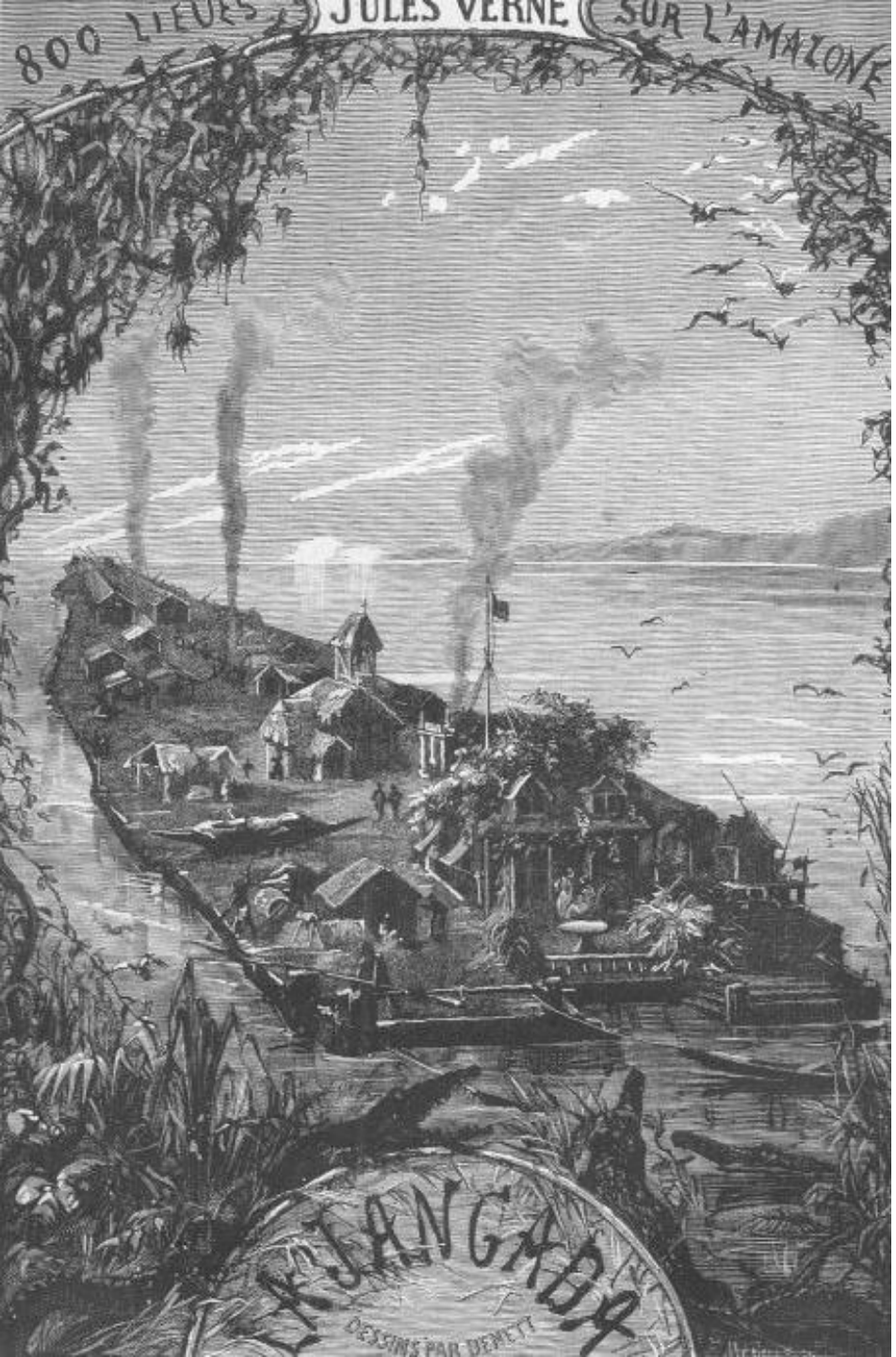
081; 8:8 ‡1 ;48 †85;4) 485† 5 288 06*8 1(‡9 ;48 ;(88
left eye of the death's-head a bee line from the tree

;4(‡?34 ;48)4‡; 161;: 188; ‡?;
through the shot fifty feet out

Jules Verne (1828-1905)

- **La Jangada**, deuxième partie, chapitres XII-XIX
- **Mathias Sandorf**, première partie, chapitre IV
- **Voyage au centre de la Terre**, chapitres II à V
- **Les enfants du capitaine Grant**, première partie, chapitre II





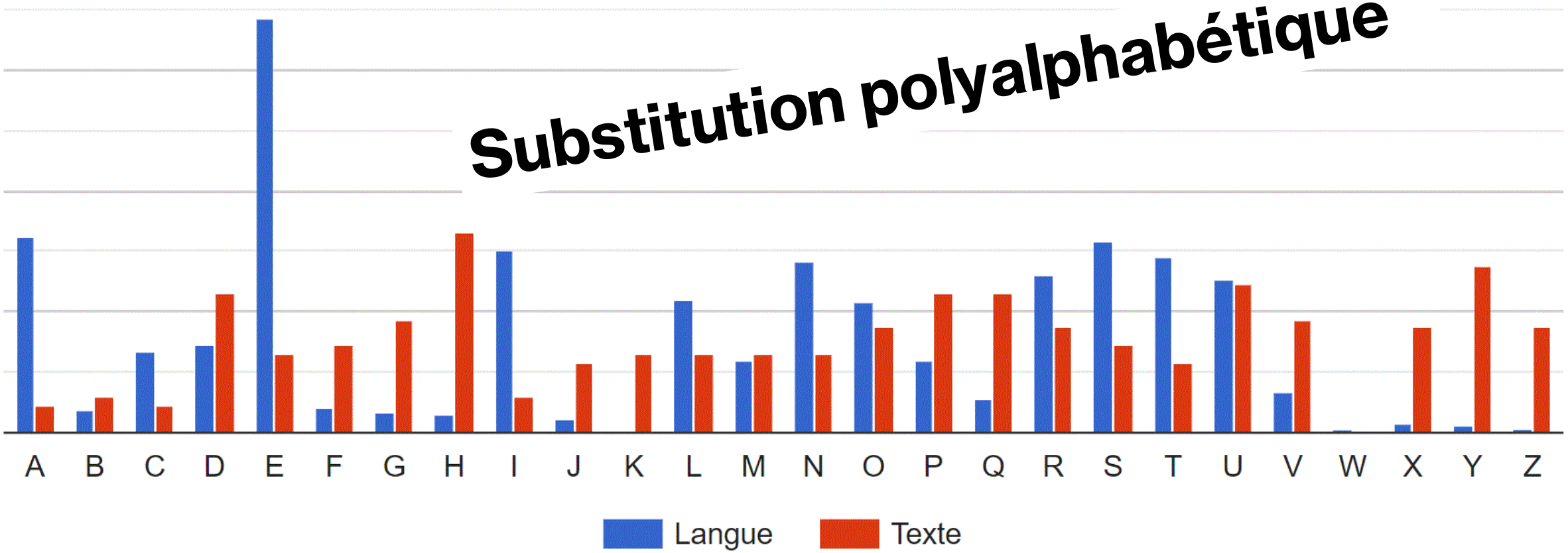
La Jangada (1881)

- Le chiffre utilisé est le chiffre de Gronsfeld (une variante du chiffre de Vigenère).
- C'est une **substitution polyalphabétique**.
- Jules Verne utilise la technique du **mot probable** pour le décrypter.

La Jangada : le cryptogramme

Phyjslyddqfdzxgasgzzqqehxgkfndrxujugiocytdxv
ksbxhhuypohdvyrymhuhpuydkjoxphetozsletnpm
vffovpdpajxhyynojyggaymeqynfuqlnmvlyfgsuzm
qiztlbqgyugsqeubvnrcredgruzblrmxyuhqhpzdrrg
crohepqxufivvrplphonthvddqfhqsntzhhhnfepmqk
yuuexktogzgkyuumfvijdqdpzjqsykrplxhxqrymvkl
ohhhotozvdksppsuvjhd.

La Jangada : histogramme des fréquences



La Jangada : un mot probable (crib)

```
Phyjslyddqfdzxgasgzzqqehxgkfndrxu...

                    ...qrymvklohhhotozvdksppsuvjhd
                                                Ortega
                                                432513
```

La Jangada : décryptement

Phyjslyddqfdzxgasgzzqqehxgkfndrxu

Leweriuableavuevrdvwolde...

432513432513432513432513...

...eqrymvklohhhotozvdksppsuvjhd

...demonwrainomOrtega

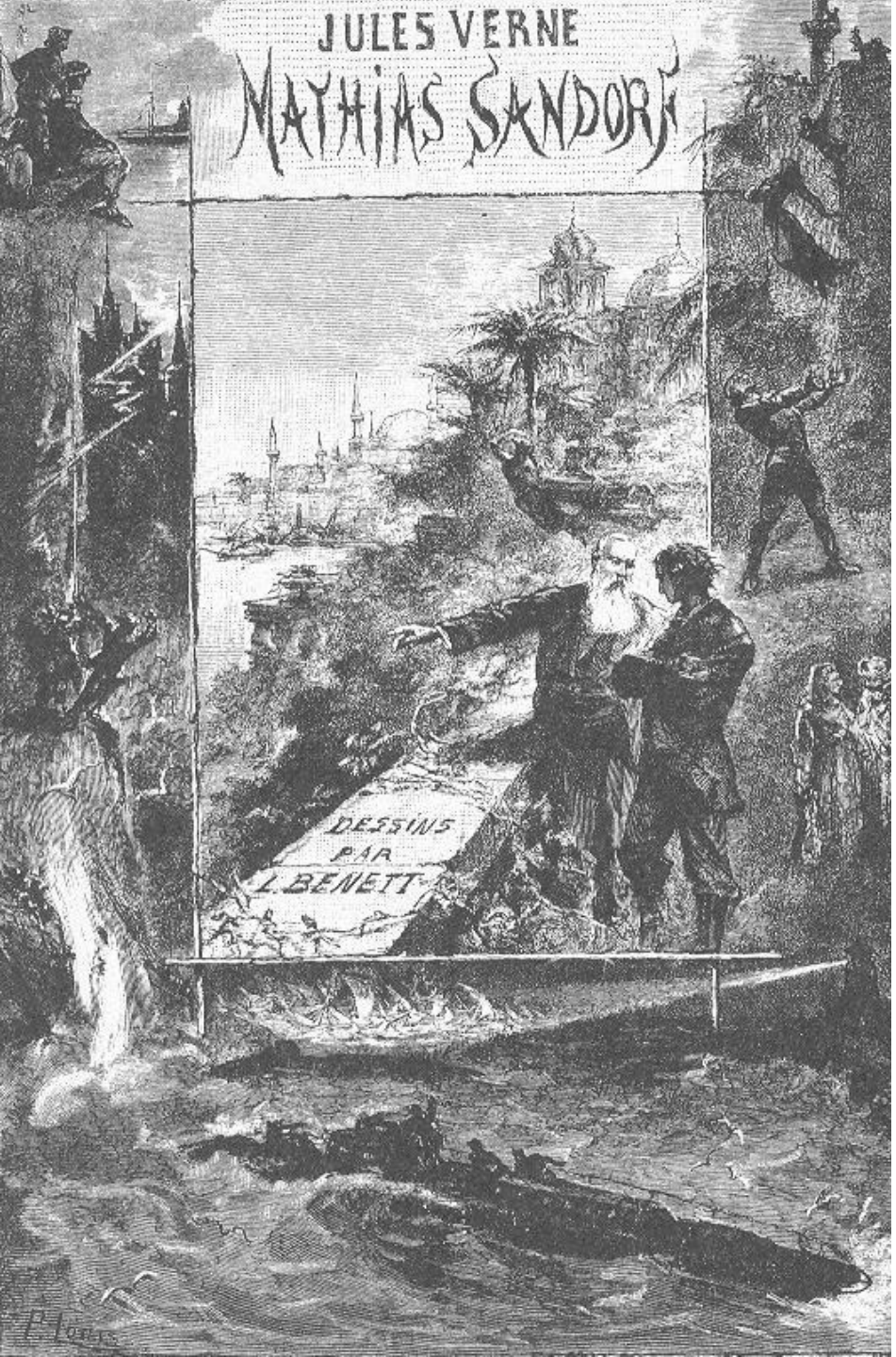
...432513432513432513

La Jangada : erreur… ou pas ?

- Quand *La Jangada* a été écrite, le w n'était pas *vraiment* une lettre de l'alphabet.
- *Le Grand Robert* ne la reconnaît comme 23^{e} lettre de l'alphabet qu'en 1964, tandis que le *Petit Larousse* l'avait intégrée depuis 1948.

- Il n'y a donc pas d'erreur et le texte commence par :

  "Le véritable auteur du vol de..."



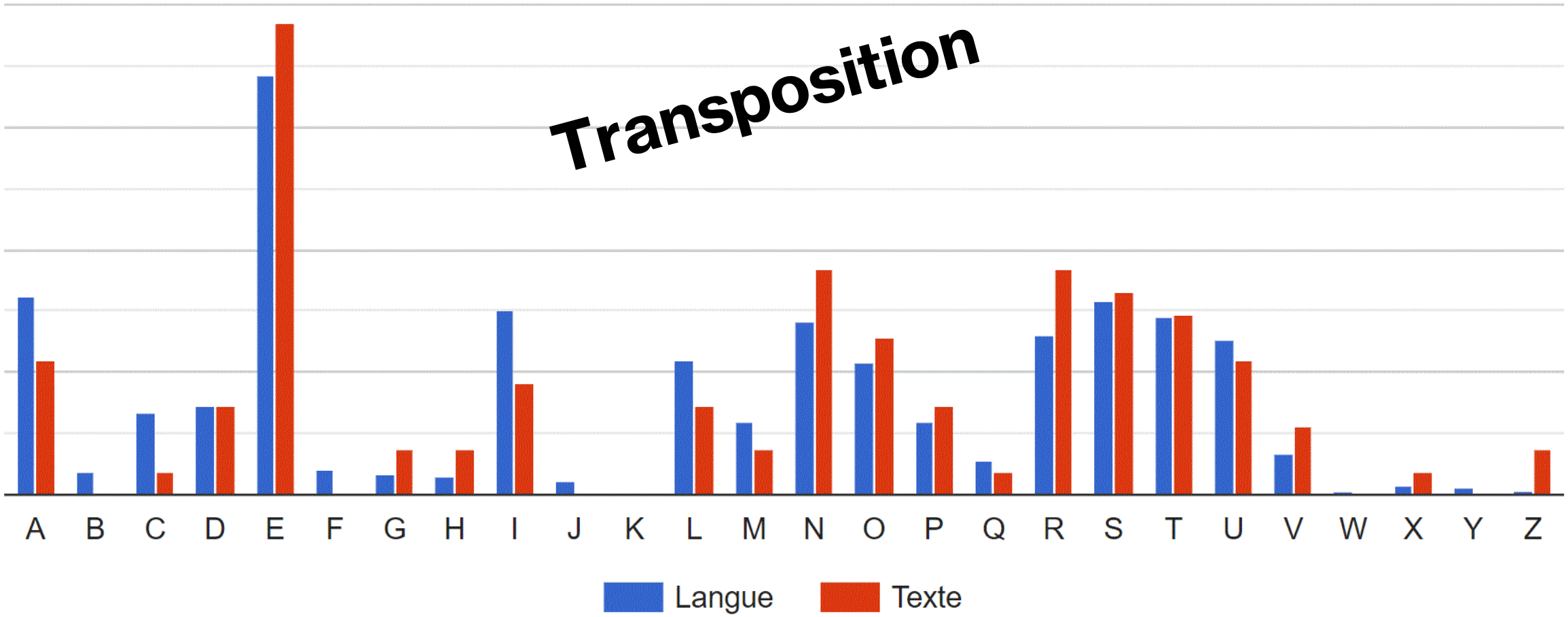
Mathias Sandorf (1885)

- Dans ce roman, Jules Verne utilise une **grille tournante**.
- Invention du colonel autrichien Eduard B. Fleissner von Wostrowitz (1825-1888).
- On mélange les lettres mais on ne les remplace pas. C'est une **transposition**.

Mathias Sandorf : le texte chiffré

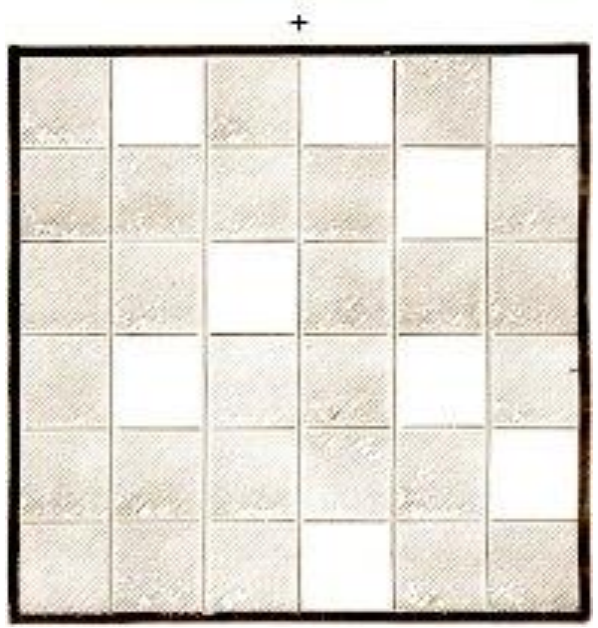
```
ihnalz zaemen ruiopn
arnuro trvree mtqssl
odxhnp estlev eeuart
aeeeil ennios noupvg
spesdr erssur ouitse
eedgnc toeedt artnee
```

Mathias Sandorf : histogramme



Mathias Sandorf : le cache

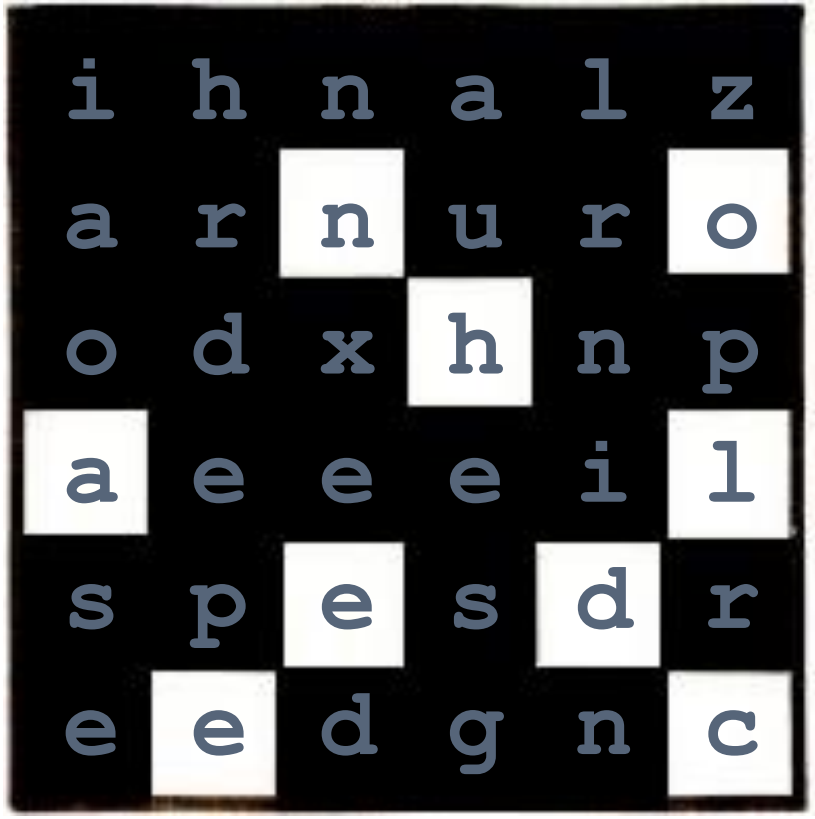
- Cache utilisé par Jules Verne dans le roman :



Mathias Sandorf : le cache

hazrxeirg

Mathias Sandorf : le cache



hazrxeirg

nohaledec

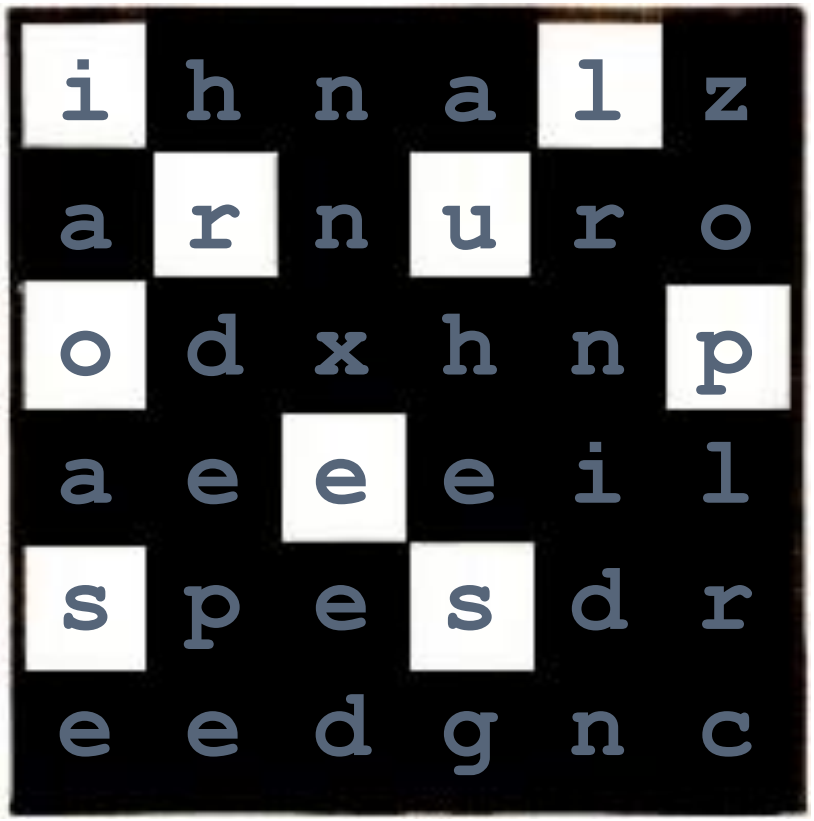
Mathias Sandorf : le cache

hazrxeirg

nohaledec

nadnepedn

Mathias Sandorf : le cache



hazrxeirg

nohaledec

nadnepedn

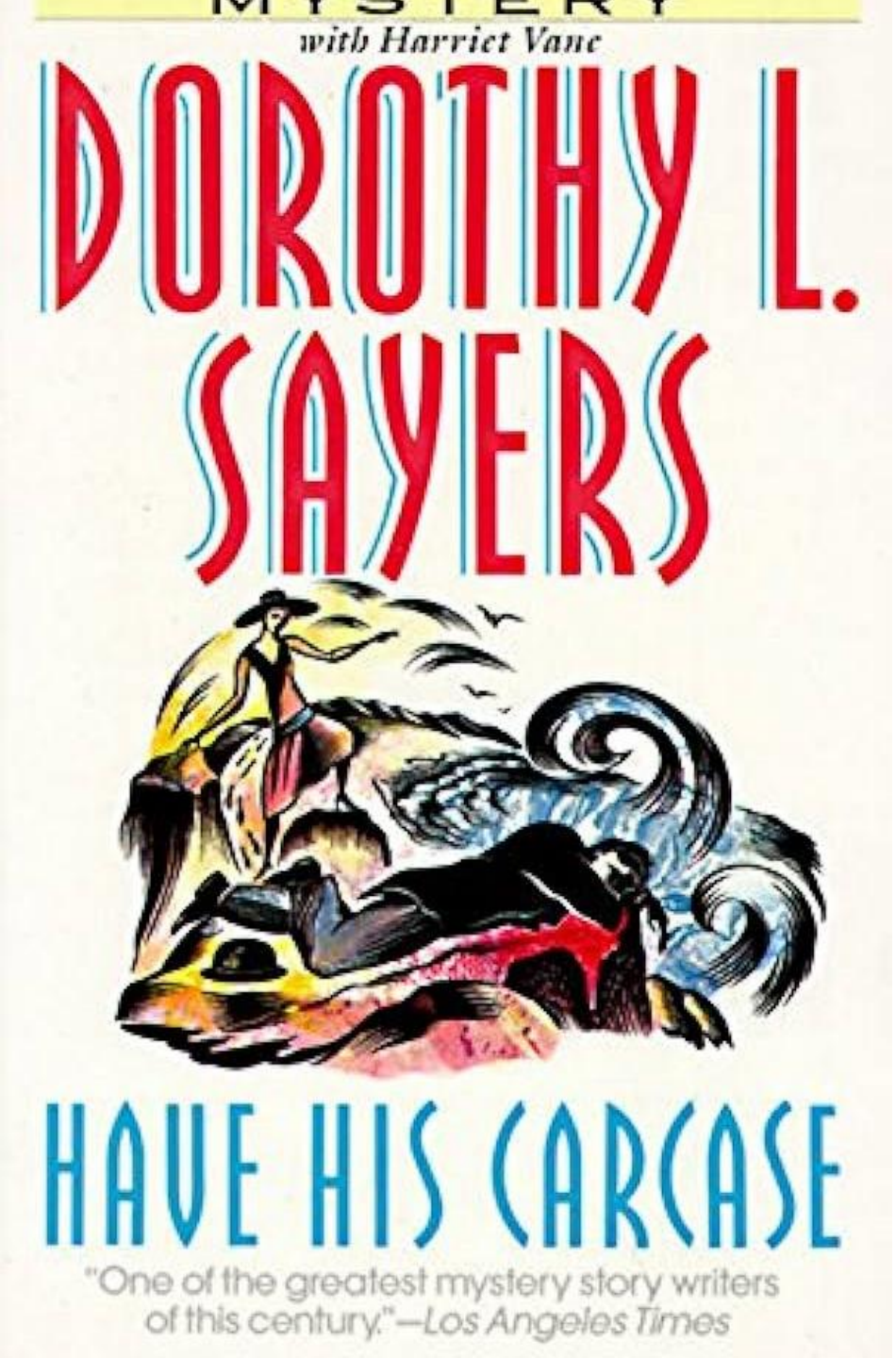
ilruopess

Mathias Sandorf : le texte clair

Pour compliquer le décryptement, le texte a été surchiffré : avant de mélanger les lettres avec le cache tournant, on a écrit le texte de droite à gauche.

Message clair :

Tout est prêt. Au premier signal que vous nous enverrez de Trieste, tous se lèveront en masse pour l'indépendance de la Hongrie. Xrzah.



Have his carcase (1932)

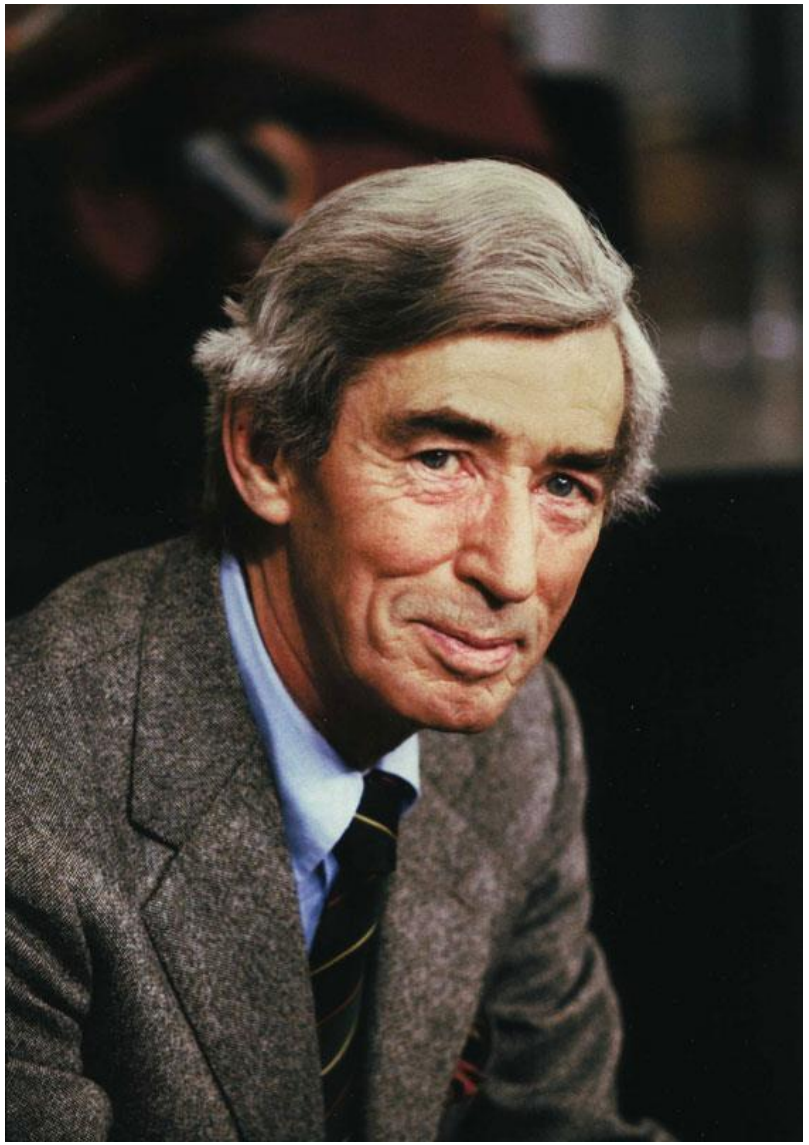
Dorothy L. Sayers, 1893-1957, britannique

- On y trouve au chapitre 28 la description du **chiffre de Playfair** et comment le décrypter.
- **Fun fact :** ce chapitre a été supprimé dans la version française (trop dur à traduire ?)

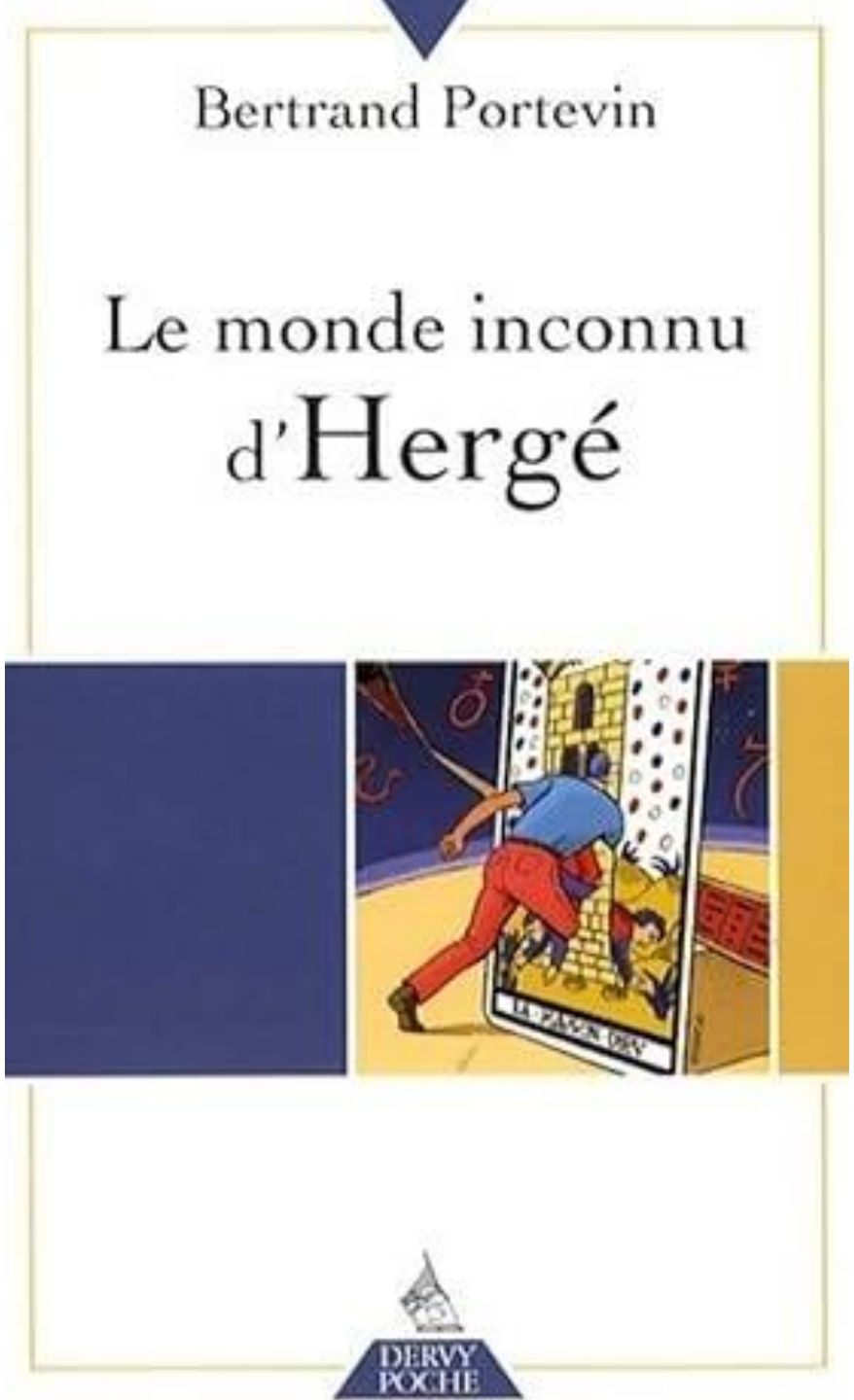
Hergé (1907-1983)

- Hergé, très amateur de tarots, aurait puisé son inspiration dans l'occultisme, la mythologie, la franc-maçonnerie, etc.

- **Le lotus bleu**
- **Le secret de la Licorne**
- **Vol 714 pour Sydney**



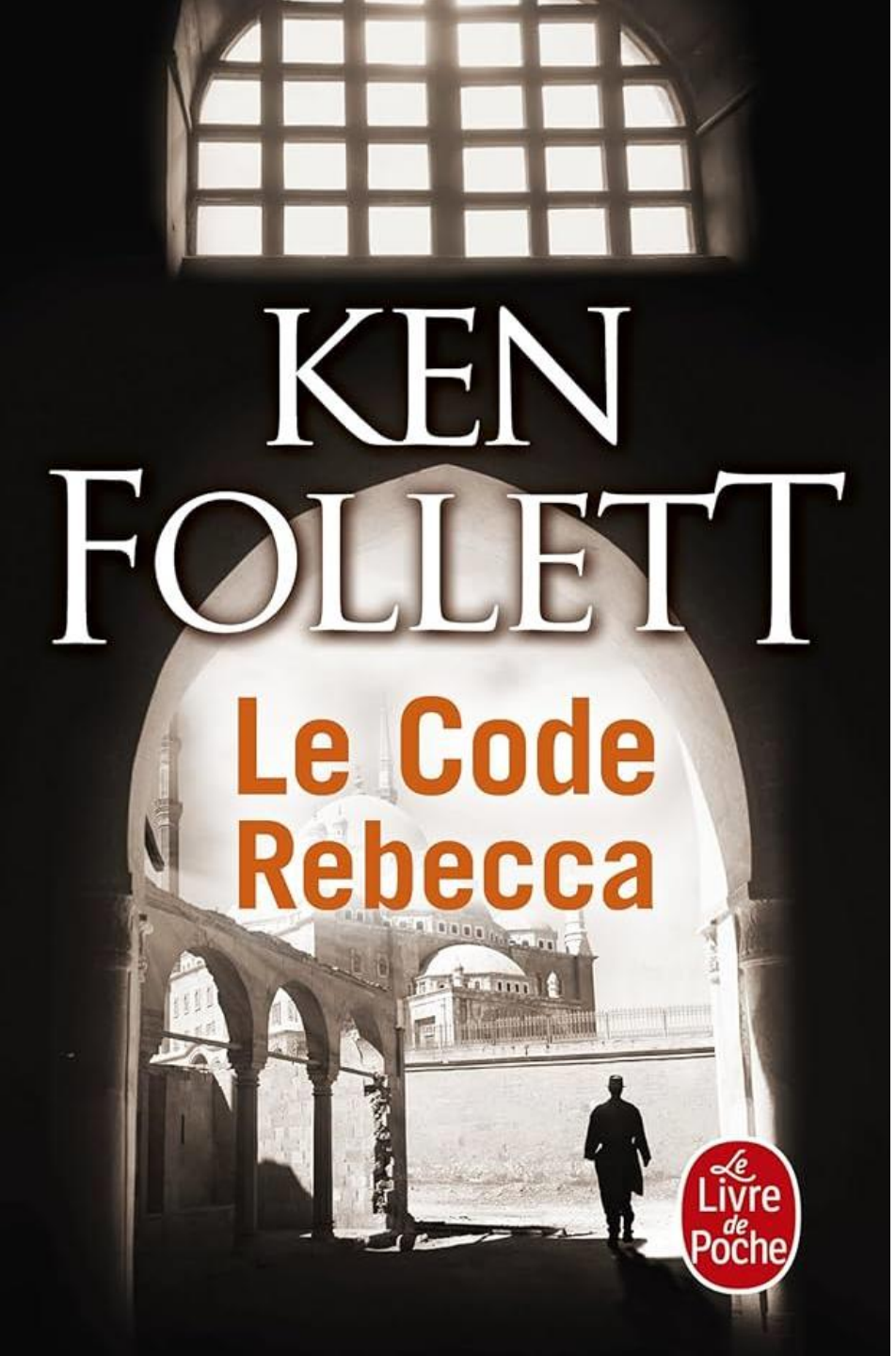
Le lotus bleu (1936)



Le monde inconnu d'Hergé

Bertrand Portevin analyse case par case l'album *Vol 714 pour Sydney* (1968) sous l'angle du symbolisme :

- alchimie,
- franc-maçonnerie,
- occultisme,
- jeux de mots,
- …



Le code Rebecca (1980)

Ken Follett, né en 1949, britannique.

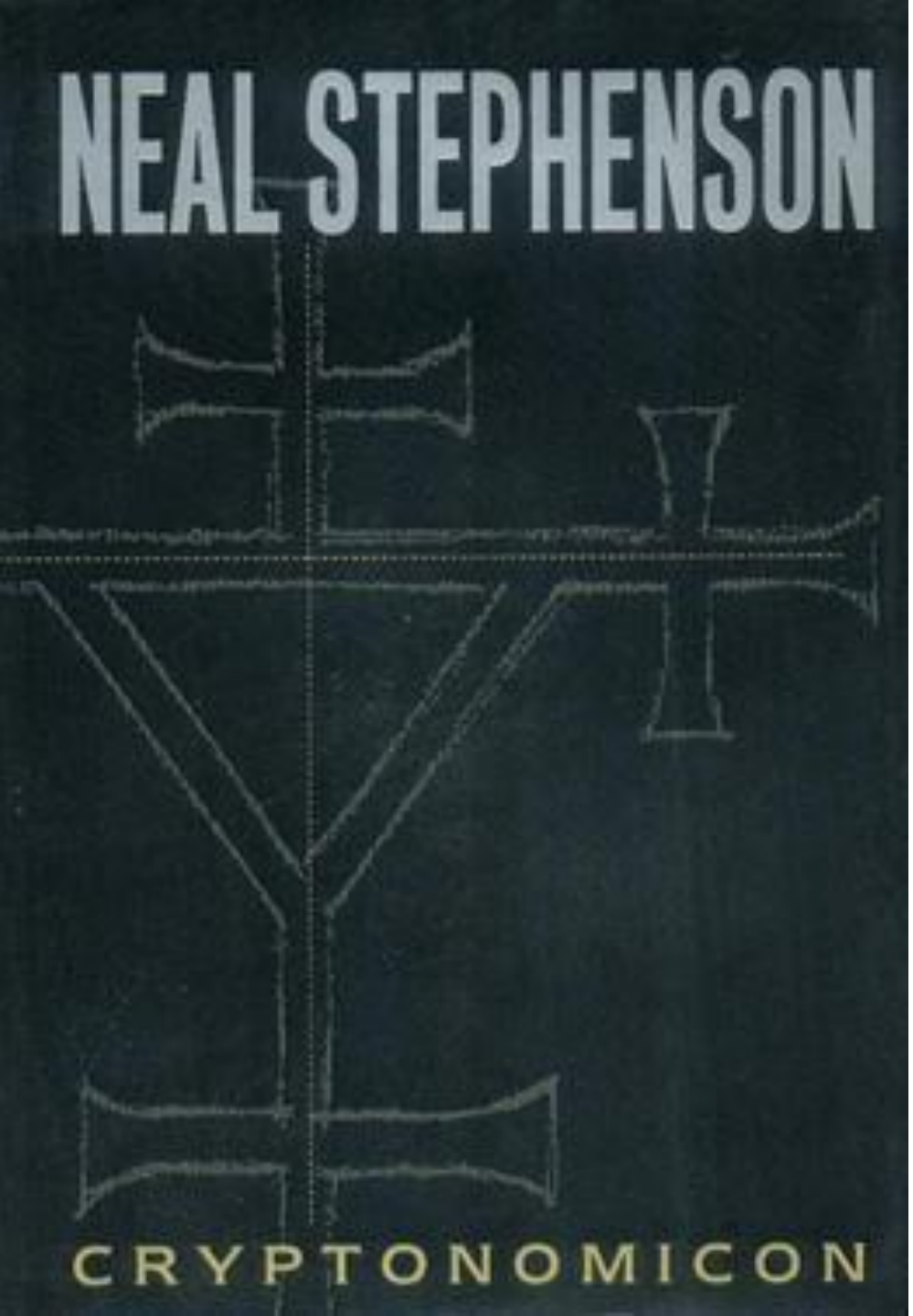
- On y trouve une description d'un code basé sur un livre intitulé *Rebecca*.
- C'est un **code du livre** (ou **système du dictionnaire**).

Le code Rebecca (extrait)

[...] Wolff s'approcha du buffet où il dissimulait l'émetteur radio. Il prit le roman anglais et la feuille de papier sur laquelle était inscrit le chiffre du code. Il l'étudia. On était aujourd'hui le 28 mai. Il fallait ajouter 42 - le chiffre de l'année - à 28 pour arriver au numéro de la page du roman qu'il devait utiliser pour coder son message. Mai était le cinquième mois de l'année, aussi allait-il supprimer une lettre sur cinq dans la page.

Le code Rebecca (suite de l'extrait)

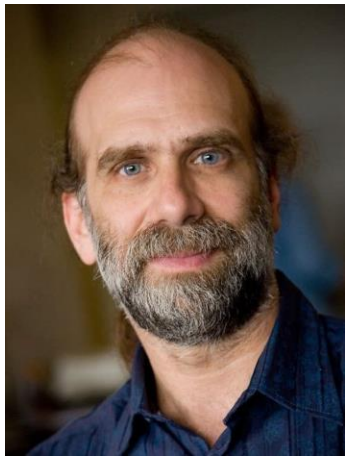
Il décida d'envoyer comme message SUIS ARRIVE. M'INSTALLE. ACCUSEZ RECEPTION. Commençant en haut de la page 70 du livre, il chercha la lettre S. En supprimant une lettre sur cinq, le S était le dixième caractère de la page. Dans son code, il serait donc représenté par la dixième lettre de l'alphabet, le J. Il fallait ensuite un U. Dans le livre, la troisième lettre après le S était un U. Le S de SUIS serait donc représenté par la troisième lettre de l'alphabet, le C. Il y avait des façons particulières pour représenter les lettres rares, comme le X, par exemple. […]

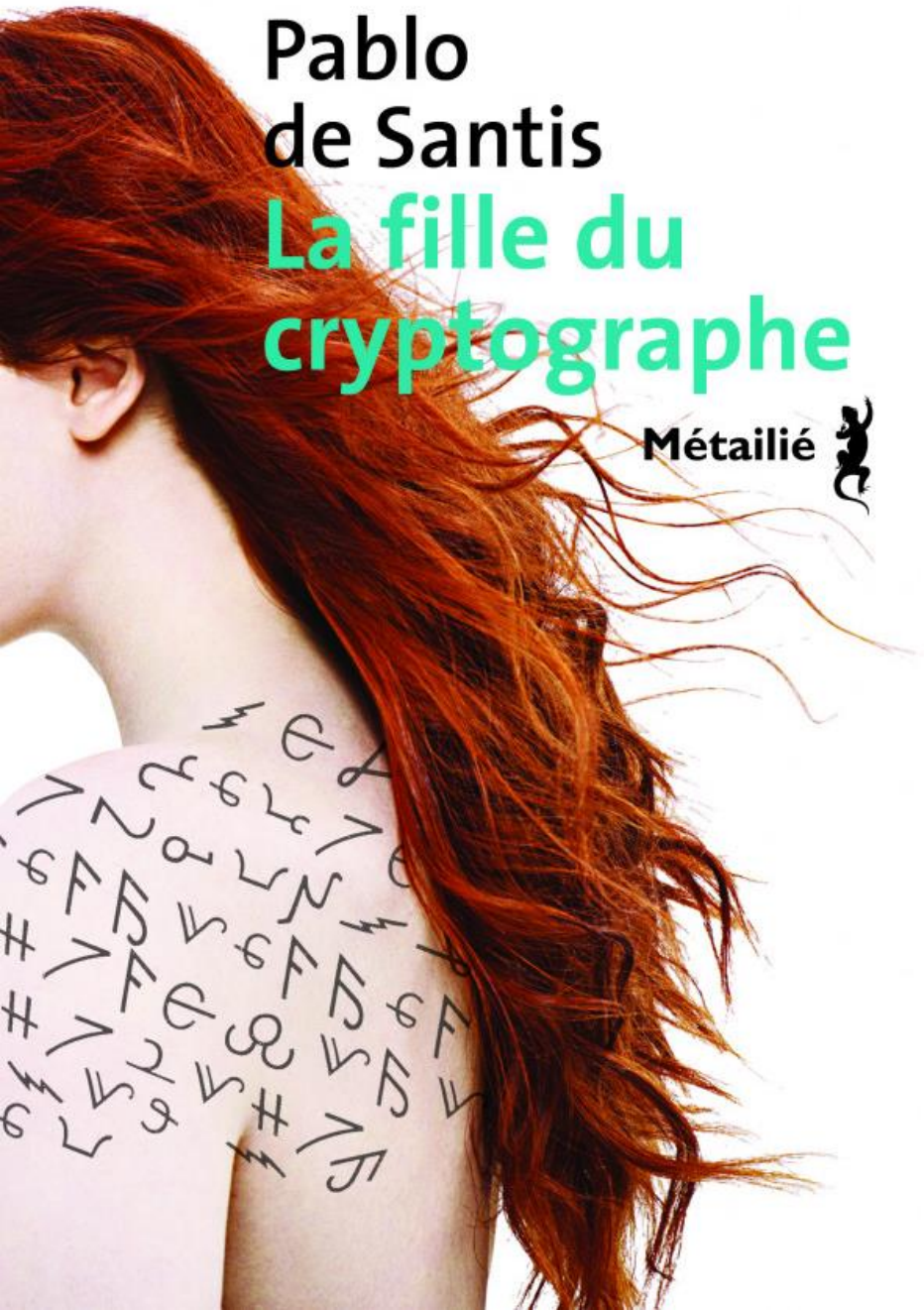


Cryptonomicon (1999)

Neal Stephenson, né en 1959, USA

- Le cryptologue Bruce Schneier a conçu pour ce roman un cryptosystème robuste nommé **Solitaire** (*Pontifex* dans le livre) utilisant un jeu de 54 cartes.

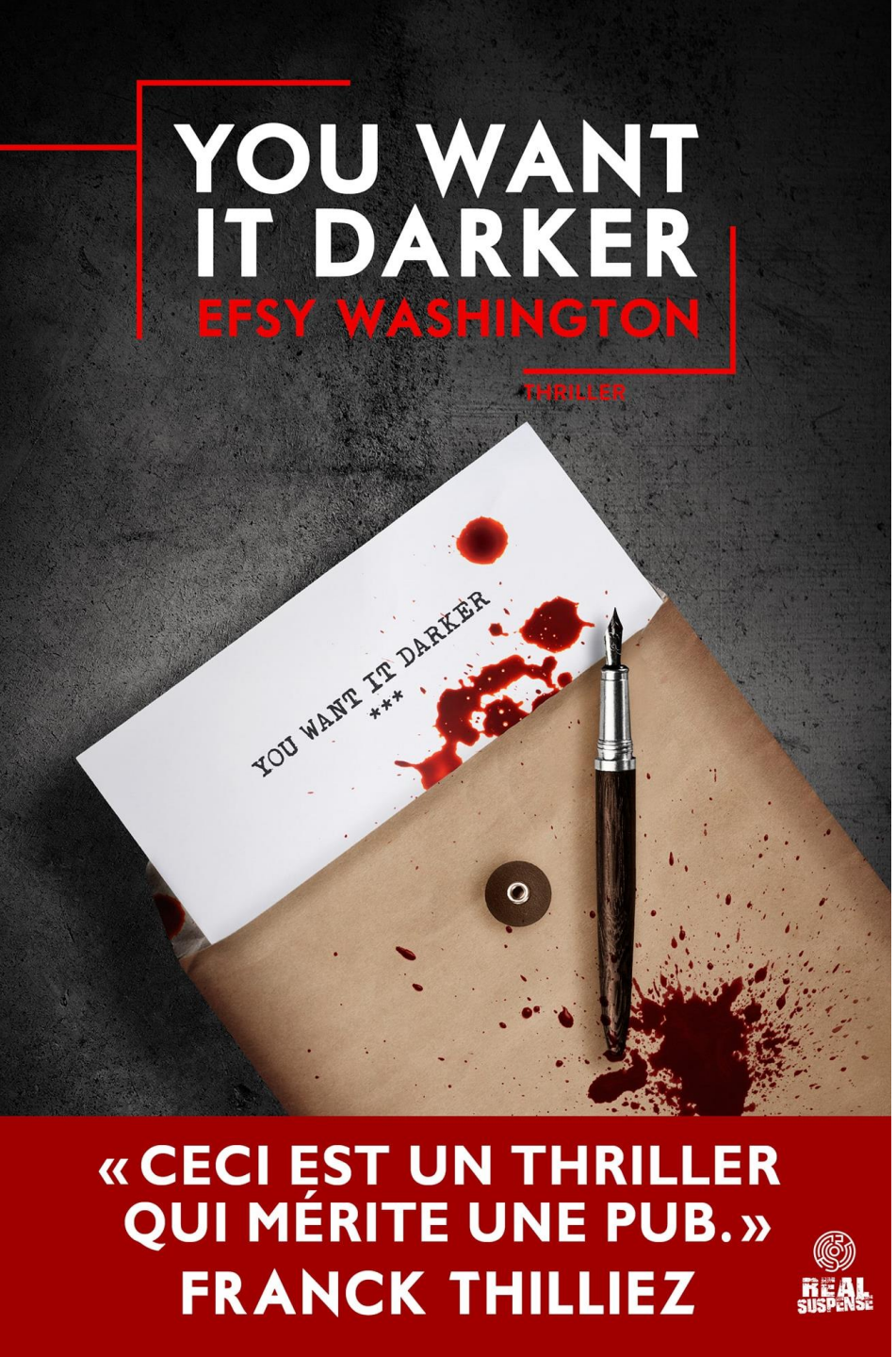




La fille du cryptographe (2017)

Pablo de Santis, né en 1963, Argentine

- On y trouve la description du **chiffre de Vigenère** (chapitre "Un message secret")
- Cryptogramme de 28 lettres seulement
- On cherche à deviner la clef (pas réaliste)



You want it darker (2023)

Efsy Washington (pseudonyme)

- Qui est Efsy Washington, l'ami(e) de Franck Thilliez ?
- Pour le découvrir, il faudra décrypter le "Kryptos".

You want it darker : le cryptogramme

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

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

You want it darker : Kryptos

D'autres livres...

https://www.4el.ch/crypto/litterature/

Seconde partie

DIDIER MÜLLER

Les 9 couronnes (2009)

- Ecrit à Saint-Pétersbourg (2004-05)
- Idée : écrire un cours de cryptologie sous forme d'un roman policier
- Chacun des 9 chapitres commence par un message codé laissé par un tueur en série

Les 9 couronnes (premier courriel, début)

De : Stéphane Périat <Stephane.Periat@jura.ch>
Date : Thu, 9 Sep 2004 11:44:42 +0200
A : <crypto@apprendre-en-ligne.net>
Objet : besoin d'aide

Salut Max,
Je sais que tu es à Saint-Pétersbourg pour une dizaine de mois, mais j'ai besoin de toi! En effet, un meurtre étrange a eu lieu ce matin à Seleute. Un vieillard a été tué de deux balles dans le coeur. Il était coiffé d'une couronne de laurier et, dans sa bouche, nous avons trouvé un message codé.
C'est là que j'ai besoin de toi. Je sais que tu as donné un cours de cryptographie au Lycée cantonal de Porrentruy et j'ai pensé que tu pourrais m'aider à déchiffrer le message codé.

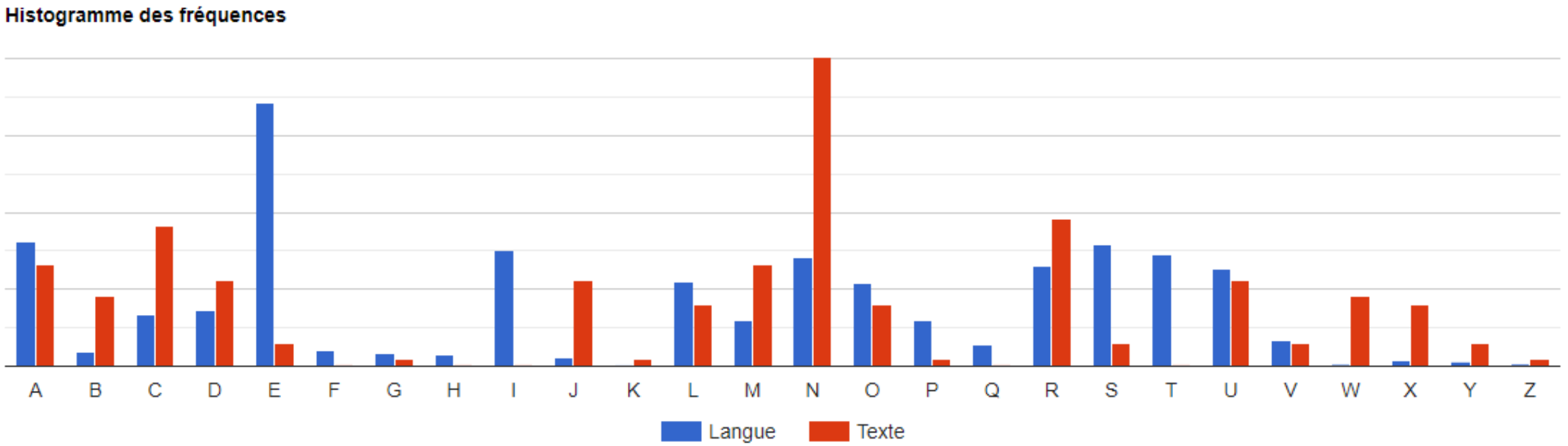
Les 9 couronnes (premier courriel, fin)

La population ne connaît pas encore l'existence de ce message, aussi je te demande la plus grande discrétion. Voici le message:

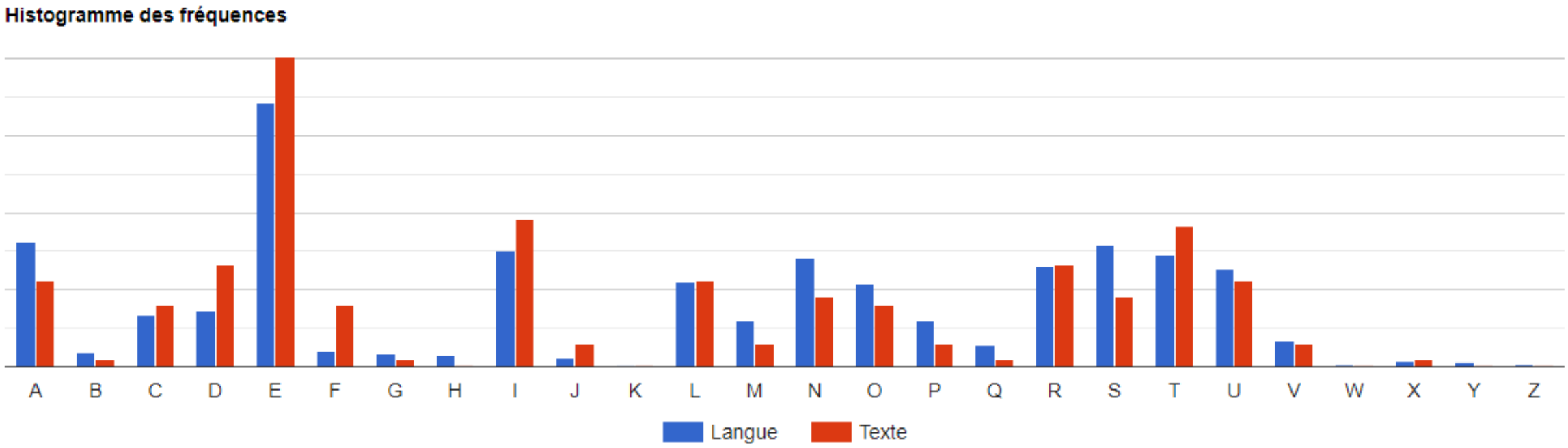
UNWER NMNCD NANBC MNENW DNCAX YOXAC NJDAJ RSNUN LXDAJ PNMNU NOJRA NLNUJ
WNMXR CYJBN CANMR OORLR UNMND GKJUU NBMJW BUNLX NDANC LNBCO RWRRU BDOOR
CMJCC NWMAN DWNER LCRVN WRVYX ACNZD RMNCR ANANC UNCXD ANBCS XDNLN BCMNL
RMNMN VJRWS NUNOJ RB

En espérant vivement ta collaboration.
Cordialement
--
Stéphane Périat, police scientifique jurassienne

Les 9 couronnes : statistiques



Les 9 couronnes : décalage de 9 crans



Les 9 couronnes (chapitre 1)

Chiffre de César

- *Niveau : facile*
- Analyse des fréquences
- Histogrammes
- Attaque par force brute (programmation)

Les 9 couronnes (chapitre 2)

Substitution simple

- *Niveau : moyen-difficile*

- Analyse des fréquences
- Histogrammes
- Attaque par mot probable

- Programmation

Les 9 couronnes (chapitre 3)

Grille tournante

- *Niveau : moyen*

- Comment construire un cache (où mettre les trous) ?
- Combien de caches *nxn* différents existe-t-il ?
- Le cache doit-il être carré ? D'autres formes sont-elles possibles ?

- Dans *Mathias Sandorf*, on avait le cache pour déchiffrer. Comment décrypter un message si on n'a pas le cache ?

Les 9 couronnes (chapitre 4)

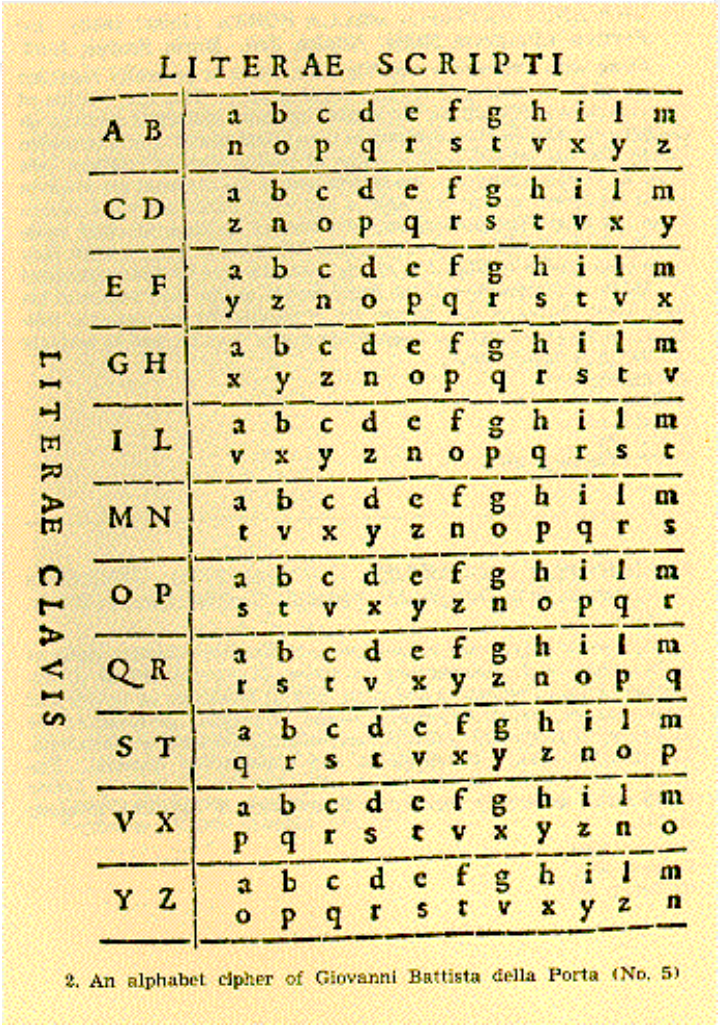
Chiffre de Porta

- *Niveau : moyen*

- Un des premiers chiffres polyalphabétiques
- Chiffre réversible

- Attaque par mot probable

- Recherche de motifs


LITERAE SCRIPTI

LITERAE CLAVIS	a	b	c	d	e	f	g	h	i	l	m
A B	n	o	p	q	r	s	t	v	x	y	z
C D	z	n	o	p	q	r	s	t	v	x	y
E F	y	z	n	o	p	q	r	s	t	v	x
G H	x	y	z	n	o	p	q	r	s	t	v
I L	v	x	y	z	n	o	p	q	r	s	t
M N	t	v	x	y	z	n	o	p	q	r	s
O P	s	t	v	x	y	z	n	o	p	q	r
Q R	r	s	t	v	x	y	z	n	o	p	q
S T	q	r	s	t	v	x	y	z	n	o	p
V X	p	q	r	s	t	v	x	y	z	n	o
Y Z	o	p	q	r	s	t	v	x	y	z	n

2. An alphabet cipher of Giovanni Battista della Porta (No. 5)

Les 9 couronnes (chapitre 5)

Chiffre du livre

- *Niveau : impossible* si on n'a pas le livre...

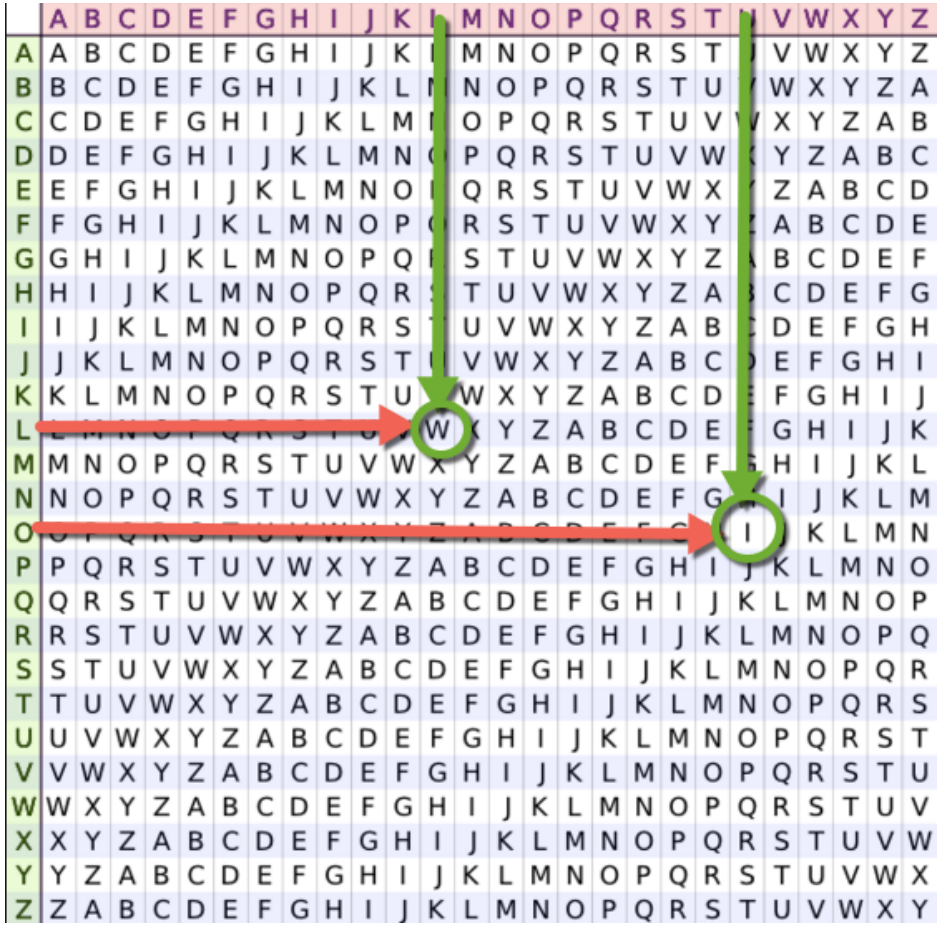
- Chiffre homophonique

Les 9 couronnes (chapitre 6)

Chiffre de Vigenère

- *Niveau : moyen*

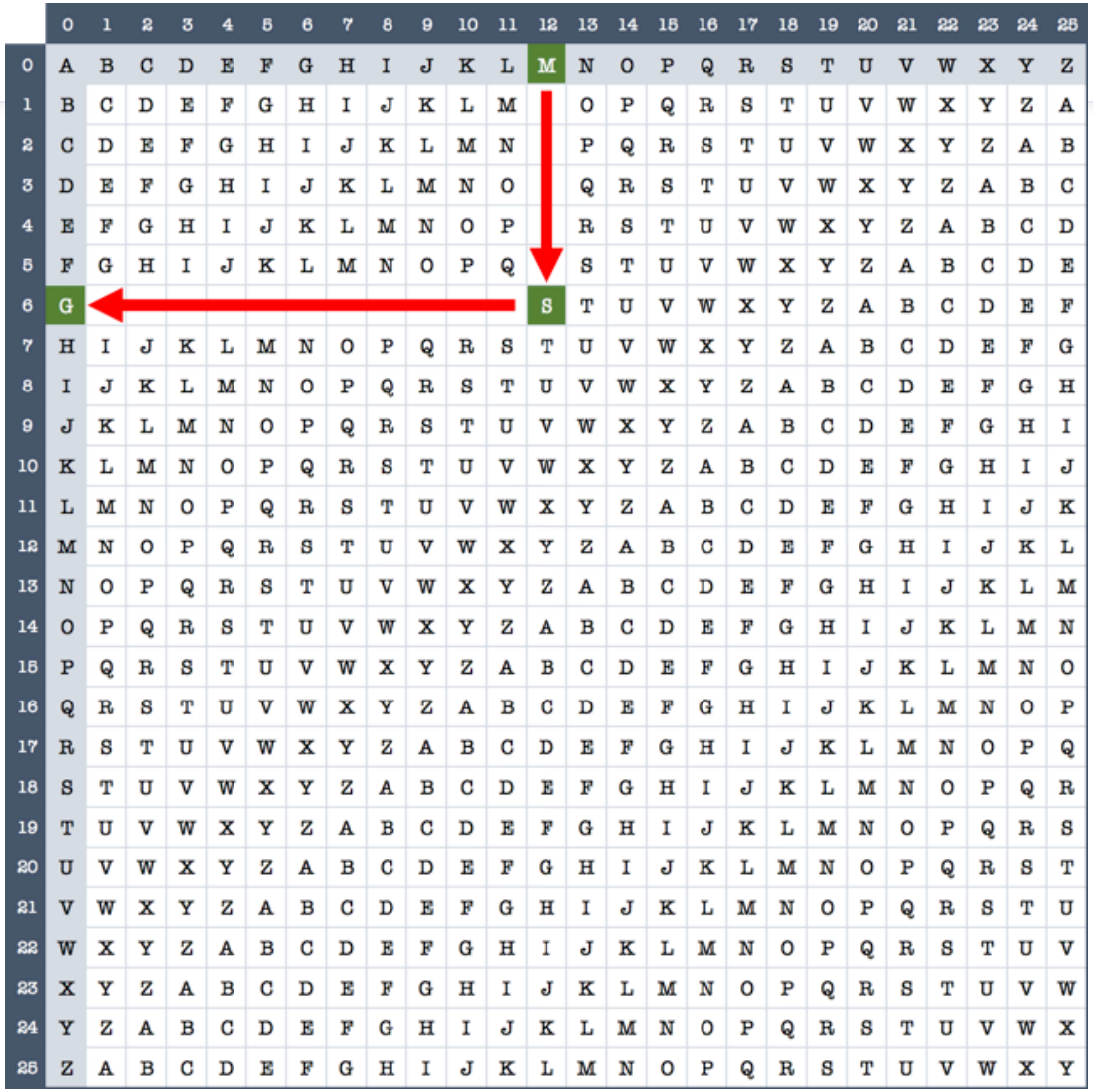
- Chiffre polyalphabétique le plus connu
- Différentes techniques de décryptement :
  - Kasiski / Babbage
  - Friedman
  - visuelle (histogrammes)
  - Bazeries



Les 9 couronnes (chapitre 7)

Chiffre de Beaufort

- *Niveau : moyen*
- Chiffre polyalphabétique (réversible)
- Utilise le tableau de Vigenère d'une autre façon



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M		O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N		P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O		Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P		R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q		S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G												S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	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
23	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	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Les 9 couronnes (chapitre 8)

Chiffre de Playfair

- *Niveau : difficile*
- Chiffre polygrammique
- **Fun fact :** Lord Playfair a popularisé l'utilisation de ce chiffrement imaginé par Charles Wheatstone.

BR -> MS (2)

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

EA -> TO (3)

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

KI -> FE (3)

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

NG -> GO (1)

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

Les 9 couronnes (chapitre 9)

Chiffre ADFGVX

- *Niveau : très difficile* (mais possible...)

- Utilisé par les Allemands pendant la Première Guerre mondiale.
- Surchiffrement
- Substitution suivie d'une transposition

	A	D	F	G	V	X
A	1	4	7	R	E	G
D	I	M	N	T	A	B
F	C	D	F	H	J	K
G	L	O	P	Q	S	U
V	V	W	X	Y	Z	0
X	2	3	5	6	8	9

P	R	I	V	A	C	Y
4	**5**	**3**	**6**	**1**	**2**	**7**
D	V	D	G	D	G	D
V	F	A	F	X	D	V
D	G	A	A	X	A	V
X	V	X	D	V	D	D

Attack at 1200 am
devient
DXXV GDAD DAAX DVDX VFGV GFAD DVVD

Pour en savoir plus

Ars cryptographica

www.apprendre-en-ligne.net/crypto

Questions ?


QUESTIONS IN ACADEMIC CONFERENCES
A PIE CHART
ATTEMPTS TO LOOK CLEVER
ALREADY ANSWERED ON THE SLIDES
UNCONNECTED RANDOM THOUGHTS
INTERESTING AND ADD TO THE CONFERENCE
ODDLY PERSONAL ATTACKS ON THE SPEAKER
@ERRANTSCIENCE