ITER_02_06

Chapitre 6 : la mystérieuse devise du cadran de Jumièges

Bien des gnomonistes se sont réjouis en lisant le N°4 de la « Lettre Régionale de la Fondation du Patrimoine en Haute-Normandie », de Juillet, Août, Septembre 2005 : enfin, le remarquable cadran de Port-Jumièges, sur la commune d'Heurteauville, venait d'être restauré.

On peut le découvrir facilement, sur la RD 65, sur le mur-pignon de la maison d'habitation actuellement numérotée 135, proche du pont de Port-Jumièges et du four à chaux qui dépendait des jardins de culture d'Heurteauville-Port-Jumièges, propriété de la célèbre abbaye. Ce four à chaux qui avait fonctionné de 1833 à 1873, a également été restauré en 2005. A la fin du XIXème siècle la maison était habitée par Henri-Michel Saint-Denis, (1841-1926), historien, journaliste, directeur et imprimeur du journal « L'Elbeuvien » (1881-1925).

Le cadran est estimable à plus d'un titre. D'abord, ses dimensions de 2 mètres de largeur par 3 mètres de hauteur en font ce qu'on peut nommer « une belle pièce ». Ensuite, la présence des tracés constructifs, très ostensiblement marqués et conservés sur le cadran terminé, y jouent le rôle de démonstration géométrique. Enfin, son large bandeau supérieur offre à la sagacité du passant, une devise non encore élucidée et que les lignes suivantes tenteront de présenter, sans, hélas, apporter la solution. Il faut cependant noter ici que la restauration récente a rendue encore plus difficile la lecture de la devise, complétée, à côté du cadran, par l'inscription : « Après l'heure finie, l'infini … ».

La première image du cadran, que possède la Société Astronomique de France est une photo en noir et blanc de Monsieur Bernard Clouet, datée de 1957. Il était temps ! Une photo immédiatement postérieure, de 1976, ne permet déjà plus de déchiffrer la devise qui nous préoccupe.

Photo de 1957

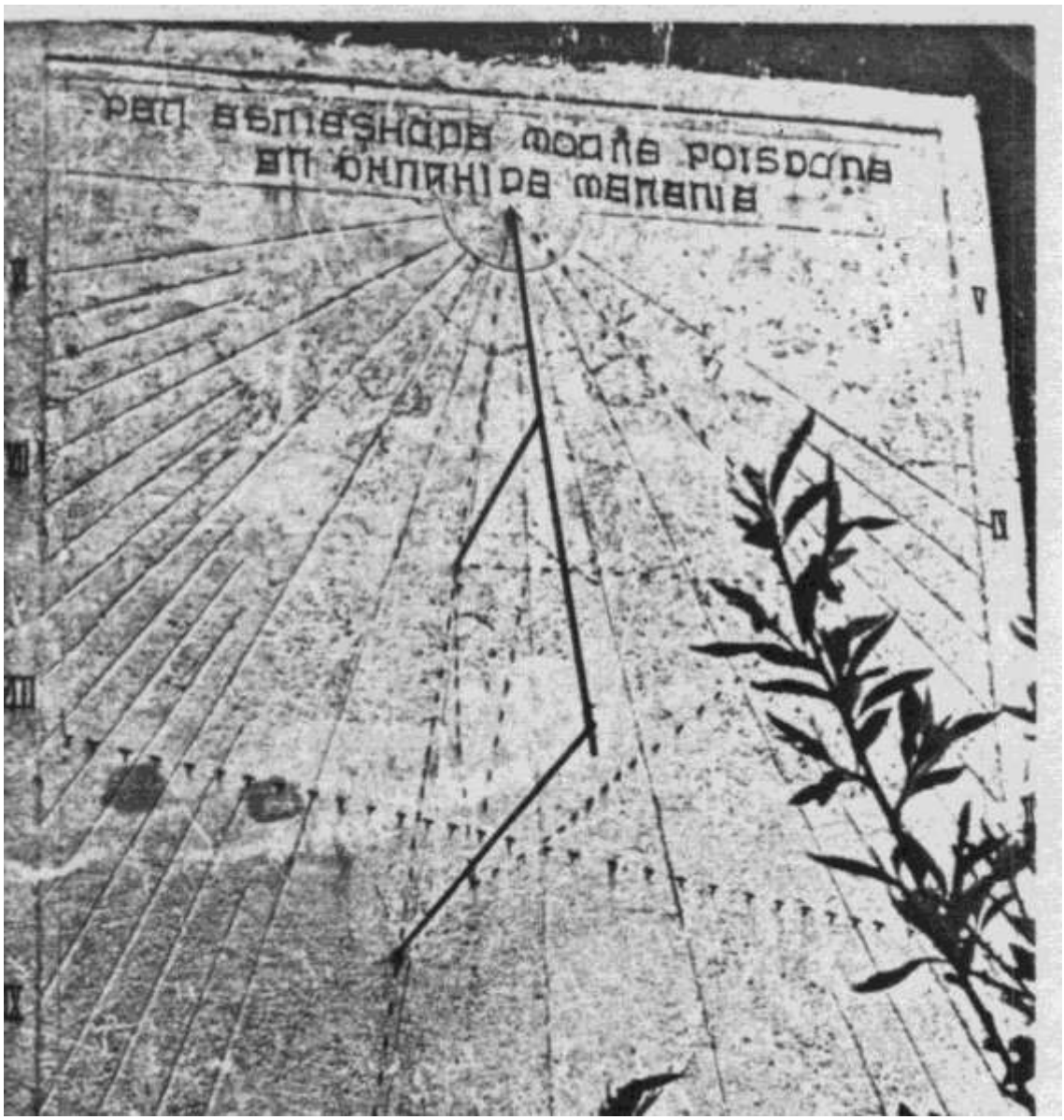

Photo de 1976

Le cadran en septembre 2008. La devise d'origine est désormais illisible. Mais une nouvelle a été placardée sur le mur: "Après l'heure finie, l'infini..."

Photo: Marc Ribès.

http://jumieges.free/jumieges.htm

Photo de 1957 avec les tracés constructifs renforcés en blanc

Bien que l'objet de cette note ne soit pas d'étudier le modus operandi du cadranier, il nous a semblé intéressant de mettre en évidence, sans commentaires, les manœuvres géométriques qu'il a accomplies sur le cadran lui-même et dont il n'a pas effacé les traces.

Agrandissement de la devise

1°) postulat de travail

Pour avoir le droit de parler de cette « devise » nous devons admettre que ces 7 groupes de signes représentent des mots d'une langue intelligible et que chacun de ces 43 signes représente une lettre, avec cette remarque, sur laquelle nous aurons à revenir, que cette lettre est toujours la même pour un signe donné ou bien qu'elle peut être différente à chaque occurrence du signe. Les espaces peuvent aussi être significatifs ou modifier la longueur apparente des mots. Si, au contraire, on pense que ces 7 groupes de signes ne sont pas des constructions linguistiques, mais seulement des images provenant d'un dictionnaire composé ad hoc et arbitrairement, par le crypteur, pour le déchiffreur et pour leur correspondance particulière, on ne peut aucunement tenter de briser ce code.

2°) alphabet

Nous n'avons pas trouvé d'alphabet composé rigoureusement avec ces signes ; notre source pour examiner les alphabets les plus vraisemblables a été le site internet http://pedroly.free.fr/alphabets

Plus récemment, nous avons regardé les alphabets de missionnaires, souvent désespérants parce qu'ils comportent un nombre élevé de signes, les uns pour les lettres et d'autres pour les syllabes.

A partir de cette constatation deux hypothèses apparaissent :

21°) il s'agit des caractères de l'alphabet français ou latin au milieu du XIXème siècle, mais tracés avec une certaine fantaisie. Alors, on pourrait lire ceci :

« PEN ESNIESHAPE MOANE POISDANE EN DHNRHIDE MENENIE »

Dans ce cas nous sommes, probablement, en présence d'un chiffre de substitution polyalphabétique avec clé, qui utilise un nouveau caractère à chaque occurrence d'une même lettre du texte clair. Un chiffre monoalphabétique serait peu sûr.

22°) les signes de la devise sont purement conventionnels à l'intérieur d'un groupe peu nombreux d'utilisateurs ; à la rigueur, seulement deux personnes.

Nous répugnons à imaginer une seule personne, car écrire une phrase si longue, en si gros caractères d'un alphabet inconnu, implique bien que quelqu'un la lira, ou que quelques uns la liront, même si c'est un langage d'initiés. Le chiffre employé pourrait alors n'être qu'un chiffre de substitution monoalphabétique qui utilise le même signe à chaque occurrence d'une même lettre du texte clair et, donc, laisse les lettres à leur place. Voir ce que nous dirons plus loin à propos des substitutions monoalphabétiques et polyalphabétiques.

3°) langue

Elle nous est inconnue. Si l'on admet que le cadran date du milieu du XIXème siècle on va penser au français ou au latin. Des patois normands, plus ou moins influencés par la langue des Vikings, sont moins probables car les patois sont plus parlés qu'écrits. Mais, près d'une abbaye, le grec et l'hébreu restent envisageables. Notons que l'alphabet français compte 26 lettres, l'alphabet latin 23 ou 25 selon qu'on différencie ou non le « i » d'avec le « j » et le « v » d'avec le « u » ; l'alphabet grec compte 24 lettres.

4°) examen superficiel et premières remarques

Si l'on écarte l'hypothèse de lettres connues mais tracées avec fantaisie, pour privilégier celle de signes inconnus, on remarque ceci :

41°) les signes semblent un mélange de lettres gothiques, d'onciales, de runes, de lettres grecques et de caractères inconnus (est-ce un indice pour mettre sur la voie d'une stéganographie ?)

42°) les mots sont plutôt longs : un de 10 signes ; deux de 8 signes ; un de 7 signes. En français les mots de 10 lettres représentent 3% du vocabulaire (estimé à 150000 mots). Ceux de 8 lettres représentent 6%.

43°) tous les mots, sauf les deux petits (3 signes et 2 signes) se terminent par le même signe qui ressemble à un E majuscule gothique. Si l'on a affaire à une langue qui se décline on pourrait penser à une construction avec une préposition qui introduit, puis un ensemble de trois mots interdépendants, puis une seconde préposition qui compare, puis un groupe de deux mots interdépendants ; un peu comme AD AUGUSTA PER ANGUSTA.

44°) la devise ne peut pas se lire par transparence. Lue dans un miroir, ou renversée, ou par la droite, elle reste toujours aussi mystérieuse.

Il faut maintenant dire deux mots des techniques cryptographiques, en considérant que le cadran date approximativement du milieu du XIXème siècle :

1°) on appelle chiffre de substitution monoalphabétique un chiffre de substitution où l'alphabet chiffré reste le même au cours de tout le chiffrement. Une même lettre du texte clair est toujours représentée par un même signe.

2°) on appelle chiffre de substitution polyalphabétique un chiffre de substitution où l'alphabet chiffré change au cours du chiffrement, selon une clé connue du scripteur et du lecteur. Une même lettre du texte clair est représentée par un

signe qui change à chaque occurrence de la lettre claire. Exemple bien connu : le carré de Vigenère.

Si la devise de Port-Jumièges a subi un chiffrement monoalphabétique, le même signe représentant toujours la même lettre claire, on peut espérer la décrypter, en attaquant le mot faible, c'est à dire le dernier mot qui comporte un groupe de trois signes identiques et un autre groupe de deux signes identiques pour seulement 7 caractères. S'il s'agit d'un chiffrement polyalphabétique, faute de trouver la clé qui engendre la séquence de permutation des alphabets, elle restera probablement à jamais inconnaissable, car une attaque en force brute exigerait du temps et des moyens informatiques qui ne sont pas à la portée de simples amateurs.

Il faut ici faire une remarque : nous trouvons 11 signes différents mais il se pourrait qu'un de ces signes, n'apparaissant qu'une seule fois, soit en réalité un signe déjà trouvé et qui aurait été dégradé par une aspérité de la pierre. Nous donnons cette hypothèse pour ce qu'elle vaut : il s'agit du signe occupant la quatrième place du sixième mot et qui, alors, serait identique au signe occupant la troisième place de ce même mot.

A partir de là, pour éviter d'avoir à reproduire ces signes qui n'existent pas dans les polices d'imprimerie des ordinateurs, nous pouvons les remplacer par les chiffres de 1 à 9 et 0, en donnant au premier signe le chiffre 1 et en augmentant d'une unité à chaque apparition d'un nouveau signe. Le signe discutable sera numéroté par un point d'interrogation et les lecteurs qui se lanceront dans l'aventure auront tout loisir de le conserver tel quel ou de l'assimiler à un autre.

Voici le résultat de cette conversion qui ne change absolument rien au problème:

'' 123 2435246782 90732 10548732 23 863?6582 9232352 ''

La fréquence d'apparition de ces chiffres, capitale pour déterminer la langue employée, dans le cas de substitution monoalphabétique, se mesure ainsi :

chiffre 1 = 2 fois
chiffre 2 = 11 fois
chiffre 3 = 8 fois ou 9 fois si on y ajoute le chiffre ?
chiffre 4 = 3 fois
chiffre 5 = 4 fois
chiffre 6 = 3 fois
chiffre 7 = 3 fois
chiffre 8 = 4 fois
chiffre 9 = 2 fois
chiffre 0 = 2 fois
chiffre ? = 1 fois

La présence dominante du chiffre 2 donnerait à penser qu'il représente le E du français, lettre suivie par SAINTURLO, mot mnémotechnique que connaissent

tous les cryptographes. En latin, plus probablement le A. Pour essayer de traduire le mot faible il faut mener l'attaque sur le dernier mot qui comporte trois fois le chiffre 2 et deux fois le chiffre 3. Ainsi, on pourrait obtenir en français, mais pour sourire, BANANIA et en latin LARARIA pluriel de LARARIUM qui est l'oratoire domestique où les Romains rendent un culte privé à leurs dieux lares. Mais ce ne sont là que des exemples de la méthode. Nous sommes loin de la vérité.

Si l'on songe à une attaque par force brute, avec alphabet connu et langue connue, par exemple le français avec 26 lettres, on s'aperçoit vite de l'immensité de la tâche. Il s'agit de composer avec les 2, 3, 4, … lettres supposées de la devise, ce que les statisticiens appellent un « arrangement ordonné avec répétitions », soit : 26^2, puis 26^3, etc. Déjà le mot de 7 lettres peut revêtir plus de 8 milliards de formulations, alors que le plus exhaustif des dictionnaires (*) ne connaît qu'environ 30 000 mots français, intelligibles, de cette longueur.

En résumé et par ordre de difficultés croissantes, nous aurions à explorer quatre hypothèses :

1°) alphabet français et substitution monoalphabétique
2°) alphabet français et substitution polyalphabétique
3°) alphabet inconnu et substitution monoalphabétique
4°) alphabet inconnu et substitution polyalphabétique

Ces dernières remarques sont quelque peu développées « ANNEXE-CRYPTO » placée dans « ALBUM_02_06 ».

(*) Il s'agit du Dictionnaire du Scrabble qui accueille parmi ses 300 000 mots, les verbes conjugués, les néologismes, les mots rares et disparus, le vocabulaire de spécialité des plus abstruses sciences et même les emprunts discutables à d'autres langues.

Message de Didier Muller, sur le site de Jumièges qui publie notre étude :

Didier Müller a écrit le *17/11/2010 à 23h02*

Bonjour
J'ai jeté un oeil sur cette page web. Je suis d'accord avec l'analyse qui en est faite. Je pencherais plutôt pour du latin (souvent les devises sur les cadrans solaires sont en latin). Quant aux symboles eux-mêmes, je n'en ai jamais vu de pareil.
Reste qu'il sera difficile de décrypter cette devise, étant donné la petite longueur du texte.
--
Cordialement
Didier Müller

Pages : [**1**]

Bibliographie sommaire :

Muller André : Les écritures secrètes ; PUF. Que sais-je ? N°116
Muller André : Le décryptement ; PUF. Que sais-je ? N° 2112
Singh Simon : Histoire des codes secrets ; Ed. J-C. Lattès 1999

et chacun de ces ouvrages présente une abondante bibliographie ainsi que des liens vers des sites internet. Voir en particulier l'Ars cryptographica de Didier Muller (de Porrentruy) : http://apprendre-en-ligne.net/auteur

L'œuvre de Maurice Leblanc (Arsène Lupin) regorge de cryptogrammes et se déroule souvent à proximité de Jumièges : peut-être à voir, d'autant que ses relations amicales avec Henri-Michel Saint-Denis et avec Conan Doyle sont bien établies.

Annexe : Notes en vrac à propos de la cryptographie.

1°) analyse combinatoire et attaque en force brute.

Nous admettons que les caractères de la devise forment des mots correctement séparés et que, donc, les espaces n'interviennent pas dans le décryptage. Représentés en alphabet français ou latin, malgré des graphies bizarres, ces mots deviendraient :

PEN ESNIESHADE MOANE POISDANE EN DHNRHIDE MENENIE

Nous admettons aussi que chaque caractère du cryptogramme correspond à une lettre unique du texte clair. Le décryptage consiste à remplacer chaque lettre du cryptogramme par une autre lettre, de telle façon qu'apparaisse un texte clair, intelligible en français ou en latin, puisque pour l'instant nous nous bornons à cette hypothèse.

L'attaque en force brute consiste à essayer, pour chaque lettre du cryptogramme, toutes les 26 (ou 23 en latin) lettres de l'alphabet choisi. La manœuvre consiste à pratiquer ce que les statisticiens appellent un « arrangement ordonné et avec répétitions (ou remises) ». Il est évident que plus un mot comporte de caractères et plus le nombre de ses traductions en clair, sera important. Là réside l'immensité de la tâche. Dans les ouvrages de mathématiques, au chapitre « Statistiques et probabilités », on trouve souvent la formule adéquate pour cette manœuvre d'arrangement, sous l'appellation de « Théorème 4 », soit : « le nombre a(n, k) des arrangements avec répétitions de 'n' éléments pris 'k' à 'k', est a(n, k) = n^k. »

Il s'agit d'analyse combinatoire vue comme une sorte de préface au calcul des probabilités ; outre les arrangements, elle traite des dénombrements, des permutations et des combinaisons. Ici nous devons réussir un arrangement ordonné d'un certain nombre d'éléments pris parmi un ensemble, avec cette obligation qu'un même élément peut être choisi plusieurs fois (répétition de lettres). Donnons un exemple : un mot de 2 lettres aura en français 26^2 = 676 arrangements et, en latin, seulement 23^2 = 529. Le tableau ci-après montre la vastité du problème de l'attaque en force brute, car on peut conserver en esprit qu'un siècle ne compte qu' environ 3 155 760 000 secondes et que si un ordinateur d'amateur présente dix propositions de décryptage par seconde, il lui faudra 470 ans pour épuiser toutes les configurations, en français, du mot de 10 lettres. Mais déjà, dans les années 80, dans les grands pays, des organismes d'Etat équipés d'engins à multi-processeurs, étaient capables de tester un arrangement avec répétition, toutes les microsecondes, donc 100 000 fois plus vite que dans notre précédent calcul. Il eût alors suffi de patienter non plus 470 ans, mais pas même deux jours et les mots intelligibles en latin ou en français

auraient seuls fait surface. Mais quel gnomoniste possèderait l'outil informatique de la CIA ?

Pour notre propos immédiat et à notre niveau, il vaudrait mieux que la devise fût en latin et combien il serait fâcheux qu'elle eût été cryptée avec l'un de ces alphabets de missionnaires qui comportent une trentaine de signes, les uns représentant des lettres et les autres des syllabes !

Longueur mots Nb de lettres	Français 26 lettres Nb arrangements	Latin 23 lettres Nb arrangements	Dictionnaire du Scrabble français
2 lettres	676	529	75
3	17 576	12 167	571
4	456 976	279 841	2 364
5	11 881 376	6 436 343	7 277
6	308 915 776	148 035 889	16 622
7	8 031 810 176	3 404 825 447	29 996
8	2.088 E + 11	7.8311 E + 10	44 664
9	5.4295 E + 12	1.4295 E + 12	55 309
10	1.4116 E + 14	4.4116 E + 13	58 149

Pour être complet nous signalons que le Dictionnaire du scrabble, en français, trouve encore des mots de
11 lettres = 53 026
12 lettres = 42 227
13 lettres = 29 666
14 lettres = 18 550
15 lettres = 10 589
et, pour finir, un mot de 29 lettres : hexakosioihexekontahexaphobie qui n'est autre que la peur du nombre 666. Elémentaire !

On voit que l'attaque par force brute exige des moyens immensément surdimensionnés par rapport aux 300 000 mots possibles en français ; et, encore, ce nombre est-il lui-même très exagéré, puisqu'on dit qu'un Français cultivé en connaît environ 50 000 et que Victor Hugo en connaissait 150 000. L'attaque par force brute va déployer des milliards d'arrangements pour découvrir sept mots. Elle n'est pas à la portée de l'amateur.

Quant à l'attaque de l'ensemble des 43 signes elle signifie 43^26 arrangements soit 3 E+42 propositions.

2°) le carré de Vigenère

C'est une méthode de cryptage qui nous semble pouvoir convenir à la période probable de la création du cadran : la seconde moitié du XIXème siècle. Le principe est simple : une phrase choisie par le crypteur et connue du lecteur, indique, pour chaque lettre à transposer, le décalage des alphabets successifs à

employer. Il n'y a aucune difficulté à télécharger légalement et gratuitement un logiciel qui applique à un texte codé, une phrase-code à introduire. Compte tenu du contexte normand et lupinesque, nous avons fait des tentatives avec les phrases-codes suivantes ; sans succès. (*) A la différence de l'attaque en force brute, ici le résultat est immédiat et n'exige que très peu de moyens.

Et in Arcadia ego
I tego arcana Dei
In robore fortuna
Fête du loup vert
Boucles de la Seine
Jumièges
Abbaye de Jumièges
Ad lapidem currebat olim regina
Agnès Sorel
Saint Wandrille
Port Lupin
Clos Lupin
Comtesse de Cagliostro
Saint Philibert
Enervés de Jumièges
Nunquam in eodem flumine natator
Devine si tu peux et choisis si tu l'oses
C'est facile
Applique toi
Consiste viator horam aspice et abi.
Veni vidi vici
Ad augusta per angusta

… / …

(*) Nous avons même lu l'ouvrage :
Patrick Ferté
Arsène Lupin, supérieur inconnu
Ed. Trédaniel ; 1992 / 2004

Les théorèmes de base :

Théorème 1 : permutations sans répétitions

Le nombre P(n) des permutations, sans répétition, de n éléments est :

P(n) = n !

Théorème 2: permutations avec répétitions

Le nombre P(n1, n2, …) des permutations de n éléments, avec permutations n1, n2, … est :

P(n1, n2, …, n k) = n ! / (n1 ! . n2 ! …, n k !)

Théorème 3 : arrangements sans répétition

Le nombre A (n, k) d'arrangements, sans répétition, de n éléments, pris k à k, est :

A(n, k) = n ! / (n-k) !

Théorème 4 : arrangements avec répétitions

Le nombre A*(n, k) des arrangements, avec répétitions, de n éléments pris k à k est :

A*(n, k) = n^k

Théorème 5 : combinaisons sans répétition

Le nombre C(n, k) des combinaisons, sans répétition, de n éléments pris k à k est :

C(n, k) = n ! / k ! . (n-k) !

Théorème 6 : combinaisons avec répétitions

Le nombre C*(n, k) des combinaisons, avec répétitions, de n éléments pris k à k est :

C*(n, k) =C[(n+k-1), k]

Exemple : lancers indépendants de 5 dés identiques : n = 6 ; k = 5

C*(n, k) = C(10,5) = (10.9.8.7.6 / 1.2.3.4.5) = 30 240 / 120 = 252

Remarque : C* comme A*, plus haut, indique la multiplication.
