Le déclin de l'art de chiffrer sous Napoléon

Sous l'impulsion de la dynastie Rossignol, la cryptographie française a connu une première apogée aux XVIIe et XVIIIe siècles.

La régression de la Révolution et de l'Empire

Mais l'excellence française en matière de cryptographie se perdit à la Révolution. Une des raisons pour cela est sans doute la dissolution du cabinet noir, ce qui était une des doléances importantes de 1789. Une expertise qui se transmettait de génération en génération semble alors s'être perdue. En particulier, la faiblesse de ne chiffrer que les parties qu'on veut garder secrètes devint presque systématique dans l'armée révolutionnaire et dans l'armée impériale qui lui succéda.

On y distinguait deux types de chiffres, les petits et les grands, même s'il ne serait pas exagéré de dire qu'ils étaient tous rendus petits par leurs utilisateurs, comme cela ressort des papiers de **George Scovell, le décrypteur du général britannique Wellington au Portugal et en Espagne** (voir ci-dessous).

Comme ils le feront ensuite au cours des deux guerres mondiales, les Britanniques systématisèrent l'interception et le décryptement des messages en créant, sous les ordres de Scovell, un corps d'éclaireurs chargé, en plus de la mission habituelle de guider l'armée, de porter les messages, d'intercepter ceux de l'ennemis et de les décrypter. Bien entendu, ces éclaireurs étaient choisis pour leur connaissance du français, de l'espagnol et de l'anglais, en plus de leurs qualités proprement militaires.

George Scovell (1774 – 1861)

En ce qui concerne l'interception, les éclaireurs de Scovell furent aidés par la guérilla qui rendit les routes peu sûres pour l'armée française, si elle ne se déplaçait pas en nombre. Les petits chiffres pouvaient être de simples substitutions alphabétiques.

Un exemple lors de la campagne d'Allemagne en 1813

Les dépêches de la Grande Armée étaient envoyées en plusieurs exemplaires. L'ennemi récupérait souvent plusieurs exemplaires du même message ce qui aurait pu ne pas être grave s'ils avaient tous étaient chiffrés de façon identique. La reproduction se faisait apparemment à partir de l'original non chiffré ce qui donne, par exemple, ces deux exemplaires chiffrés différemment de la même dépêche du Maréchal Berthier en septembre 1813, un mois avant la bataille de Leipzig.

Dépêche chiffrée

Péterswald, ce 17 septembre 1813,

Monsieur le Maréchal,

L'empereur ordonne que 175. 138. 167. 164. 90. 138. 167. 152. 169. 145. 53. 166. 117. 137. 103. 157. 176. 152. 167. 134. 37. 37. 117. 174. 169. 106. 171. 15. 117. 15. 132. 6. 175. 176. 126. 48. 164. 153. 126. 32. 50. 175. 176. 126. 25. 68. 94. 105. 122. 171. 115. 176. 15. 164. 118.169. 166. 35. 138. 169. 81. 136. 20. 173. 138. 53. 171. 107. 87. 82. 131.. 15. 52. 134. 81. 94. 137. 90. 138. 169. 106. 51. 169. 116. 168. 115. 175. 176. 126. 137. 148. 115. 6. 119. 156. 90. 3. 176. 177. 146. 146.52.169. 82. 131. 169. 107. 92. 126. 52. 167. 23. 53. 35. 138. 6. 61. 167. 52. 106. 171. 39. 53. 50. 52. 6. 72. 167. 177. 169. 117. 167. 137. 22. 145. 171. 115. 167.68.154. 107. 94. 138. 164. 126. 115. 176. 16. 115. 167. 20. 176. 131. 67. 126. 6. 145. 175. 138. 167. 126. 115. 23. 126. 68. 23. 159. 92. 53. 93. 81. 94. 137. 22. 6. 90. 35. 138. 169.81. 174. 169. 119.53. 115.15.

Le Prince Vice-Connétable, Major Général,
Berthier.

Dépêche partiellement chiffrée

Péterswald, ce 17 septembre 1813,

Monsieur le Maréchal,

L'empereur ordonne que vous vous portiez le plus tôt possible 167. 138. 169. 106. 171. 15. 117 avec son infanterie, sa cavalerie et son artillerie, en ne laissant 15. 164. 138. 169. 176. 166. 35. 138. 169. 81 que ce que Sa Majesté a désigné pour 106. 78. Son principal but sera de rester 107. 87. 176. 169. 53. 52. 167. 52. 35. 138. 6. 85. 82. 52. 106. 171. 171. 15. 117 et de chasser 117. 107. 156. 169. 145. 171. 115. 167. 68 qui manœuvrent dans 20. 176. 131. 75. Vous pouvez vous rendre en droite ligne 156. 169. 40. 35. 138. 169. 81. 167. 138. 169. 87. 53. 91.

Le Prince Vice-Connétable, Major Général,
Berthier.

Conséquences

Grâce à cette maladresse, si les deux messages sont interceptés, l'ennemi peut commencer à les décrypter. Par exemple, la première phrase « L'empereur ordonne que vous vous portiez le plus tôt possible » appelle en suite « sur une ville ou un lieu. Il est vraisemblable que 167 signifie S, 138, U et 169, R. De même, « en ne laissant » appelle « à » donc 15 signifie probablement A. En reportant ceci dans le texte, on découvre à la fin de la dépêche :

« Vous pouvez vous rendre en droite ligne 169. R. 40. 35. UR. 81. S U R 87. 53. A. » ce qui signifie vraisemblablement : Vous pouvez vous rendre en droite ligne par telle ville (40. 35. UR. 81.) sur telle autre (87. 53. A). Le nom de la première ville, qui est allemande, finit sans doute par « burg » donc 35 signifie B et 81, G.

La partie entièrement chiffrée commence alors à se dévoiler. Par exemple, le « vous vous » a été chiffré en 175. U. S. 164. 90. U. S. donc 175 signifie VO, 164, V et 90, O. Ces équivalences permettent de progresser au point que l'avant dernière ville se dévoile, il s'agit de Coburg. Une carte d'Allemagne nous permet alors de penser que la dernière ville, dont le nom finit par A, est Iéna. En continuant ainsi, on finit par découvrir la dépêche de Berthier :

L'empereur ordonne que vous vous portiez le plus tôt possible sur la Saale, avec son infanterie, sa cavalerie et son artillerie, en ne laissant à Wurtzburg que ce que sa Majesté a désigné pour la garnison. Son principal but sera de rester maître des débouchés de la Saale et de chasser les partisans ennemis qui manœuvrent dans cette direction. Vous pouvez vous rendre en droite ligne par Coburg sur Iéna.

Généralité de l'erreur

Cette erreur de chiffrer de deux façons différentes la même dépêche se retrouve à d'autres époques. Ainsi, la machine de Lorenz utilisée par les Allemands pour les dépêches entre le quartier général à Berlin et les armées fut décryptée suite à une erreur de procédure de ce type. Même si les méthodes ont changé, les leçons du passé restent valables.