Zodiac : les messages chiffrés d'un tueur en série

Hervé Lehning et Fayçal Ziraoui

Écrivain et journaliste scientifique
Polytechnicien et entrepreneur

Au tournant des années 1960–1970, un tueur en série qui se fait appeler Zodiac sévit en Californie. Son originalité est d'avoir communiqué avec la police à travers dix-sept lettres, dont quatre chiffrées. Le premier cryptogramme a été décrypté dès 1969, le deuxième vient de l'être, fin 2020. Ils résument relativement bien les méthodes classiques de cryptographie. Les deux derniers sont trop courts pour proposer des décryptements certains, mais des coïncidences troublantes militent pour la validité des décryptements qui sont proposés dans cet article.

Les quatre cryptogrammes du Zodiac sont désignés Z408, Z340, Z32 et Z13, en fonction de leurs longueurs. *A priori*, le plus long doit être le plus facile à décrypter… et ça a bien été le cas. Il a été envoyé en trois morceaux de huit lignes et dix-sept colonnes.

Premier tiers de Z408, le premier message chiffré.

Source : San Francisco Chronicle*, 31 juillet 1969*

La première idée qui vient à l'esprit d'un cryptologue est que le message a été chiffré au moyen d'une *substitution alphabétique*, chaque lettre ayant été remplacée par un ou plusieurs symboles. Plusieurs ici puisque le nombre de symboles utilisés excède largement 26. Ce type de substitutions, dites *homophoniques*, était encore courant à la Renaissance (Marie Stuart perdit la tête d'avoir eu confiance en un chiffre de cet acabit). Son seul avantage est de résister à la *méthode des fréquences*, qui permet au moins de trouver le symbole représentant « e », la lettre la plus fréquente en anglais comme en français. L'histoire nous enseigne la façon de décrypter un tel chiffre : la *méthode du mot probable*, inventée par Giambattista della Porta (vers 1535 ; 1615). Elle consiste à chercher des mots dont la présence est probable dans le texte. C'est ce que firent les décrypteurs de Z408, un enseignant et son épouse, Donald et Betty Harden. Leur idée fut de rentrer dans la psychologie d'un tueur en série qui, selon eux, a un égo surdéveloppé. Ainsi, le message devait commencer par la lettre « I » (« je », en anglais). Ensuite, ils ont cherché

« kill » et « killing » (verbe « tuer »). Le code s'écroula ainsi petit à petit, comme toujours avec ce type de chiffre. Voici le message décrypté :

I LIKE KILLING PEOPLE BECAUSE IT IS SO MUCH FUN IT IS MORE FUN THAN KILLING WILD GAME IN THE FORREST BECAUSE MAN IS THE MOST DANGEROUS ANAMAL OF ALL TO KILL SOMETHING GIVES ME THE MOST THRILLING EXPERENCE IT IS EVEN BETTER THAN GETTING YOUR ROCKS OFF WITH A GIRL THE BEST PART OF IT IS THAT WHEN I DIE I WILL BE REBORN IN PARADICE AND ALL THE I HAVE KILLED WILL BECOME MY SLAVES I WILL NOT GIVE YOU MY NAME BECAUSE YOU WILL TRY TO SLOI DOWN OR STOP MY COLLECTING OF SLAVES FOR MY AFTERLIFE EBEORIETEMETHHPITI

Les nombreuses fautes d'orthographe étaient vraisemblablement volontaires : un tel texte est en effet plus difficile à décrypter ! On peut traduire ainsi :

« J'aime tuer les gens parce que c'est du plaisir, plus que de tuer du gibier dans la forêt, parce que l'homme est l'animal le plus dangereux de tous à tuer. C'est excitant, même plus que d'avoir du bon temps avec une fille. Le mieux sera quand je mourrai. Je renaîtrai au paradis et tous ceux que j'ai tués deviendront mes esclaves. Je ne donnerai pas mon nom car vous essayeriez de ralentir ou de stopper ma récolte d'esclaves pour mon au-delà. Ebeorietemethhpiti. »

Malheureusement, malgré ce qu'il avait annoncé à la police dans une lettre non chiffrée, sa signature était incompréhensible. Il annonçait d'ailleurs lui-même pourquoi il ne donnait pas son nom. Une raison délirante dont on peut douter qu'il y croyait.

Ce décryptement rapide a pu vexer le Zodiac, qui a voulu montrer ses capacités en envoyant un message plus difficile à décrypter, le Z340. De fait, il fallut cinquante et un ans et trois personnes pour cela : David Oranchak, un développeur informatique américain, Sam Blake, un mathématicien australien, et Jarl van Eykcke, un passionné belge de cryptographie .

Z340, avec le logo du Zodiac en signature.

Source : San Francisco Chronicle, *8 novembre 1969*

Les symboles utilisés sont de même nature que ceux du Z408, donc une partie du chiffrement est probablement une substitution homophonique. Un autre chiffrement y avait été ajouté, sinon Z340 aurait été décrypté depuis longtemps. L'histoire de la cryptographie nous suggère qu'il s'agit d'une transposition, soit une anagramme du message… ce qui ne signifie pas qu'elle soit facile à trouver. Cela nous renvoie à la Première Guerre mondiale, au cours de laquelle les meilleurs chiffres conjuguaient substitution et transposition.

Comme l'équipe des décrypteurs disposait d'un excellent logiciel (AZdecrypt, créé en 2016 par Jarl van Eykcke) permettant de décrypter les chiffres de substitutions homophoniques tels que le Z408, il fut décidé de s'attaquer d'abord à la transposition qui, vu l'époque, avait dû être effectuée à la main et donc devait suivre une règle simple. Ils ont essayé six cent cinquante mille transpositions plus ou moins logiques ! L'échec était devenu une habitude quand soudain, après passage au crible de AZdecrypt, une transposition donna des passages clairs :

E HOPE YOU ARE … TRYING TO CATCH ME … THE GAS CHAMBER.

Ces deux derniers mots étaient particulièrement encourageants car correspondaient à une réalité vécue dans une émission de télévision d'octobre 1969, où un individu se faisant passer pour le Zodiac, intervenant par téléphone, affirmait avoir peur de la chambre à gaz.

La transposition essayée est naturelle pour un joueur d'échecs. Plus précisément, le trio a découvert (par chance selon lui) que, comme le Z408, le texte a été scindé en trois parties (deux fois 9 lignes puis 2 lignes) et la suite des lettres dans chaque partie décrit le déplacement d'un cavalier aux échecs (plus précisément, deux cases vers la droite et une vers le bas) en partant du haut à gauche. Quand le bord droit est atteint, le déplacement continue à la ligne suivante, à gauche (voir encadré).

Trois tableaux pour un message en trois parties

Le texte est constitué de trois cent quarante symboles. Numérotons-les de 0 à 339, ce qui donne une suite partant de 0 (la case en haut à gauche), puis 1 (obtenu de 0 par le déplacement du cavalier) et ainsi de suite, jusqu'à remplir toutes les cases. Le début de la suite est en rouge (de 0 à 10).

Premier tableau :

0	9	18	27	36	45	54	63	72	81	90	99	108	117	126	135	144
136	145	1	10	19	28	37	46	55	64	73	82	91	100	109	118	127
119	128	137	146	2	11	20	29	38	47	56	65	74	83	92	101	110
102	111	120	129	138	147	3	12	21	30	39	48	57	66	75	84	93
85	94	103	112	121	130	139	148	4	13	22	31	40	49	58	67	76
68	77	86	95	104	113	122	131	140	149	5	14	23	32	41	50	59
51	60	69	78	87	96	105	114	123	132	141	150	6	15	24	33	42
34	43	52	61	70	79	88	97	106	115	124	133	142	151	7	16	25
17	26	35	44	53	62	71	80	89	98	107	116	125	134	143	152	8

Deuxième tableau :																
153	162	171	180	189	198	207	216	225	234	243	252	261	270	279	288	297
289	298	154	163	172	181	190	199	208	217	226	235	244	253	262	271	280
272	281	290	299	155	164	173	182	191	200	209	218	227	236	245	254	263
255	264	273	282	291	300	156	165	174	183	192	201	210	219	228	237	246
238	247	256	265	274	283	292	301	157	166	175	184	193	202	211	220	229
221	230	239	248	257	266	275	284	293	302	158	167	176	185	194	203	212
204	213	222	231	240	249	258	267	276	285	294	303	159	168	177	186	195
187	196	205	214	223	232	241	250	259	268	277	286	295	304	160	169	178
170	179	188	197	206	215	224	233	242	251	260	269	278	287	296	305	161
Troisième tableau :																
306	332	324	316	308	334	326	318	310	336	328	320	312	338	330	322	314
323	315	307	333	325	317	309	335	327	319	311	337	329	321	313	339	331

En utilisant AZDecrypt et les éléments déjà établis, cette transposition mène au texte décrypté :

I HOPE YOU ARE HAVING LOTS OF FUN IN TRYING TO CATCH ME THAT WASNT ME ON THE TV SHOW WHICH BRINGS UP A POINT ABOUT ME I AM NOT AFRAID OF THE GAS CHAMBER BECAUSE IT WILL SEND ME TO PARADICE ALL THE SOONER BECAUSE I NOW HAVE ENOUGH SLAVES TO WORK FOR ME WHERE EVERYONE ELSE HAS NOTHING WHEN THEY REACH PARADICE SO THEY ARE AFRAID OF DEATH I AM NOT AFRAID BECAUSE I KNOW THAT MY NEW LIFE IS LIFE WILL BE AN EASY ONE IN PARADICE DEATH

Nous pouvons le traduire ainsi :

« J'espère que vous vous amusez bien en essayant de m'attraper. Ce n'était pas moi à la télévision, ce qui m'amène à dire quelque chose sur moi : je n'ai pas peur de la chambre à gaz car elle m'enverra plus tôt au paradis parce que j'ai maintenant assez d'esclaves pour travailler pour moi alors que tous les autres n'ont rien quand ils arrivent au paradis : c'est pour ça qu'ils ont peur de la mort. Je n'ai pas peur car je sais que ma nouvelle vie sera facile dans l'au-delà, au paradis. »

Dès lors que le code Z340 a été résolu, il a fourni une clé de substitution permettant d'associer les symboles utilisés par le Zodiac à des lettres de l'alphabet. Cela constituait un point d'entrée à la résolution par Fayçal Ziraoui des codes Z32 et Z13. En effet, ces cryptogrammes étant très courts, aucune méthode ne permettrait d'identifier une clé de substitution uniquement à partir de leurs symboles. Un grand nombre de clés permettraient en outre de donner des résultats crédibles, sans que la vérification de leur validité ne soit possible ! L'hypothèse de départ était donc que si les cryptogrammes Z32 et Z13 peuvent être résolus, alors ils utilisent la clé de substitution du Z340 (étant tous les trois l'œuvre du même auteur).

Le code Z32 était inclus dans une lettre dans laquelle le Zodiac menaçait de faire exploser une bombe au passage d'un bus scolaire. D'après lui, il renfermait la localisation de l'engin explosif. L'application de la clé de substitution du chiffre Z340 au Z32 permet de générer une séquence de lettres, sauf pour les symboles du Zodiac qui ne sont pas décodés :

YNSETAI(?)DOBP(?)AORT / RDFNOPTIYRGAIWN

Or le Zodiac a donné trois indices permettant de supposer que le Z32 renfermait des coordonnées, et donc des chiffres :

- Un cadran dessiné sur une carte accompagnant le Z32, positionné sur le Mont Diablo, qui fut longtemps un repère pour les géomètres du cadastre et par lequel est défini un méridien principal (Méridien Diablo) ;
- Une mention manuscrite à côté du cadran, « A régler sur le N. Mag. », que l'on peut interpréter comme « À régler sur le Nord magnétique » ;
- Un post-scriptum dans un courrier indiquant que l'indice du Mont Diablo faisait référence à des « radians et des inches », qui sont les noms des unités et des décimales de mesures d'angles.

Ces trois indices réunis permettent d'émettre l'hypothèse que le code Z32 renferme des coordonnées de latitude et de longitude (qui sont des mesures d'angles), par rapport au Nord magnétique (et non géographique, communément utilisé). On voit d'ailleurs des anagrammes de NORT, EAST, WEST. Une méthode triviale pour décrypter les lettres de l'alphabet obtenues précédemment en chiffres est de leur affecter leur position dans l'alphabet. Ou encore, de ne garder que les unités de leur position. Cette substitution élémentaire donne

5495019(?)4522(?)1580 / 846456095871934

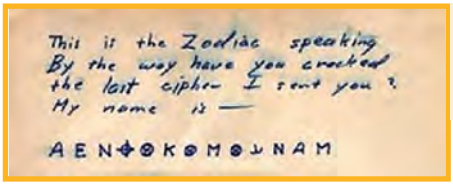
Une hypothèse pragmatique est que les coordonnées recherchées sont en Californie du Nord, zone où opère le tueur. On identifie donc une séquence de dix chiffres, parfaitement ordonnée, qui sont les coordonnées d'un lieu à proximité de South Lake Tahoe, à la frontière avec le Nevada :

YNSETAI(?)DOBP(?)AORT / RDF4560958719WN

soit 45.609 NORT(h) 58.719 WEST. Ce résultat est intéressant car on atterrit à 800 m d'une école, dans une ville qui est liée à l'affaire du Zodiac (il avait envoyé une carte postale faisant référence au lac Tahoe).

L'étape suivante est une analyse exhaustive de toutes les anagrammes possibles avec les lettres restantes. La recherche d'anagrammes n'ayant donné aucun résultat en première approche, l'hypothèse que le Zodiac a volontairement fait une erreur sur le symbole triangle (il échange le triangle plein et le triangle avec un point en son centre, ce qu'il a fait quatre fois sur huit dans le code Z408) a permis ensuite de reconstituer une seule séquence ayant une signification : LABOR DAY FIND 45.609 NORT(h) 58.719 WEST. Ce décryptage du Z32

est intéressant car le Labor Day marque la rentrée scolaire aux États-Unis, ce qui encore une fois est cohérent avec la menace du Zodiac de s'attaquer aux écoliers. Pour être totalement valide, l'hypothèse principale qui a permis de résoudre le cryptogramme Z32 doit permettre de résoudre aussi le code Z13. Dans le courrier reçu, Z13 était précédé de la mention « Mon nom est », le Zodiac laissant penser qu'il renfermait son identité.



Le cryptogramme Z13, précédé de « My name is » (« Mon nom est »).

Source : San Francisco Chronicle, *20 avril 1970*

En appliquant la même clé de substitution que le Z340, ainsi que la traduction de lettres en chiffres utilisée dans le code Z32, on obtient le résultat : 4851(?)1(?)5(?)(?)545. Les symboles du Zodiac, non décryptés par la clé Z340, peuvent être traduits également en chiffres de façon triviale en utilisant leur position dans le cadran du Zodiaque : le Cancer prend la valeur 4 et le Bélier 1. Ainsi déchiffré, le Z13 devient : 4851414541545 Cette séquence peu variée rappelle une technique de chiffrement inventée par le Français Félix-Marie Delastelle (1840–1902), qui utilise trois chiffres pour chiffrer tout l'alphabet (ici 1, 4 et 5) ; une analogie serait l'encodage binaire en électronique. En conséquence, les cryptogrammes utilisant cette technique ont une longueur qui est un multiple de 3. Or ici, la longueur est de treize caractères, qui n'est pas un multiple de 3, et malgré les répétitions de 1, 4 et 5, le caractère 8 semble de trop. En revanche, en considérant l'écart en valeur absolue entre les chiffres, on retrouve une séquence de douze caractères parfaitement déchiffrable par la méthode de Delastelle : 434.333.113.411. La méthode permet d'envisager six résultats possibles : UAMW, XNBS, DNZI, G_OE, Q_CJ, KAYR. Ce dernier est intéressant, car il fait penser à Lawrence Kaye, l'un des principaux suspects. Connu pour utiliser régulièrement le pseudo Lawrence Kane, il utilise également Larry KAY. Il se trouve que ce suspect habitait au lac Tahoe, à 6 km de l'école visée par le code Z32 ! Il fut également soupçonné d'avoir enlevé et assassiné une infirmière de South Lake Tahoe, Donna Lass.
La présence du « R » n'est pas surprenante : comme dans le code Z32, le Zodiac a pu vouloir tromper les autorités en glissant une erreur volontairement, et se protéger dans l'éventualité où son cryptogramme serait déchiffré.

Pour résoudre les codes Z32 et Z13, une approche purement cryptographique ne suffit pas du fait de leur faible longueur. Il faut émettre des hypothèses qui sont plausibles du point de vue de l'enquête criminelle. Saurons-nous un jour la vérité sur l'identité du Zodiac ?

H.L. & F.Z.