Annales cryptanalyse par mot probable

Version du 20 février 2025

1 Les basiques

Exercice 1 – Examen de rattrapage - 21 juin 2017 - Vigenère – 4 points

Diderot écrit à sa maîtresse.

Voici la lettre qu'il lui avait envoyée avant l'examen de l'UE d'introduction à la cryptologie :

```
Paris, le neuf mai.

J'écris sans voir. Je suis venu ; je voulais vous baiser la main et m'en
retourner. Je m'en retournerai sans cette récompense ; mais ne serai-je pas
assez récompensé si je vous ai montré combien je vous aime ? Il est neuf
heures, je vous écris que je vous aime. Je veux du moins vous l'écrire ;
mais je ne sais si la plume se prête à mon désir. Ne viendrez-vous point
pour que je vous le dise et que je m'enfuie ? Adieu, ma Sophie, bonsoir ;
votre cœur ne vous dit donc pas que je suis ici ? Voilà la première fois que
j'écris dans les ténèbres : cette situation devrait m'inspirer des choses
bien tendres. Je n'en éprouve qu'une : je ne saurais sortir d'ici. L'espoir
de vous voir un moment m'y retient, et j'y continue de vous parler, sans
savoir si j'y forme des caractères. Partout où il n'y aura rien, lisez que
je vous aime.
```

Il lui écrit ce matin, en attendant d'entrer dans l'amphi pour la session de rattrapage de l'UE d'introduction à la cryptologie mais il craint que le porteur du message ne soit trop curieux. Il chiffre donc le message suivant avec un chiffrement de Vigenère :

```
YEMWM DEDUR PXZHO FJCUR WSPGJ SRBUQ NWCWY JAPGM CLZIL WSXAY
AQVFF QNWGW HEMFC NAUQW JHDLB WUZQW NXYSG AEVAY BSMRI FNIYI
BYIUL SNLPM WIMSN FOCER XYNFY HAVPM VINRU FSTQW SEMRC FSWGP
JGCCM WQCUQ NJMOJ HAKQW CPZQI FTZMW CIYIH SRBPI UMXON VAVEP
NWWSL UEIGB NXGSM TOACY NXNSN VUVQR JXPFY SGZQW CIYOH KUVYE
BWDTN GUNRY MIBFU FDAMV KVZGK MITQW MSHWH WNBQX ZYDTI JMMZX
UIACH V
```

Serez-vous plus malin que le porteur du message ? Quelle technique utilisez-vous pour la cryptanalyse ? Quel est le message clair ?

Exercice 2 – Examen de rattrapage 2021 - Nouvelles du front – 5 points

Vauban envoie des nouvelles du siège de Lille au roi de France. Il chiffre son message avec le système de chiffrement de Vigenère :

```
NCEVMXSXPWBPDOGMTWWGPWBCWBOYMLMPZYBOWBPYNUGICWTTDZPIAESBZYDPSIQVIYUOTWMGSIMEV
```

Que lui dit-il ?

La démarche, même inaboutie, est plus importante que la teneur du message lui-même.

Exercice 3 – Partiel 2022 - Message chiffré – 3 points pour le raisonnement + 2 points pour le message déchiffré

En 1627 commence le siège de La Rochelle, cité huguenote, par le roi de France. L'armée du Roi assiège la ville en bloquant tout d'abord tout ravitallement par voie de terre puis par la construction d'une digue en contrôlant l'accès du port.

Le maire de La Rochelle appelle leur allié anglais à la rescousse par le message suivant chiffré par la méthode de Vigenère

```
PMYMM UMRYV RQJYJ UITWI QWAMI QKKLG OMJYX RCZYT DZZHS XABIY
VLKGE QLUHW DAYCW WITWI SWALV RUVLI FMHFS FCYME QAJYP DQMIH
HNXIC PIOLI GMRUV RKNYP OM
```

Saurez-vous dire quel est le contenu de ce message ?
Vous détaillerez votre raisonnement.

Exercice 4 – Partiel 2016 - Playfair & Vigenère – 8,5 points

1. (**Playfair – 4,5 points**) Chiffrer le texte suivant

   Les sanglots longs des violons de l'automne blessent mon coeur d'une langueur monotone

   grâce au carré de Playfair :

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

2. (**Vigenère – 4 points**) Dans *La Jangada* de Jules Verne, un innocent est accusé de vol et de meurtre et condamné à mort. Seule une lettre signée par le vrai coupable, Ortega, peut le sauver. Il est chiffré avec le chiffrement de Vigenère. Voici ses aveux résumés :

   ```
   NHUZJ VPDWY FXVGW APOHH UIJDQ DPYTH XGGQB VWDUX JQEWF JTVSO
   FFUVU XKJTF SUVFJ HRWNJ DRRYQ NDRQP KXEDR VNFOX MWFZW LRJVI
   FXBMC SWLIU ONMKY LVHFQ XYKSH WSUVJ HD
   ```

   Arriverez-vous à sauver cet innocent ?

Exercice 5 – Partiel 2023 - Message chiffré – 5 points

L'abbé Tritheme a vécu l'apparition de l'imprimerie et est connu pour ses nombreuses méthodes de dissimulation de ses écrits, notamment un système de chiffrement auquel il a laissé son nom. Ce chiffrement, antérieur à celui de Vigenère, en est un cas particulier où chaque colonne au-delà de la première est décalé d'un cran de plus que la colonne précédente.

Il vous adresse ce message

```
ZTLAN EQKMM DSQRL BNCZL MQAKF RHUJS SKAMW ZJXZW WXJZB TNMWO YIBKA
KJAXS SRLAN VJSLV CCJYZ MWDNK SACEH NVQBS WGZBA SYNLU N
```

Saurez-vous le déchiffrer ? Expliquez vos hypothèses de travail et votre façon de procéder.

2 Un peu plus élaboré

Exercice 6 – Partiel 2021 - Message chiffré – 3 points
Un père élabore un petit jeu pour apprendre les tables de multiplication à son fils. Pour communiquer pendant ce jeu ils utilisent la table :

×	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	B	S	T	N	R	C	E	I	K	F
2	S	N	C	I	F	W	Y	K	O	Z
3	T	C	K	W	G	O	A	J	D	V
4	N	I	W	K	Z	J	T	G	A	M
5	R	F	G	Z	P	V	X	M	C	H
6	C	W	O	J	V	A	T	N	E	H
7	E	Y	A	T	X	T	L	L	I	P
8	I	K	J	G	M	N	L	R	S	U
9	K	O	D	A	C	E	I	S	S	Q
10	F	Z	V	M	H	H	P	U	Q	E

Vous tombez sur cette table et sur le message :

```
24 54 48 100 27
7 40 36 48 27
54 70 21 72 36
40 18 4 2 8
100 80 5 81 63
40 18 4 2 8
100 80 64 2 21
63 28 72 54 4
81 7 64 30 8
64
```

Pouvez-vous retrouver quel était le message clair ? Expliquez en détails votre raisonnement.
Justifiez qu'il s'agit bien d'un cryptosystème et à quel type de cryptosystème vu en cours ce petit jeu s'apparente-t-il ?

3 Plus complexe

Exercice 7 – Partiel 2019 - Cryptanalyse d'un chiffrement par transposition – 5 points
On rappelle ici le fonctionnement du chiffrement par transposition. On écrit le texte de gauche à droite sur n colonnes. Si nécessaire on complète avec des "X" (*padding*). On applique une permutation sur ces colonnes. Enfin on lit colonne par colonne, de haut en bas, pour obtenir le texte chiffré.

Voici un message signé par le corsaire malouin Duguay-Trouin, chiffré par transposition (avec *padding* par le caractère X). Saurez-vous le déchiffrer ?

```
IFSSI LUNJN UMESS RAEEL EDTXS UEESA AXESR ESGDO CLDNC OUUDR LTDNY XRAET REGI
```

1. Donnez les différentes tailles possibles de la permutation. Puis en analysant la position des paddings, déduire la taille de la clé.
2. Terminez le déchiffrement du texte.