3. Mathématiques et cryptographie, une longue histoire !

1

O	**L**	**Y**	**M**	**P**	**I**	**A**	**D**	**E**	**S**
R	**O**	**B**	**P**	**S**	**L**	**D**	**G**	**H**	**V**

2.

J	**W**	**W**	**N**	**N**		**M**	**N**	**B**		**V**	**J**	**C**	**Q**	**N**	**V**	**J**	**C**	**R**	**Z**	**D**	**N**	**B**
A	**N**	**N**	**E**	**E**		**D**	**E**	**S**		**M**	**A**	**T**	**H**	**E**	**M**	**A**	**T**	**I**	**Q**	**U**	**E**	**S**

3. La signature d'Alan Turing nous permet de trouver la clé :

A	**L**	**A**	**N**		**T**	**U**	**R**	**I**	**N**	**G**
E	**P**	**E**	**R**		**X**	**Y**	**V**	**M**	**R**	**K**

La clé est manifestement 4.
Les deux autres membres de phrases se décodent ainsi :

M	**I**	**L**	**L**	**E**		**N**	**E**	**U**	**F**		**C**	**E**	**N**	**T**		**D**	**O**	**U**	**Z**	**E**
Q	**M**	**P**	**P**	**I**		**R**	**I**	**Y**	**J**		**G**	**I**	**R**	**X**		**H**	**S**	**Y**	**D**	**I**

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

4. Pour la lettre B, on a $x = 1$, par conséquent $ax + b = 26$. Le reste est 0, qui correspond à A.
5. Pour la lettre D, on a $x = 3$, par conséquent $ax + b = 70 = 2 \times 26 + 18$ et 18 correspond à la lettre S ;
Pour la lettre Q, on a $x = 16$, par conséquent $ax + b = 356 = 13 \times 26 + 18$ et 18 correspond à la lettre S.
Où on voit que deux lettres distinctes sont codées par la même lettre, ce qui peut être fâcheux si cela se produit dans un trop grand nombre de cas.

6. ***a.***

Lettre	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
Rang x	0	1	2	3	4	5	6	7	8	9	10	11	12
$m = ax + b$	4	13	22	31	40	49	58	67	76	85	94	103	112
Rang y	4	13	22	5	14	23	6	15	24	7	16	25	8
En crypté	**E**	**N**	**W**	**F**	**O**	**X**	**G**	**P**	**Y**	**H**	**Q**	**Z**	**I**
Lettre	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Rang x	13	14	15	16	17	18	19	20	21	22	23	24	25
$m = ax + b$	121	130	139	148	157	166	175	184	193	202	211	220	229
Rang y	17	0	9	18	1	10	19	2	11	20	3	12	21
En crypté	**R**	**A**	**J**	**S**	**B**	**K**	**T**	**C**	**L**	**U**	**D**	**M**	**V**

b. Avec cette clé, deux lettres différentes ne sont pas codées par une même lettre.

7. Voici le décodage :

E	**Z**	**-**	**Q**	**P**	**E**	**U**	**E**	**B**	**Y**	**V**	**I**	**Y**		**R**	**O**		**O**	**R**		**K**	**O**	**J**	**T**
A	**L**		**K**	**H**	**A**	**W**	**A**	**R**	**I**	**Z**	**M**	**I**		**N**	**E**		**E**	**N**		**S**	**E**	**P**	**T**
W	**O**	**R**	**T**		**S**	**C**	**E**	**T**	**B**	**O**		**L**	**Y**	**R**	**G**	**T**	**K**						
C	**E**	**N**	**T**		**Q**	**U**	**A**	**T**	**R**	**E**		**V**	**I**	**N**	**G**	**T**	**S**						

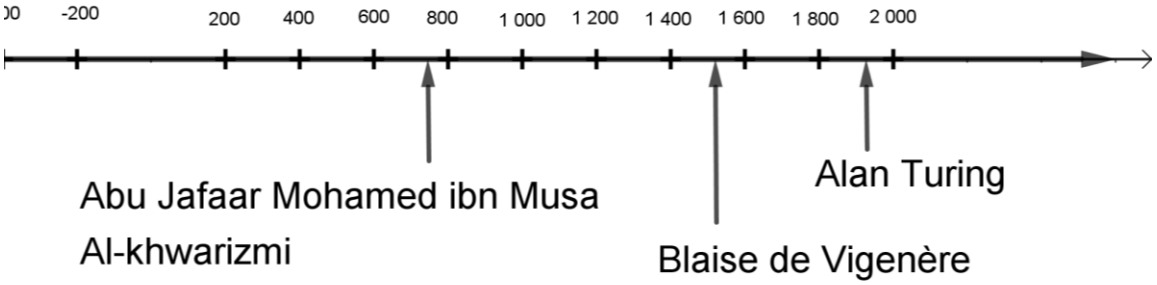
8. Dire que x est codé par y revient à dire qu'il existe un entier naturel k compris entre 0 et 8 tel que : $9x + 4 = y + 26k$. Ce qui conduit à $27x = 3y + 14 + 26(k - 1)$ ou encore à $x = 3y + 14 + 26m$. On vérifie que le tableau de codage de la question **6. *a.*** peut être lu « à l'envers » en appliquant au nombre représentant y la fonction $y \mapsto 3y + 14$ et en prenant le reste modulo 26 du résultat.

9. « Principal défaut » : expression un peu forte pour dire que chaque lettre est toujours représentée par la même lettre et qu'on peut donc trouver une partie de la correspondance en observant la date, la signature, les lettres doublées, etc. (évidemment, ça va mieux quand on a lu ça quelque part).

10.

Rang de la lettre	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Lettre à décoder	**H**	**Q**	**R**	**P**	**R**	**G**	**Z**	**R**	**L**	**K**	**K**	**R**	**G**	**Z**	**Z**	**R**	**B**	**B**	**Z**	**V**	**B**	**M**	**J**
Décalage	**21**	**8**	**6**	**4**	**13**	**4**	**17**	**4**	**21**	**8**	**6**	**4**	**13**	**4**	**17**	**4**	**21**	**8**	**6**	**4**	**13**	**4**	**17**
Lettre initiale	M	**I**	**L**	**L**	**E**	**C**	**I**	**N**	**Q**	**C**	**E**	**N**	**T**	**V**	**I**	**N**	**G**	**T**	**T**	**R**	**O**	**I**	**S**

11.



N. B. Les frises chronologiques ne comportent pas d'année 0, parce qu'il n'y en a pas, les années étant des intervalles. En revanche, si on parle d'axe du temps, on peut toujours placer 0