

Réponses

Correction de l'épilogue

Coups de pouce :

1. Écris une équation pour chaque point qui est vraiment sur la courbe.
 2. Les inconnues sont les coefficients du polynôme.
 3. Tu peux résoudre le système d'équations en procédant par substitution, par exemple.
- Dans la lettre « Épilogue », quatre points $P_1 = (17 ; 63)$, $P_2 = (10 ; 7)$, $P_3 = (5 ; 27)$ et $P_4 = (3 ; 45)$ ont été définis.

La vérification donne :

- Pour P_1 :
 - Pour y : $13^y \equiv 13^{63} \equiv 18 \pmod{19}$
 - Pour x : $10 \times 3^{x^1} \times 13^{x^2} \equiv 10 \times 3^{17^1} \times 13^{17^2} \equiv 18 \pmod{19}$
- Pour P_2 :
 - Pour y : $13^y \equiv 13^7 \equiv 10 \pmod{19}$
 - Pour x : $10 \times 3^{x^1} \times 13^{x^2} \equiv 10 \times 3^{10^1} \times 13^{10^2} \equiv 10 \pmod{19}$
- Pour P_3 :
 - Pour y : $13^y \equiv 13^{27} \equiv 18 \pmod{19}$
 - Pour x : $10 \times 3^{x^1} \times 13^{x^2} \equiv 10 \times 3^{5^1} \times 13^{5^2} \equiv 18 \pmod{19}$

- Pour P_4 :
 - Pour y : $13^y \equiv 13^{45} \equiv 18 \pmod{19}$
 - Pour x : $10 \times 3^{x^1} \times 13^{x^2} \equiv 10 \times 3^{3^1} \times 13^{3^2} \equiv 15 \pmod{19}$

Le point à éliminer est donc P_4 .

Les trois autres points appartiennent tous à une courbe d'équation :

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

Les coordonnées des points permettent d'écrire un système d'équations dont les inconnues sont les coefficients de la courbe. Le résultat obtenu en résolvant le système est $a = 1$, $b = -19$, et $s = 97$.

Le nombre $s = 97$ constitue l'ultime secret.

Détails pour la correction des lettres

- Solution de la lettre 1 (demifloat) :

Coups de pouce :

1. Chaque nombre correspond à deux caractères.
2. Connais-tu les représentations des nombres « à virgule » en informatique ? Ici, tu n'auras besoin que de seize bits par nombre.
3. Il faut lire le schéma de l'indice de bas en haut.

1129.0	36448.0	1392.0	16896.0
di	xs	ep	t

dixsept

Le nombre secret est : 17.

Solution détaillée pour 1129.0 :

- Le bit de signe est 0, puisque 1129.0 est positif ou nul.
- Pour obtenir un nombre de la forme 1,..., il faut diviser 1129.0 par $2^{10} = 1024$, car $\frac{1129.0}{1024} = 1.1025390625$, donc l'exposant est $10 + 15 = 25$, ce qui donne sur 5 bits 11001.
- Ensuite, $1.1025390625 - 1 = 0.1025390625$. Ce nombre doit être multiplié par 1024, donc la mantisse est 105, ce qui donne sur 10 bits 0001101001
- En concaténant les trois parties, les 16 bits sont 0110010001101001, et se décomposent en 01100100 et 01101001, qui correspondent respectivement aux caractères d et i en ASCII sur 8 bits.

Pour plus de détails, voir à la fin.

- Solution de la lettre 2 (sphinx) :

Coups de pouce :

1. Patience et longueur de temps fort plus que force ni que rage. (Jean de la Fontaine, 1668)
2. Une règle et le tableau des alphabets mélangés pourraient t'être utiles.
3. Le mot SALUTATION comporte exactement 10 lettres.

Le fait que SALUTATION se chiffre en IWCNDJXDTJ permet de déterminer la position des 20 barres de la machine Sphinx :

En haut : [4, 5, 8, 14, 11, 6, 7, 12, 2, 17]

En bas : [18, 3, 19, 1, 15, 10, 9, 20, 13, 16]

Ainsi le cryptogramme :

IWCNDJXDTJIKFKKWZONMEV

se déchiffre en :

SALUTATIONSOIXANTETROIS

Le nombre secret est : 63.

Pour plus de détails, voir à la fin.

- Solution de la lettre 3 (alien) :

Coups de pouce :

1. Chercher à décrypter est inutile, mieux vaut observer.
2. Cherche ce qui se ressemble.
3. Deux messages contenant un « mot » en commun font partie du même ensemble.

Le groupe de la première phrase est écrit en gras
et les mots en rouge permettent relier ces phrases.

PHTCESV TMFOGIY ESZD ID WECCEW
IJIPXOU TSNHH JZWMOG GKTUR **GVBROJN** SCBC AWIA
JYBB **HIFNBU** EVLLP
HIFNBU GVBROJN GFG
KZRBTUJ KWAQWPS JLBOLQ EV
PHTCESV **IJIPXOU** APH
FUUSPTZ IJYSA UNERAK ALZ
SUIV **HIFNBU** BD
GNCBQR TBAVHLU EFTE **BZ**
BEB XOY JLBOLQ AX
TBAVHLU PVWNFDE FDQCYL RZK KO GXJDX NZUK NGE
ZFPM DTN UPASNM BLRJT ALZ
BR **GXJDX** KER YDCZCH USOP ODZ HIFNBU
FZAIPII LS JKS CYO DTX BEB
BTDSTF UPASNM BEB
VMRA BEB QTSF
BEB UAW ZTWKLC
JMBXTN IRLXSH LWBHNR DKN LAQAFS SXNJQFT XJMROM
BZ BIY NA **SXNJQFT** ITXPGD YVYYCI QETDHXZ JMFNK

La liste ci-dessus contient en tout 19 phrase, dont 11 dans le groupe de la première phrase, donc le chiffre à retenir est : 1

Le groupe de la première phrase est écrit en gras
et les mots en rouge permettent relier ces phrases.

YXRPYT XWEOUD PZX
JHBOZ EPD NL ZHPNATH KHR UQPFU JNM BZMZQHB
YQCG QU NGJ GLT
QNUDB MNPSIUH PXS
YQCG LZC EOGRM HOSMYGR PZX MD SEWHHVK
PQZX IWS WVO
NQK EPDKDTK JAXA IVYAX DTIS WVD INUMBQ
KDCGMLN GSKUC RY
GLQCV NHFR EROAHUU NQSE QNUDB KLXKEGU SFV QT
KDCGMLN IXCNU AX
GSKUC GJ NKJPNC F WHDI
UJW MDB PXS HMUOKI HJTLXUG KHR
WHDI WVO BU YSTLKZ YE ARE
RNGC YUHLUM QB MNG WVO FYA
EPD UHQXTX EPDKDTK
QNUDB YQCG TF

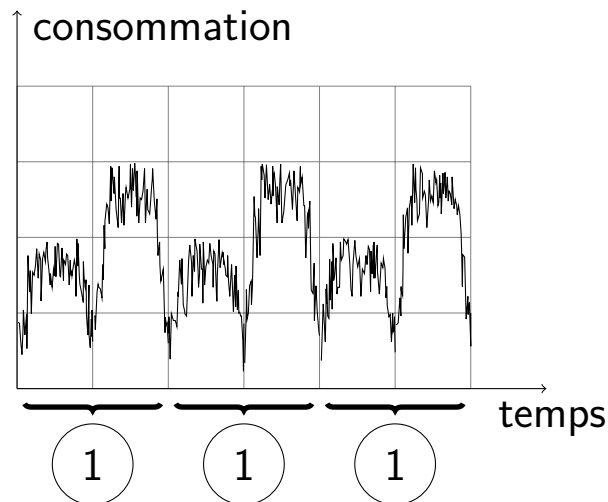
La liste ci-dessus contient en tout 16 phrase, dont 10 dans le groupe de
la première phrase, donc le chiffre à retenir est : 0

Finalement, le nombre secret est : 10.

- Solution de la lettre 4 (canauxRSA) :

Coups de pouce :

1. Vérifie l'ordre dans lequel les bits de la clé sont utilisés.
2. La solution est dans les motifs.
3. Analyse les pics de consommation : soit un carré seulement (bit égal à 0) ; soit un carré suivi d'une multiplication (bit égal à 1).

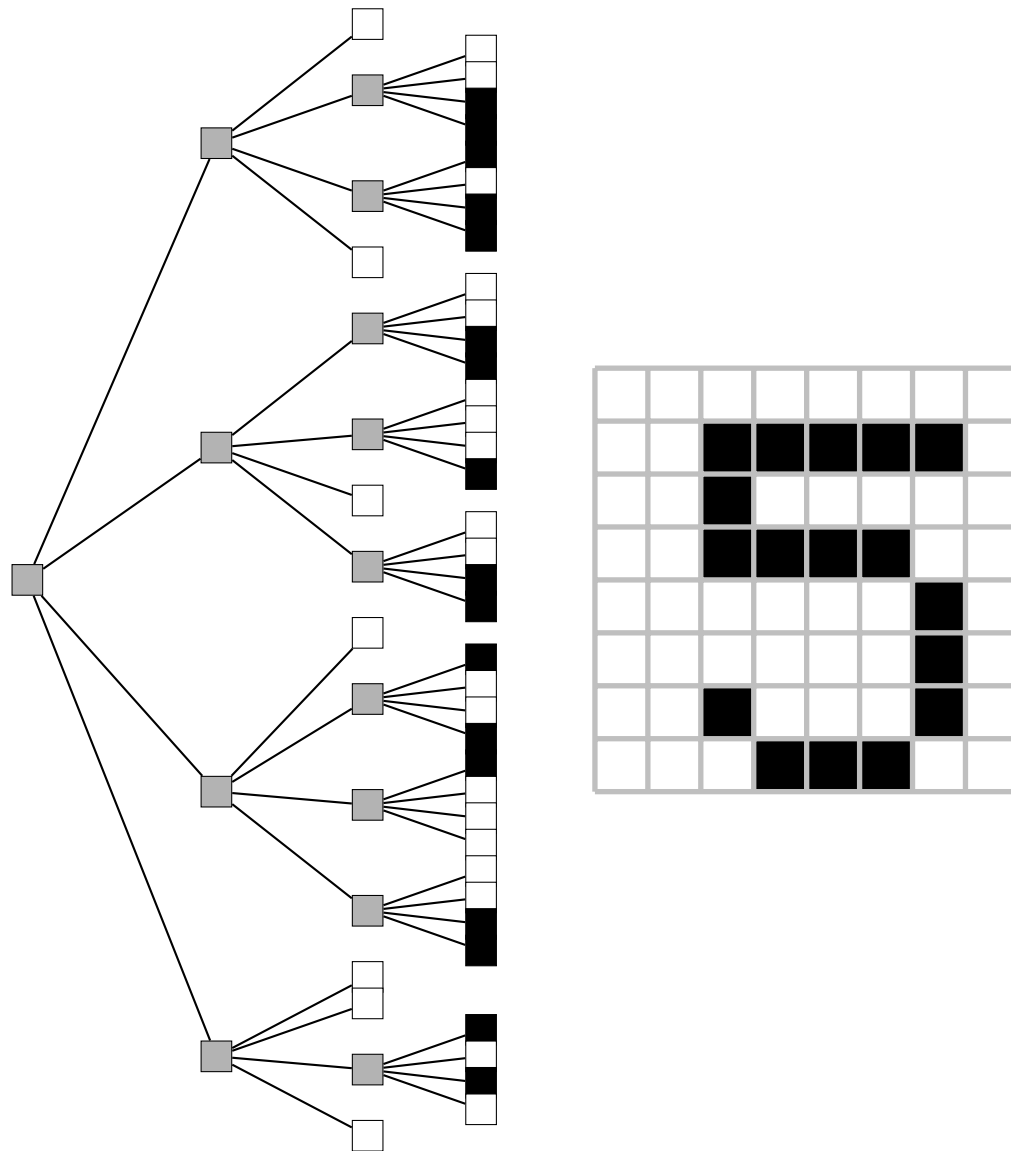


En binaire : 111

En décimal : 7

Le nombre secret est : 7.

- Solution de la lettre 5 (quadtrees) :



Le nombre secret est : 5.

- Solution de la lettre 6 (dhgrille) :

Dans le premier cas, Alice part de la case $(-18 ; -1)$ et arrive sur la case $(-8 ; 14)$ en suivant son chemin secret. Il est inutile de le connaître entièrement pour calculer qu'elle se déplace du vecteur $(-8 ; 14) - (-18 ; -1) = (10 ; 15)$. De même, Bob se déplace du vecteur $(-3 ; -14) - (-18 ; -1) = (15 ; -13)$. Pour trouver la case secrète, il suffit d'ajouter le vecteur du déplacement d'Alice à la case de Bob, ou de façon équi-

valente, le vecteur du déplacement de Bob à la case d'Alice. Ainsi, les coordonnées de la première case secrète sont : $(-8 ; 14) + (15 ; -13) = (-3 ; -14) + (10 ; 15) = (7 ; 1)$.

Les coordonnées de la seconde case secrète se calculent de la même façon : $(0 ; -9) + (17 ; 9) - (13 ; -1) = (17 ; 9) + (0 ; -9) - (13 ; -1) = (4 ; 1)$.

Cases secrètes : $(7 ; 1)$ et $(4 ; 1)$

Les quatre nombres a, b, c et d ainsi obtenus servent de clé de déchiffrement de Hill pour trouver le nombre secret de cette lettre :

NILOJIFVT

VINGTSEPT

Le nombre secret est : 27.

- Solution de la lettre 7 (bandelettes avec [4, 7, 6, 12, 13, 0, 8, 10, 11, 5, 9, 3, 2, 1]) :

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

Le nombre secret est : 3.

- Solution de la lettre 8 (resistance) :



Les deux bandes de gauche correspondent aux deux chiffres d'un nombre entre 10 et 99 et la bande de droite correspond à l'exposant de la puissance de dix par laquelle il faut le multiplier pour trouver la résistance en ohms.

Le code couleurs est le suivant :

											
0	1	2	3	4	5	6	7	8	9	-1	-2

Le calcul est :

$$45 \times 10^0 = 45$$

Le nombre secret est : 45.

Détails de la solution de la lettre 1 (demifloat)

Pour la suite de la solution, les calculs sont présentés sous forme de tableaux :

Nombre	36448.0	
Signe	≥ 0	Sur 1 bit 0
Exposant	$\frac{36448.0}{2^{15}} = 1.1123046875$ $15 + 15 = 30$	Sur 5 bits 11110
Mantisse	$(1.1123046875 - 1) \times 1024$ $= 115$	Sur 10 bits 0001110011
Regroupement sur 16 bits	0111100001110011	
Codes ASCII sur 8 bits	01111000	01110011
Caractères	x	s

Nombre	1392.0	
Signe	≥ 0	Sur 1 bit 0
Exposant	$\frac{1392.0}{2^{10}} = 1.359375$ $10 + 15 = 25$	Sur 5 bits 11001
Mantisse	$(1.359375 - 1) \times 1024$ $= 368$	Sur 10 bits 0101110000
Regroupement sur 16 bits	0110010101110000	
Codes ASCII sur 8 bits	01100101	01110000
Caractères	e	p

Nombre	16896.0	
Signe	≥ 0	Sur 1 bit 0
Exposant	$\frac{16896.0}{2^{14}} = 1.03125$ $14 + 15 = 29$	Sur 5 bits 11101
Mantisse	$(1.03125 - 1) \times 1024$ $= 32$	Sur 10 bits 0000100000
Regroupement sur 16 bits	0111010000100000	
Codes ASCII sur 8 bits	01110100	00100000
Caractères	t	espace

Détails de la solution de la lettre 2 (sphinx)

Voici les positions de la machine pour ce message :

[illegible]

[illegible]

[illegible]

