

Didier Müller

Les 9


couronnes

Petit cours de cryptographie classique
sous forme d'un roman policier

Préface de l'auteur

Une envie : écrire un « roman didactique » ou un « cours romancé », le livre que vous avez entre les mains.

Un but : présenter une histoire résumée de la cryptographie classique à travers neuf chiffres choisis entre l'Antiquité et le début du 20^e siècle. Ce livre est couplé avec le site web « Ars Cryptographica », à l'adresse www.apprendre-en-ligne.net/crypto/ .

Une histoire : un tueur en série laisse des cryptogrammes dans la bouche de ses victimes. Peut-être est-ce des indices qui permettront de l'arrêter ?

Vous pourrez utiliser ce livre de deux façons. Lisez-le de la première à la dernière page, et vous aurez un cours de cryptographie romancé. La deuxième manière est plus ludique : ne lisez que la première page de chaque chapitre, où est présenté le cryptogramme, puis essayez de le déchiffrer vous-même avant de lire la suite du chapitre.

Le dernier cryptogramme du tueur n'est pas décrypté dans le livre, et il reste un doute quant au dénouement de l'histoire. Si vous réussissez à résoudre le dernier cryptogramme, vous pourrez lire la fin du neuvième chapitre sur le site www.apprendre-en-ligne.net/crypto/9/, après avoir introduit un... mot de passe, évidemment.



Chapitre 1

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.

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 GKJUJ 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

L'atmosphère dans le cybercafé « Quo Vadis » était celle d'une fourmilière : des dizaines de doigts tapotaient les claviers avec frénésie. Maximilien Bendit et sa compagne Pénélope étaient à Saint-Pétersbourg depuis le début du mois et ils venaient d'en finir avec les problèmes administratifs. Cela n'avait pas été facile : heureusement que Pénélope parlait déjà la langue avant de venir ici, car on ne peut pas dire que les fonctionnaires russes soient polyglottes. Il avait fallu refaire le test du SIDA dans un hôpital vétuste (car le test fait en Suisse n'était pas valable ici), faire la queue debout pendant deux heures sans rien dans l'estomac, retourner le lendemain chercher les résultats, faire des photographies noir et blanc car les photos couleur ne convenaient pas, payer les cours à l'université, pour enfin obtenir le visa qui allait leur permettre de séjourner dix mois à Saint-

Pétersbourg.

C'était la seconde fois qu'ils se rendaient dans ce cybercafé, idéalement situé sur la célèbre perspective Nevski, presque en face de la cathédrale de Kazan. Il était essentiellement fréquenté par des étrangers qui voulaient rester en contact avec leur famille et savoir ce qui se passait dans le monde. La tragédie de Beslan, en Ossétie du Nord, où des terroristes avaient pris en otage mille deux cents personnes dans une école le 1^{er} septembre, jour de la rentrée des classes en Russie, et l'intervention de l'armée du 3 septembre « à la russe », ou plutôt « à la Pyrrhus », qui s'était soldée par la mort de trois cent trente personnes, dont plus de la moitié étaient des enfants, faisait encore la une des journaux. Mieux valait ne pas être pris en otage dans ce pays, se disait amèrement Maximilien, car ici la vie des otages n'avait pas plus de valeur que celle des kidnappeurs. Le seul but du gouvernement était de montrer que les Russes ne cédaient jamais au chantage, quel qu'en soit le prix.

Pénélope, assise devant un ordinateur voisin, lisait le message qu'une de ses copines lui avait envoyé du Canada. Au début de leur relation, elle détestait les ordinateurs, jusqu'à ce qu'elle découvre le courrier électronique et la possibilité d'acheter en ligne, avec la carte de crédit de Maximilien...

Lui aussi lisait son courrier électronique. Il avait commencé par les messages provenant de sa sœur, avant d'ouvrir le courriel de son cousin Stéphane. C'était la première fois qu'il le contactait depuis des années, aussi Maximilien était-il curieux d'en connaître la raison. La lecture de ce message le laissait songeur. Perdu dans ses pensées, il n'entendait pas que Pénélope lui parlait. Agacée, elle lui secoua énergiquement le bras.

« Dis ! Tu m'écoutes quand je te parle ?

- Hein ? Désolé ! J'ai reçu un mail qui me perturbe. Regarde...
- Qu'est-ce que c'est que cette histoire ? Peut-être une blague d'un de tes anciens élèves, non ?
- Non, cela vient de Stéphane, mon cousin qui a fait l'école de police scientifique à Lausanne. C'est très sérieux.
- Et alors ? Qu'est-ce que tu vas faire ?
- Tu connais ma passion pour la cryptographie. Je ne peux pas dire non. Je vais essayer de décrypter ce message dès notre retour à l'hôtel. »

```
De : Maximilien Bendit <crypto@apprendre-en-ligne.net>  
Date : Thu, 9 Sep 2004 18:52:33 +0400  
A : <Stephane.Periat@jura.ch>  
Objet : Re: besoin d'aide
```

```
Steph,  
Je me penche sur le cryptogramme tout de suite. Je t'envoie le  
resultat de mes tentatives (ou le non-resultat) des que possible.  
Cordialement  
P.S. Tu m'excuseras, mais, en Russie, les claviers n'ont pas  
d'accents ;-)  
--  
Maximilien Bendit  
http://www.apprendre-en-ligne.net/
```

Sur le site du « Quotidien Jurassien », il était évidemment question de ce meurtre crapuleux. Un tel événement ne pouvait pas passer inaperçu dans un canton où presque tout le monde se connaissait, surtout dans un village d'une septantaine d'habitants comme Seleute. Les journalistes auront (enfin) du grain à moudre...

Quand ils sortirent du « Quo Vadis », une brise glaciale leur fouetta le visage. Ils traversèrent la « Nevski Prospekt » et prirent la « Kazanskaya oulitsa » pour retourner à leur hôtel, qui se situait une centaine de mètres derrière ce Vatican miniature qu'est la cathédrale Notre-Dame de Kazan.

Ils n'avaient pas de ligne téléphonique dans leur chambre - la 448 -, ni télévision, ni radio. Elle était suffisamment grande pour y vivre dix mois sans souffrir de la promiscuité : environ huit mètres de long sur trois de large. Il y avait une armoire pour les habits, un petit réfrigérateur, un bureau, deux chaises, deux lits, deux tables de nuit. Les fenêtres occupaient tout un côté de la chambre et donnaient sur la cour intérieure. L'hôtel avait une centaine de chambres, principalement occupées par des étudiants étrangers ou des touristes russes.

La literie n'était pas de première qualité : les lits craquaient au moindre mouvement. Par contre, les femmes de chambre passaient l'aspirateur tous les trois jours, changeaient les draps chaque semaine et vidaient la poubelle quotidiennement. Dommage qu'elles ne prissent pas la poussière sur les meubles...

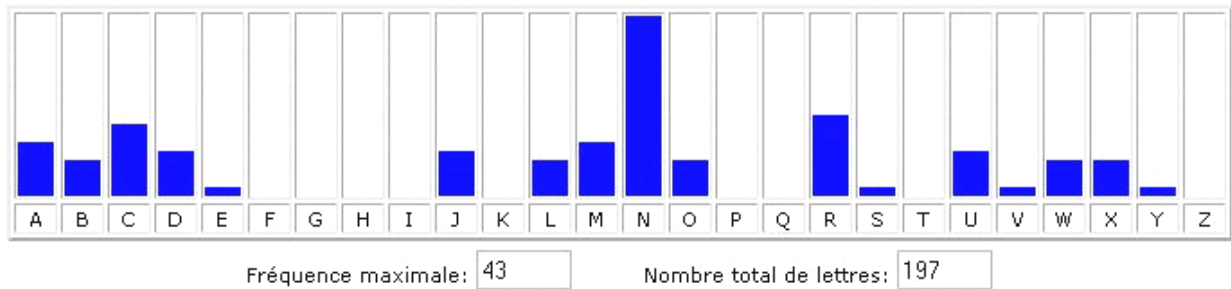
La salle de bain était commune avec la chambre voisine, et on devait acheter soi-même le papier-toilette. L'eau chaude arrivait de manière chaotique et était reconnaissable à sa couleur jaune.

Maximilien sortit son ordinateur portable d'un tiroir du bureau et se mit au travail. Il choisit dans sa bibliothèque multimédia sa chanteuse préférée : Tori Amos. Il ne maîtrisait pas assez l'anglais pour comprendre les paroles, d'autant plus qu'elles étaient très énigmatiques, mais qu'importe : cette voix envoûtante et infiniment triste ne cessait de le charmer. Il mit des écouteurs bon marché pour s'isoler, mais il entendait quand même Pénélope fredonner sur son lit. Elle avait une mémoire fabuleuse des paroles de chansons ; c'est pour cela qu'un des surnoms qu'il lui avait donnés était « le juke-box vivant ». Comme cela l'empêchait de se concentrer, il marmonnait dans sa barbiche. Ses paroles intriguèrent Pénélope qui jeta un coup d'œil par-dessus son épaule.

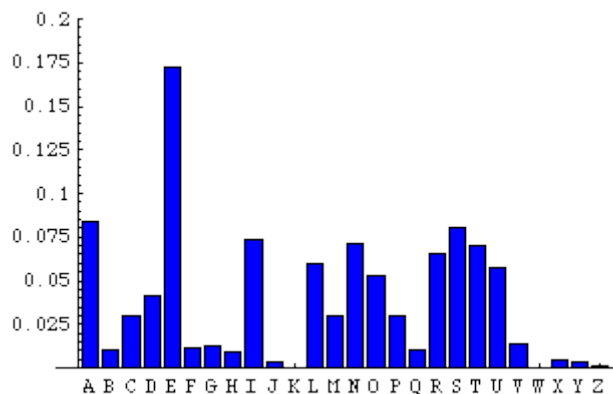
« Mais qu'est-ce que tu fais ? »

- La première chose à faire quand on veut décrypter un message secret : une analyse des fréquences.
- Une quoi ?
- Une analyse des fréquences des lettres. Une grande lectrice comme toi a déjà remarqué que certaines lettres apparaissent bien plus souvent que d'autres...
- Évidemment, en français, le E, le A, les voyelles en général apparaissent bien plus souvent que le Z ou le X.
- Exactement ! Et pour me la péter, je peux te dire que c'est le savant arabe Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah Oòmran ibn Ismaïl al-Kindi qui a eu le premier l'idée d'utiliser cette information pour décrypter des messages, et cela au 9^e siècle.
- Abu Yusuf quoi ? Dis, tu te fous de moi ? Toi qui n'es pas capable de retenir un mot russe de plus de trois syllabes !
- J'avais écrit son nom dans mon cours de cryptographie. Heureusement que j'ai une copie de mon site sur mon portable...
- Et cette histoire de fréquences est valable pour les autres langues ?
- Oui, enfin plus ou moins. Disons que la répartition des fréquences n'est pas la même, mais que dans toutes les langues il y a des lettres plus fréquentes que d'autres.
- Tu connais les fréquences pour le russe ?
- Là, tu me colles. Mais il y aurait un moyen amusant de s'en faire une idée : il faudrait acheter un jeu de Scrabble russe. En effet, dans ce jeu, il y a 100 jetons portant une lettre.
- Merci, je ne suis pas débile. Je sais ce que c'est que le Scrabble !
- Bon ! Eh bien tu as remarqué que plus une lettre est commune, plus le nombre de jetons portant cette lettre est grand. Et si la lettre est rare, il n'y a qu'un ou deux jetons portant cette lettre.
- Donc, si je te suis bien, il suffit de compter le nombre de jetons portant une lettre pour connaître approximativement sa fréquence.
- Oui. Si par exemple on compte 12 « A », on pourra dire que la fréquence du « A » est d'environ 12%, puisqu'il y a 100 jetons en tout.
- Tu es un petit malin, toi !
- Pour revenir à notre décryptement, je vais m'y prendre comme al-Kindi et compter les fréquences

des lettres du cryptogramme. J'ai écrit il y a quelques mois un petit programme qui va me faire ça très vite. Regarde !



- Attends ! Je pensais voir des chiffres ! Qu'est-ce que c'est que ces barres bleues ?
- C'est une représentation graphique du résultat. L'ensemble des barres forme ce que l'on appelle un histogramme. La hauteur de chaque barre est proportionnelle à la fréquence de la lettre correspondante. Par exemple, le N est la lettre la plus fréquente du cryptogramme avec 43 occurrences.
- Ok. Et alors ?
- Je vais comparer maintenant cet histogramme avec celui de la langue française.
- Et tu vas le trouver où, cet histogramme ?
- Toujours dans mon cours. Comme je ne trouvais pas d'histogramme récent, j'en ai calculé un moi-même en prenant différents textes français qui contenaient, une fois réunis, 100'000 lettres au total.
- Et tu as compté ça à la main ? Tu es encore plus fou que je ne le pensais !
- Mais non ! C'est l'ordinateur qui s'est chargé de cette basse besogne.
- Ah d'accord ! Et quel a été le résultat ?
- Attends que je le retrouve... Ah! le voici :



- Je ne comprends plus rien. Pourquoi y a-t-il des nombres à virgule sur l'axe vertical ?
- J'ai simplement divisé le nombre de lettres par 100'000 pour avoir un pourcentage. Tu remarques que la lettre la plus fréquente en français est le E.
- Quelle surprise... Je te l'avais dit tout à l'heure d'instinct !
- Certes. Mais cet histogramme te donne plus d'informations. On voit bien que, comme tu le disais si justement tout à l'heure, les voyelles, à part le Y, sont parmi les plus fréquentes. Parmi les consonnes, ce sont le R, S, T, N et L qui sont les plus fréquentes. On voit aussi deux « trous », un à l'endroit des lettres J et K, et l'autre sur W, X, Y et Z.
- Il n'y a guère de B et de Q également...
- En effet. Mais revenons à l'histogramme du cryptogramme. On voit que là aussi les lettres ne sont

pas uniformément réparties : certaines sont plus fréquentes que d'autres. Certaines sont même carrément inexistantes. Cela indique que l'assassin a probablement utilisé un système de chiffrement simple, où chaque lettre est remplacée par une autre, toujours la même. Que constates-tu d'autre ?

- Ben, il y a aussi des trous. Et comme par hasard un trou de 4 barres et un trou de 2 barres.
- Exact ! Tu es belle, je t'aime ! Allons plus loin et supposons que FGHI correspondent à WXYZ. Si on répète l'alphabet, J correspond à A, K à B, etc., et le deuxième trou PQ correspond au trou JK.
- Et tu en déduis ?
- J'en déduis que l'assassin a simplement décalé les lettres de l'alphabet de neuf rangs vers la gauche, puisque le E du texte clair correspond à un N dans le message chiffré. C'est un bête chiffre de César !
- Qu'est-ce que César vient faire là-dedans ?
- On a donné ce nom à ce système de chiffrement, car Suétone a écrit, dans son livre « La vie des douze Césars », que Jules César chiffrait ses messages en décalant les lettres de l'alphabet de trois rangs vers la gauche. L'empereur Auguste, qui succéda à César, ne décalait, lui, les lettres que d'un rang.
- Mais tu adores te la péter, ma parole !
- Oui, j'aime bien. Enfin bref, voyons ce que donne le message décrypté :

```
LENVI EDETU EREST DEVEN UETRO PFORT EAURA IJELE COURA GEDEL EFAIR
ECELA NEDOI TPASE TREDI FFICI LEDEU XBALL ESDAN SLECO EURET CESTF
INIIL SUFFI TDATT ENDRE UNEVI CTIME NIMPO RTEQU IDETI RERET LETOU
RESTJ OUECE STDEC IDEDE MAINJ ELEFA IS
```

- Ah bravo ! On ne comprend toujours rien !
- C'est parce que l'assassin a groupé les lettres par cinq, comme on le fait habituellement en cryptographie.
- Pourquoi cinq plutôt que six ou quatre ?
- Je ne sais pas vraiment. Peut-être parce que cinq est généralement la limite au-delà de laquelle on est obligé de compter les objets.
- Quoi ?
- Si je te montre cinq billes, tu me diras instantanément qu'il y en a cinq. Si j'en mets six, tu devras compter pour être sûre du nombre.
- Ah bon !?
- Maintenant regarde ce que cela donne si je remets les espaces aux bons endroits :

```
L'envie de tuer est devenue trop forte. Aurai-je le courage de le
faire? Cela ne doit pas être difficile. Deux balles dans le coeur et
c'est fini. Il suffit d'attendre une victime, n'importe qui, de tirer
et le tour est joué. C'est décidé, demain je le fais!
```

- Bravo, Maxou ! Tu es rapidement venu à bout de ce message codé ! Pas terrible le chiffre de César...
- En effet, et pourtant il a duré plus de mille ans. Il faut dire qu'en ces temps reculés, le simple fait d'écrire constituait déjà un système de chiffrement, puisque seuls les érudits savaient lire. C'est comme quand je vois des mots russes. Je n'arrive pas encore à les lire aisément parce que je ne suis pas habitué à l'alphabet cyrillique.
- Mille ans. Pourtant c'est très facile à déchiffrer. Tu n'as même pas besoin de faire d'analyse des fréquences. Il suffit d'essayer les vingt-cinq décalages possibles.
- Exact. C'est ce qu'on appelle une recherche exhaustive de la clef. Une telle attaque est possible avec des chiffres qui ont peu de clefs.

- Une clef ? Qu'est-ce que c'est ?
- Dans notre cas, la clef est 9 puisqu'on a décalé l'alphabet de neuf rangs. En général, c'est un nombre, un mot ou une phrase qui permet de [chiffrer](#) ou de [déchiffrer](#) un message, en utilisant un certain système de chiffrement.
- En tout cas, c'était facile.
- Tu as raison. Trop facile même, je trouve... On dirait que l'assassin voulait être sûr que quelqu'un allait décrypter son message. Et, malheureusement, cela ne va guère aider la police, puisque, apparemment, il s'agit d'un acte gratuit.
- Pourquoi s'amuse-t-il à mettre des messages dans la bouche des gens qu'il tue ? C'est conceptuel !
- Aucune idée, baby. Pour faire parler de lui peut-être. Cela me rappelle le tueur en série qui se faisait appeler « Zodiaque ». Il avait envoyé des messages chiffrés à la presse. Cela se passait près de San Francisco à la fin des années soixante, si je me rappelle bien... On a pu déchiffrer certains messages, mais on n'a jamais retrouvé l'assassin.
- Ah non ?
- Non. Les enquêteurs avaient alors avancé trois hypothèses : soit il était mort, soit il était en prison, soit il avait quitté la région. En effet, un tueur en série ne s'arrête pas de tuer comme ça...
- Tu penses que le gars de Seleute est un tueur en série ?
- Seul l'avenir le dira.
- Et puis, il y a aussi cette couronne de laurier... Qu'est-ce que cela peut vouloir dire ?
- Je ne sais pas. Peut-être un signe de dérision, la marque d'une vengeance, que sais-je ?
- Moi, je crois que j'ai trouvé ! Tu connais la bande dessinée d'Astérix intitulée « Les lauriers de César » ? Je pense que le meurtrier voulait nous donner une piste pour nous aider à déchiffrer le message.
- On n'avait pas vraiment besoin d'aide, mais c'est une possibilité... En tout cas, le message chiffré et la couronne montrent que le crime a été prémédité. On a affaire à quelqu'un d'organisé, qui, malgré ce que dit son message, planifie tout dans les moindres détails. Il lui a fallu écrire le message, le chiffrer, tresser une couronne de laurier. Tout cela prend du temps.
- J'ai une autre hypothèse : le meurtrier voulait vraiment tuer ce vieillard et il a mis le message et la couronne pour brouiller les pistes...
- Oui. Tout est possible. Je fonce au « Quo Vadis » pour envoyer un e-mail à Stéphane. Il est un peu tard, mais cet Internet Café est ouvert 24 heures sur 24. »

Ils ne dormirent pas beaucoup cette nuit-là, et pas seulement à cause des moustiques qui étaient encore voraces à cette période de l'année. Jusqu'aux lueurs du jour, ils échafaudèrent des dizaines d'hypothèses, toutes aussi farfelues les unes que les autres.

Le lendemain après-midi, Maximilien retourna au « Quo Vadis ».

```
De : Stéphane Périat <Stephane.Periat@jura.ch>
Date : Fri, 10 Sep 2004 9:12:48 +0200
A : <crypto@apprendre-en-ligne.net>
Objet : Re : decryptement
```

```
Max,
Merci pour ton aide précieuse et tes intéressantes hypothèses.
Je me permettrai de te solliciter à nouveau en cas de besoin.
Cordialement
--
Stéphane Périat, police scientifique jurassienne
```

C'était un message typique de leur famille : épuré.

Pas loin de l'Internet Café se trouvait le magasin DLT (Dom Leningradskoï Targovli) où il y avait un grand choix de jeux et de jouets. Il acheta un Scrabble russe, histoire d'occuper les soirées et, de retour à l'hôtel, il put satisfaire sa curiosité sur les fréquences des lettres en russe.

- «Tu vois Pénélope, dans le Scrabble russe, il y a 102 lettres et deux jetons blancs - qui ne nous intéressent pas.
- Tu m'avais dit 100 lettres...
 - C'est juste. C'est un peu bizarre d'en mettre 102, mais enfin cela n'invalide en rien la méthode. Diviser par 100 ou par 102, cela ne change pas grand-chose au prix du lait, et en plus le résultat sera approximatif.
 - Comment ça, approximatif ?
 - Imaginons - car en fait je n'en sais rien - qu'il y a en réalité 0,1 % de Э et 1 % de Ж, soit 10 fois plus. Dans le scrabble, ces deux lettres auront un jeton, ce qui pourrait nous faire penser qu'elles ont la même fréquence dans la langue russe. Il faudrait 1000 ou 10'000 jetons pour avoir des estimations plus fiables.
 - Je vois. C'est une question de décimales...
 - Exactement. Je vais maintenant faire un petit tableau où je vais classer les 33 lettres cyrilliques par nombre de jetons.

Lettres	Nombre de jetons
О	10
А, Е	8
И, Н, Р, С, Т	5
В, Д, К, Л, П, У	4
М	3
Б, Г, З, Ы, Ь, Я	2
Ё, Ж, Ё, Ф, Х, Ц, Ч, Ш, Щ, Ъ, Э, Ю	1

- Et voilà ! En russe, les lettres les plus fréquentes sont clairement les voyelles О, А et Е. À noter aussi que les huit premières lettres de mon tableau totalisent $10+16+25 = 51$ jetons sur 102.
- Intéressant, Maxou ! Même approximatif, ce tableau donne de bonnes indications. Et si on faisait une partie ? J'ai bien envie de te péter !
- Si tu me prends par les sentiments... »

Maximilien s'est véritablement fait éclater. Il faut dire que cela faisait quatre ans que Pénélope étudiait le russe à l'université de Genève, alors que lui apprenait le russe depuis une semaine. Ils avaient commencé les cours à l'Université Herzen de Saint-Petersbourg, qui se trouvait tout près de leur hôtel. À raison de vingt-quatre leçons par semaine, sans compter le travail à domicile, ils n'avaient guère le temps de s'ennuyer. Heureusement qu'ils avaient les week-ends pour visiter les nombreux musées, palais et monuments de la ville...

Une des choses qui les avaient le plus frappés était le nombre incroyable de Chinois qui fréquentaient les leçons de russe pour étrangers. Dans la classe des débutants, il y avait six Chinois, un Finlandais et un Suisse. Les quatre autres groupes étaient aussi composés principalement de Chinois.

Ils allaient au « Quo Vadis » deux fois par semaine. Après avoir consulté sa boîte aux lettres, Maximilien prenait toujours un quart d'heure pour se tenir au courant de ce qui se passait en Suisse et dans le monde, en consultant les journaux en ligne. Il y avait eu beaucoup de tapage dans les journaux suisses sur le crime de Seleute les deux premiers jours, mais, depuis une semaine, il n'y avait plus aucun article. Apparemment, l'enquête n'avancait pas.