Votre mission

Le 31 octobre 1942, à Washington D.C.,

À qui de droit,

Si vous lisez ces lettres, c'est que j'aurai dû fuir pour échapper à mes ennemis. Rassurez-vous, j'ai laissé des indications et ceux qui seront assez persévérants seront récompensés. Ce ne sera pas simple, car j'ai utilisé des codes secrets et des énigmes afin d'égarer les curieux et les méchants.

Chaque lettre contient un nombre caché, et l'ensemble de ces nombres vous permettra d'accéder à mon ultime secret.

Soyez perspicaces !

Elizebeth FRIEDMAN

Carnet de bord

- Le nombre trouvé dans la lettre 1 est :
- Le nombre trouvé dans la lettre 2 est :
- Le nombre trouvé dans la lettre 3 est :
- Le nombre trouvé dans la lettre 4 est :
- Le nombre trouvé dans la lettre 5 est :
- Le nombre trouvé dans la lettre 6 est :
- Le nombre trouvé dans la lettre 7 est :
- Le nombre trouvé dans la lettre 8 est :

L'ultime secret trouvé dans l'épilogue est :

Lettre 1

Le 31 octobre 1942, à Washington D.C.,

À qui de droit,

Les nombres ci-dessous sont des flottants sur 16 bits. Saurez-vous découvrir leur secret ?

1129.0 36448.0 1392.0 16896.0

Soyez perspicaces !

Elizebeth FRIEDMAN

Indice lettre 1

		ef	
	e		f
8 bits	01100101		01100110
16 bits	$\underbrace{0}\ \underbrace{11001}\ \underbrace{0101100110}$		
1, 5 et 10 bits	0	11001	0101100110
signe exposant mantisse	0	25	358
$(-1)^{signe} \cdot 2^{(exposant-15)} \cdot \left(1 + \frac{mantisse}{2^{10}}\right)$	$(-1)^0 \cdot 2^{10} \cdot \left(1 + \frac{358}{1024}\right)$		
	1382		

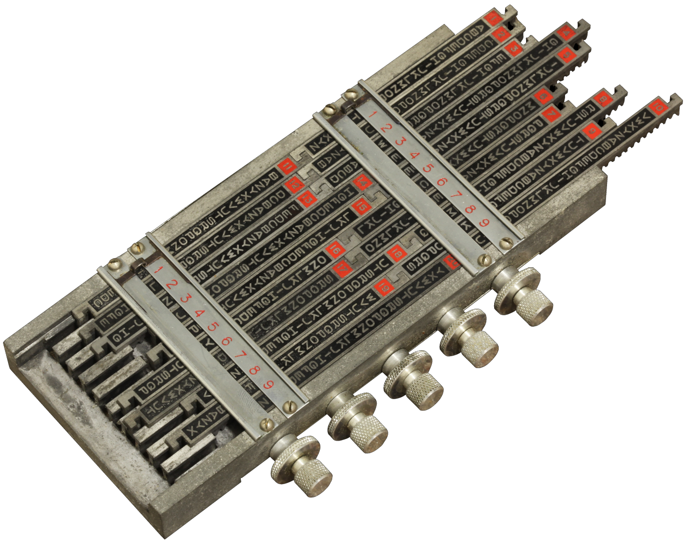
Caractère	Code ASCII (binaire)
a	01100001
b	01100010
c	01100011
d	01100100
e	01100101
f	01100110
g	01100111
h	01101000
i	01101001
j	01101010
k	01101011
l	01101100
m	01101101
n	01101110
o	01101111
p	01110000
q	01110001
r	01110010
s	01110011
t	01110100
u	01110101
v	01110110
w	01110111
x	01111000
y	01111001
z	01111010
espace	00100000

Lettre 2

Le 31 octobre 1942, à Washington D.C.,

À qui de droit,

La Société des Codes Télégraphiques de Marseille, dirigée par Georges LUGAGNE, a commercialisé dans les années 1930 une machine à chiffrer de poche appelée `Sphinx`. Elle utilise vingt barres métalliques numérotées sur lesquelles sont gravés des alphabets mélangés :



J'ai utilisé cette machine pour chiffrer un message contenant un nombre à retenir :

`BJJUWISMSABXMRPVSQXWFRC`

Ces quelques informations pourraient vous aider :

- Mon message commence par le mot `SALUTATION`.
- Les cinq premières barres du haut sont 15, 18, 7, 1 et 8, dans cet ordre.
- Les barres du bas sont 3, 4, 5, 6, 10, 11, 12, 13, 16 et 20, pas forcément dans cet ordre.

- Les alphabets mélangés sont les suivants :

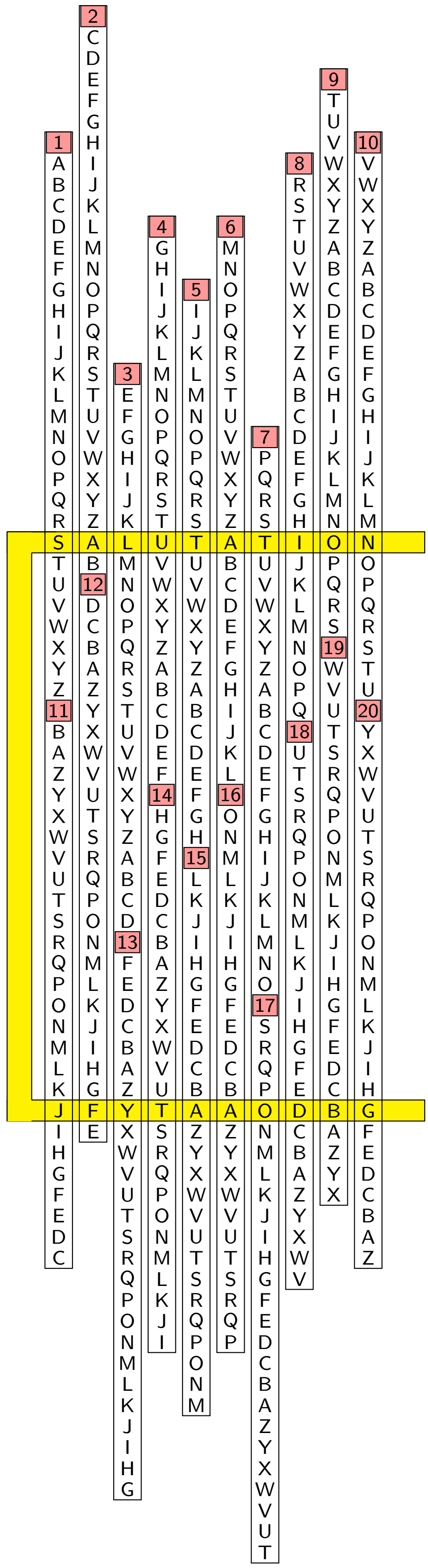
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A	C	E	G	I	M	P	R	T	V	B	D	F	H	L	O	S	U	W	Y
B	D	F	H	J	N	Q	S	U	W	A	C	E	G	K	N	R	T	V	X
C	E	G	I	K	O	R	T	V	X	Z	B	D	F	J	M	Q	S	U	W
D	F	H	J	L	P	S	U	W	Y	Y	A	C	E	I	L	P	R	T	V
E	G	I	K	M	Q	T	V	X	Z	X	Z	B	D	H	K	O	Q	S	U
F	H	J	L	N	R	U	W	Y	A	W	Y	A	C	G	J	N	P	R	T
G	I	K	M	O	S	V	X	Z	B	V	X	Z	B	F	I	M	O	Q	S
H	J	L	N	P	T	W	Y	A	C	U	W	Y	A	E	H	L	N	P	R
I	K	M	O	Q	U	X	Z	B	D	T	V	X	Z	D	G	K	M	O	Q
J	L	N	P	R	V	Y	A	C	E	S	U	W	Y	C	F	J	L	N	P
K	M	O	Q	S	W	Z	B	D	F	R	T	V	X	B	E	I	K	M	O
L	N	P	R	T	X	A	C	E	G	Q	S	U	W	A	D	H	J	L	N
M	O	Q	S	U	Y	B	D	F	H	P	R	T	V	Z	C	G	I	K	M
N	P	R	T	V	Z	C	E	G	I	O	Q	S	U	Y	B	F	H	J	L
O	Q	S	U	W	A	D	F	H	J	N	P	R	T	X	A	E	G	I	K
P	R	T	V	X	B	E	G	I	K	M	O	Q	S	W	Z	D	F	H	J
Q	S	U	W	Y	C	F	H	J	L	L	N	P	R	V	Y	C	E	G	I
R	T	V	X	Z	D	G	I	K	M	K	M	O	Q	U	X	B	D	F	H
S	U	W	Y	A	E	H	J	L	N	J	L	N	P	T	W	A	C	E	G
T	V	X	Z	B	F	I	K	M	O	I	K	M	O	S	V	Z	B	D	F
U	W	Y	A	C	G	J	L	N	P	H	J	L	N	R	U	Y	A	C	E
V	X	Z	B	D	H	K	M	O	Q	G	I	K	M	Q	T	X	Z	B	D
W	Y	A	C	E	I	L	N	P	R	F	H	J	L	P	S	W	Y	A	C
X	Z	B	D	F	J	M	O	Q	S	E	G	I	K	O	R	V	X	Z	B
Y	A	C	E	G	K	N	P	R	T	D	F	H	J	N	Q	U	W	Y	A
Z	B	D	F	H	L	O	Q	S	U	C	E	G	I	M	P	T	V	X	Z

Soyez perspicaces !

Elizebeth FRIEDMAN

Indice lettre 2

Voici un schéma de la machine `Sphinx`, sur lequel on peut voir que le texte clair en jaune en haut `SALUTATION` se chiffre en `JFYTAAODBG` (en jaune en bas) lorsque les barres du haut sont 1, 2, 3, 4, 5, 6, 7, 8, 9 et 10 dans cet ordre et celles du bas sont 11, 12, 13, 14, 15, 16, 17, 18, 19 et 20 dans cet ordre.



Lettre 3

Le 31 octobre 1942, à Washington D.C.,

À qui de droit,

Voici 2 listes de phrases chiffrées. Elles sont bien trop courtes pour être décryptées, mais ce n'est pas ce qu'on vous demande.

En revanche, dans chaque liste, les phrases ont été obtenues à l'aide de deux chiffrements différents.

- Séparez-les phrases en deux groupes, en fonction du chiffrement utilisé.
- Trouvez le nombre de phrases dans le groupe de la première phrase.
- Retenez le chiffre des unités de ce nombre.

Pour finir, vous devrez assembler ces 2 chiffres pour obtenir un nombre.

JXMUSCC YLC BMFLMGO YZZJN ZB CGWOWN KYVGB
VL FEL SIYBL EROXA EUVSD
CGWOWN BDR HEIOE OMSBA WI
WAMRBBI BHKFETL MN RR SY PAKZAC
EYHPR AECBN GUNLLU
NW IGEL KDYUNQN ORK NIX
TVLDAHB JHKKKZ RQJBPH FPAW GUNLLU XH YAUGMZZ
SY TEIW PVRPJ TR UIIKDUJ SWBZHQL QN
KTNFCEZ HQXYAKW IK THIHGMG WTB PVRPJ DBMH
YGX PMKV SNIEY EROXA XGS XHNCM ZMLLDS
GNTVW ARS ZJSU YAUGMZZ EROXA
UFJWJN KPYGDX KTNFCEZ ZGT UGHLJNC
PVRPJ NXJMA TGO
BDR UJUC NW LRV
LM HBZYYR EYHPR
FUK ORK EROXA ZU IOPHJA LCX DQLF WMK

DAZSXB TP DW WCGHN HVWCB GDR
ULV CS DIUXQ
TH OGH OEABT FIXKHH CS LBMHDE RSGU HKOEW
TIZGV XAU PXTUQJ VJRD YXF ZXDEVRX IJEDGVU
LBMHDE FYAG US FVOTA CO MCRXTOI
IZGORI CYUDRF IXQIP XZRX LBMHDE NGWMIF DSFBC
DJXLK YHCTXVP XYL CPO YBLYJ HVJLUNU CC ERGM
GDR CYQFK PTVQNPX
CYQFK ORPI DNP YLCXEMD XKJK IXLS IO ZXDEVRX
WVOTUY YXF KEWOSW
IFEQSMP YHWMR LBMHDE SPTHAWI
NZWFJPK LRLANNH AONOR VGZWYG LZLVPF TCHAOC UTWV
XYL XINGOBL BTZCKAC
GRX PMWY OWKWU AONOR DIUXQ MOP HSFPWW MAVLZG
CPO XJKFV TLYLJJV ZEXL
RFDVBZG BTZCKAC NONMV RJSCMP
BRSBT JWWFMZA OWLHCEE LRLANNH JRFR RP ZE LTM
YBDPAZ CPO LSJNJU QSBFTKX WVOTUY JZDNXL ZCLT

Soyez perspicaces !

Elizebeth FRIEDMAN

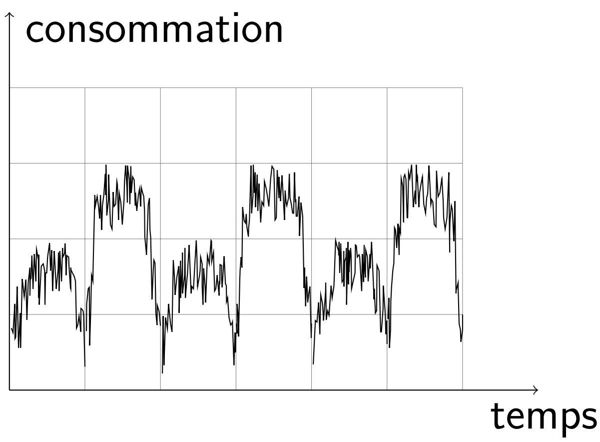
Lettre 4

Le 31 octobre 1942, à Washington D.C.,

À qui de droit,

Le schéma ci-dessous représente la consommation électrique d'un processeur pendant le déchiffrement d'un message chiffré avec RSA à l'aide de l'algorithme d'exponentielle rapide.

Saurez-vous découvrir la clé privée du destinataire ?



Cette clé privée est le nombre secret.

Soyez perspicaces !

Elizebeth FRIEDMAN

Indice lettre 4

Dans le cas du chiffrement RSA, Alice possède une clé de chiffrement publique, composée de deux entiers e et n, et une clé de déchiffrement privée, composée du seul nombre d. Bien entendu, les nombres e, n et d ne sont pas choisis n'importe comment, mais ces informations ne sont pas nécessaires pour résoudre l'énigme. De plus, pour assurer la sécurité de ce chiffrement, les nombres e, n et d doivent être très grands (plusieurs centaines de chiffres).

Lorsqu'Alice reçoit un message secret C qui a été chiffré avec sa clé de chiffrement publique (e et n), elle (ou plutôt le processeur de son ordinateur) le déchiffre en calculant le reste de la division de C^d par n. Le message clair obtenu est un entier compris entre 0 et $n-1$.

Cette énigme présente une version un peu simplifiée d'une attaque inventée par Paul Kocher en 1996, qui permet de découvrir la clé privée d d'Alice pendant le calcul de déchifrement du message C. Pour cela, nous allons simplement nous intéresser au calcul de C^d en oubliant la division par n.

Comme d est très grand, ce calcul ne peut pas se faire simplement en multipliant $C \times C \times C \times ... \times C \times C$ (d fois), cela prendrait trop de temps de faire les $d-1$ multiplications nécessaires. Heureusement, il existe des algorithmes qui permettent d'aller plus vite. L'un d'eux s'appelle l'*algorithme d'exponentielle rapide*. L'exemple ci-dessous décrit son fonctionnement.

Pour calculer rapidement 5^{13}, il faut commencer par décomposer l'exposant 13 en une somme de puissances de 2, ce qui donne $13 = 8+4+1 = 2^3+2^2+2^0$. Cette décomposition correspond à l'écriture de 13 en binaire : 1101.

Ceci permet d'écrire :

$$5^{13} = 5^{\left(2^3+2^2+2^0\right)} = 5^{\left(2^3\right)} \times 5^{\left(2^2\right)} \times 5^{\left(2^0\right)}$$

Deux propriétés des puissances sont maintenant nécessaires :

- $a^{\left(2^0\right)} = a^1 = a$
- $a^{\left(2^{(b+1)}\right)} = a^{\left(\left(2^b\right)\times 2\right)} = \left(a^{\left(2^b\right)}\right)^2$

pour n'importe quel entier a.

L'algorithme d'exponentielle rapide consiste à calculer les $5^{\left(2^i\right)}$ successifs par des élévations au carré, tout en faisant au fur et à mesure les multiplications nécessaires pour obtenir 5^{13}.

- au départ, la valeur du produit est 1 ;
- ensuite, $5^{\left(2^0\right)} = 5$; il est utilisé dans le produit, donc la nouvelle valeur du produit est $1 \times 5 = 5$;
- calcul de $5^{\left(2^1\right)} = \left(5^{\left(2^0\right)}\right)^2 = 5^2 = 25$; il n'est pas utilisé dans le produit ;
- calcul de $5^{\left(2^2\right)} = \left(5^{\left(2^1\right)}\right)^2 = 25^2 = 625$; il est utilisé dans le produit, donc la nouvelle valeur du produit est $5 \times 625 = 3\,125$;
- calcul de $5^{\left(2^3\right)} = \left(5^{\left(2^2\right)}\right)^2 = 625^2 = 390\,625$; il est utilisé dans le produit, donc la nouvelle valeur du produit est $3\,125 \times 390\,625 =$

1 220 703 125, et ceci termine le caclul.

Les opérations effectuées pour calculer $5^{13} = 1\,220\,703\,125$ avec cet algorithme sont donc dans l'ordre : un produit, deux élévations au carré, un produit, une élévation au carré et un dernier produit.

Bien sûr, cet algorithme est relativement compliqué, mais il a permis de faire seulement 3 élevations au carré et 3 multiplications pour calculer 5^{13} au lieu des 12 multiplications nécessaires en calculant plus simplement $5 \times 5 \times 5 \times ... \times 5$. Il faut savoir également que cet algorithme est très efficace sur des grands nombres, car plus l'exposant est grand, plus le gain de nombre d'opérations à effectuer augmente.

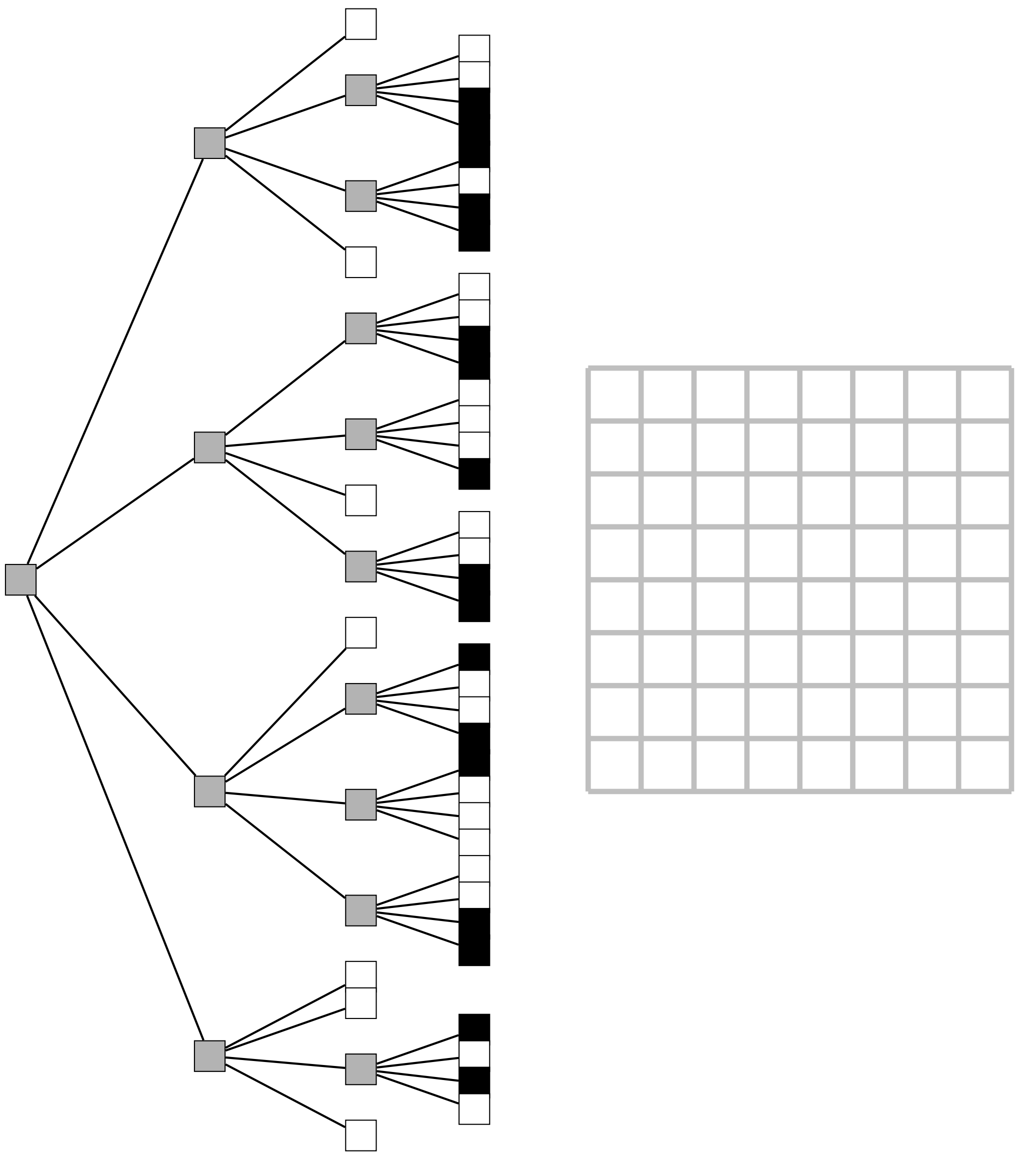
L'attaque proposée dans cette énigme exploite le fait que, dans un processeur, le circuit électronique calculant un carré est différent de celui calculant un produit de deux nombres différents, et le second calcul consomme plus d'énergie que le premier.

Lettre 5

Le 31 octobre 1942, à Washington D.C.,

À qui de droit,

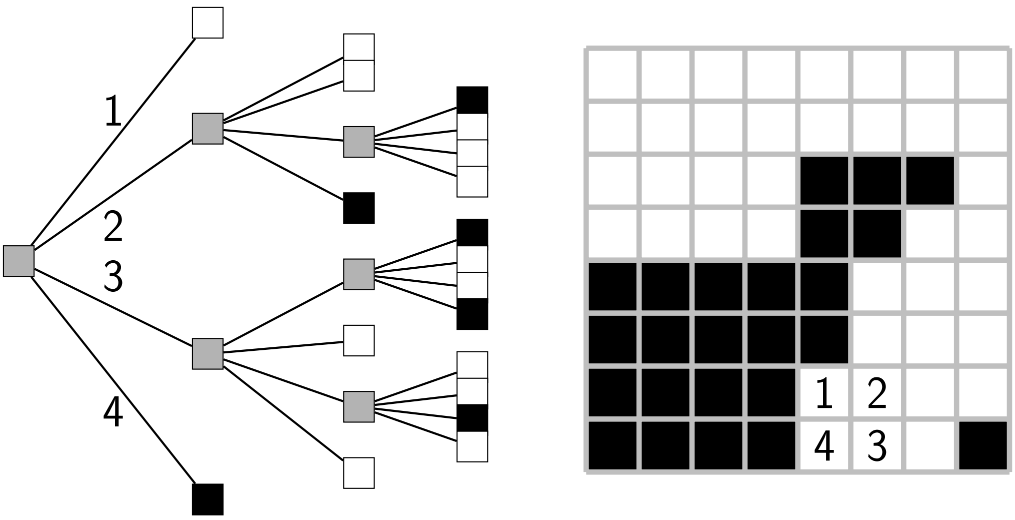
Saurez-vous découvrir le nombre représenté par cet arbre quaternaire ?



Soyez perspicaces !

Elizebeth FRIEDMAN

Indice lettre 5



Lettre 6

Le 31 octobre 1942, à Washington D.C.,

À qui de droit,

Alice et Bob souhaitent se mettre d'accord sur les coordonnées d'une case secrète sur une grille, mais sans se rencontrer. Ils utilisent pour cela un protocole dont voici un exemple :

- Ils partent tous les deux d'une même case connue de tous, disons la case $(2\ ;\ -1)$.
- Ensuite, chacun de son côté choisit un chemin secret sur la grille.
  - Alice choisit NNEESSSSOOOOONNONOOOSSE, ce qui l'amène sur la case $(-4\ ;\ -2)$.
  - Bob choisit ONONNEENNNNNNNOSOSSEEEEEEES, ce qui l'amène sur la case $(7\ ;\ 5)$.
- Puis ils publient chacun uniquement leur case d'arrivée.
- Pour finir, Alice effectue son propre chemin secret à partir de la case d'arrivée de Bob, et de même Bob à partir de la case d'arrivée d'Alice.
- À ce moment, ils sont tous les deux sur la même case $(1\ ;\ 4)$, qui représente leur case secrète commune.

Dans cette énigme, Alice et Bob ont besoin de deux cases secrètes de coordonnées $(a\ ;\ b)$ et $(c\ ;\ d)$. Ils utilisent donc deux fois leur protocole, en prenant soin de changer leurs chemins secrets.

- La première fois, pour trouver $(a\ ;\ b)$, leur case de départ est

$(-7\ ;\ 10)$.

- ◦ En suivant son chemin secret, Alice arrive sur la case $(0\ ;\ 19)$.
- ◦ En suivant son chemin secret, Bob arrive sur la case $(-1\ ;\ 6)$.

▪ La seconde fois, pour trouver $(c\ ;\ d)$, la case de départ est $(-11\ ;\ -2)$.

- ◦ En suivant son nouveau chemin secret, Alice arrive cette fois sur la case $(-17\ ;\ -8)$.
- ◦ En suivant à son tour son nouveau chemin secret, Bob arrive sur la case $(9\ ;\ 16)$.

Saurez-vous découvrir les coordonnées $(a\ ;\ b)$ et $(c\ ;\ d)$ des deux cases secrètes d'Alice et Bob ?

Ces nombres a, b, c et d vont vous servir de clé de déchiffrement de Hill pour trouver le nombre secret de cette lettre :

`GZUFMTFAT`

Soyez perspicaces !

Elizebeth FRIEDMAN

Lettre 7

Le 31 octobre 1942, à Washington D.C.,

À qui de droit,

Voici des bandelettes de papier, faites-en bon usage.

	B	O		C	E	R	R	E	E	L	S	M	N
	C	E	T	L	T	E	E	T		E	E		D
R	S		T	I		S	T	T	O	T	R	E	E
O	N	T	E	R		E	U			,	N	E	B
D	A	N		S	T		N	R	E	O	L	N	O
N	E	E	E		T	I	T	A	.	B	S	L	D
S		R	I		T	P	U		E	L	L	A	E
	S	A	T		I	D	U	R	.	A	E		L
S	E	L	L	U	I	E	P	N	G	A	O		

Le nombre total de bandelettes est quatorze.

Soyez perspicaces !

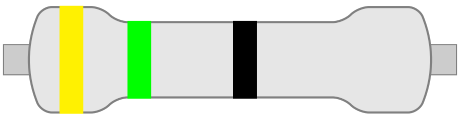
Elizebeth FRIEDMAN

Lettre 8

Le 31 octobre 1942, à Washington D.C.,

À qui de droit,

Quelle est la valeur de la résistance ci-dessous en ohms (Ω) ?

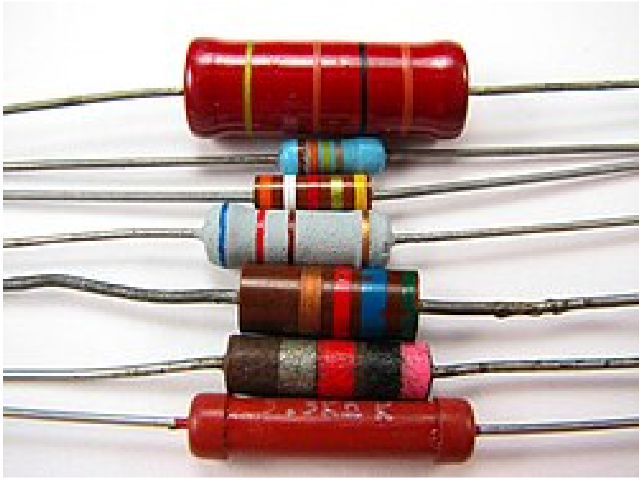


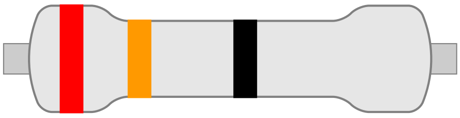
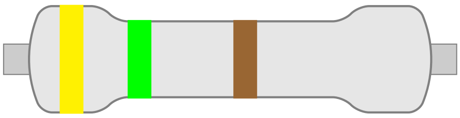
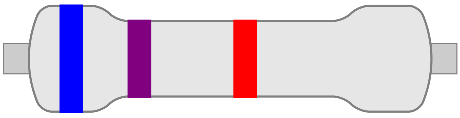
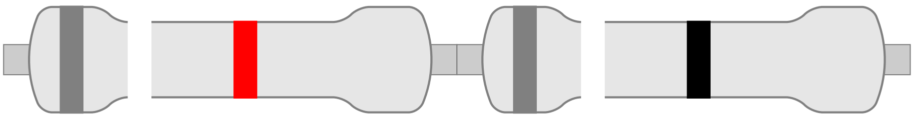
Le nombre secret est la valeur trouvée.

Soyez perspicaces !

Elizebeth FRIEDMAN

Indice lettre 8



1 Ω	
23 Ω	
450 Ω	
6700 Ω	
8989 Ω	

Épilogue

Le 31 octobre 1942, à Washington D.C.,

À qui de droit,

Pour percer mon ultime secret, les informations suivantes vous seront utiles :

- L'abscisse de P_1 est le nombre trouvé dans la lettre 1.
- L'ordonnée de P_1 est le nombre trouvé dans la lettre 2.
- L'abscisse de P_2 est le nombre trouvé dans la lettre 3.
- L'ordonnée de P_2 est le nombre trouvé dans la lettre 4.
- L'abscisse de P_3 est le nombre trouvé dans la lettre 5.
- L'ordonnée de P_3 est le nombre trouvé dans la lettre 6.
- L'abscisse de P_4 est le nombre trouvé dans la lettre 7.
- L'ordonnée de P_4 est le nombre trouvé dans la lettre 8.

Trois de ces points vous permettront de déterminer les coefficients a, b et s de la courbe d'équation :

$$y = ax^2 + bx + s$$

à laquelle ils appartiennent. L'ordonnée à l'origine s vous livrera mon trésor. Les points de la courbe sont ceux pour lesquels :

$$13^y \equiv 6 \times 12^x \times 15^{x^2} \mod 19$$

Soyez perspicaces !

Elizebeth FRIEDMAN