Nom: Zambon

Prénom: Yanick

Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

Maths spécifiques II — HEIA 2017–2018

Test 1

Cryptologie

mercredi 25 avril 2018

Exercice	1	2	3	4	5	6	Total
Points	4	1.5	3	6.5	3	2	20
Obtenus	4	1,5	2,5	6	1,5	2	17,5

Note
5,4

Consignes et Indications

- Temps à disposition: 90 minutes.
- Matériel autorisé: formulaires et tables, calculatrice et 4 pages A4 recto-verso de résumé.
- Toutes les solutions et les développements sont à écrire sur les feuilles distribuées.
- **Soigner et détailler les résolutions. Des points peuvent être retirés en cas de résolutions mal présentées ou insuffisamment détaillées.**
- ... bon test!

4/4

Exercice 1 (4 pts)

a) Chiffrer le message “On réfléchit” avec la méthode de Vigenère standard et le mot–clé COLOMBIE.

b) Déchiffrer le message “YI KFUWWIZRR” avec la méthode de Vigenère autoclave et le mot–clé PÉROU.

Aidez–vous du carré de Vigenère ci–contre.

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

a) ON REFLECHIT
+ CO LOMBIECOL
→ QB CSRMMGJWE ✓

b) ~~YI KFUWWIZRR~~
~~PEROUNMBTO~~
~~NMBTO~~
Rendu par

YI K F U W W I Z R R
- P E R O U J E T R A N
~~RWSH~~
~~IDS~~
JE TRANSPIRE ✓ (car il fait chaud ou car c'est difficile...)

Exercice 2 (1.5 pts)

1.5/1.5

Voici la sortie donnée par MatLab du calcul de l'indice de coïncidence κ effectué sur un texte chiffré et le même texte décalé de k lettres, pour k entre 1 et 18.

k	$\kappa(X, X_k)$
1	0.0385
2	0.0371
3	0.0404
4	0.0371
5	0.0359
6	0.0379
7	0.0769
8	0.0403
9	0.0331
10	0.0420
11	0.0391
12	0.0374
13	0.0379
14	0.0753
15	0.0391
16	0.0367
17	0.0349
18	0.0378

a) Le texte a été crypté (cochez la(les) bonne(s) case(s)):
- ☐ par une méthode de subtitution monoalphabétique
- ☐ par une méthode de transposition
- ☒ par une méthode de subtitution polyalphabétique
- ☐ impossible de déterminer la méthode de chiffrement avec cette sortie

b) Justifiez votre réponse! * polyalphabétique car les sous-textes n'ont pas tous le même indice ✓

c) Déterminer la longueur probable de la clé utilisée.

longueur de 7 car l'indice se rapproche d'un indice de coïncidence d'une langue.

C'est également le cas pour 14 mais c'est parce que la clé de 7 est répétée:

→ la clé 'OISEAUX' et "OISEAUXOISEAUX" tendront vers un résultat similaire.

Exercice 3 (3 pts)

2.5/3

Dans cet exercice, l'utilisation de la calculatrice sert simplement à faire de petites opérations et/ou à vérifier des calculs. En aucun cas elle ne peut servir à donner directement la solution. Mentionnez toutes les étapes de votre calcul, lequel, hormis 54804, ne doit comporter ***aucun*** *nombre de plus de 4 chiffres!*

Quels sont les trois derniers chiffres de 33^{54804} ?

$1000 = 2^3 \cdot 5^3$

$\rightarrow \varphi(1000) = (2^2 \cdot 1) \cdot (5^2 \cdot 4) = 4 \cdot 100 = 400$ ✓

Pour trouver les 3 derniers chiffres on cherche le modulo 1000 ✓

$33^{54804} \equiv_{1000} x$ ✓

Or $33^{54804} = (33^{400})^{137} \cdot 33^4 \equiv_{1000} x$ ✓

Si pgdc(a,n)=1 inutile!

Par le théorème d'Euclide : $a^{\varphi(n)} \equiv_n 1 \rightarrow 33^{400} \equiv_{1000} 1$ ✓

Donc : $(33^{400})^{137} \cdot 33^4 \equiv_{1000} (33^{400} \bmod 1000)^{137} \cdot (33^4 \bmod 1000)$ ✓

$\equiv_{1000} 1^{137} \cdot (33^4 \bmod 1000)$ ✓

$\equiv_{1000} 33^4 \bmod 1000$

$\equiv_{1000} (33^2 \bmod 1000)^2$

$\equiv_{1000} (1089 \bmod 1000)^2$

$\equiv_{1000} 89^2$

$\equiv_{1000} 7921$

$\equiv_{1000} \underline{921}$ ✓

Exercice 4 (6.5 pts)

6/6.5

Dans cet exercice, l'utilisation de la calculatrice est autorisée pour calculer sauf pour le point b) où elle peut uniquement servir à vérifier.

a) Alain souhaite envoyer le message 10 11 01 01 11 11 chiffré par le cryptosystème de Merkle–Hellman. Il choisit comme clé privée la suite supercroissante $(1, 2, 4, 10, 20, 40)$ et les paramètres $p = 53$ et $m = 120$. Déterminer sa clé publique et le message chiffré.

b) Calculer p^{-1} mod 120 via l'algorithme d'Euclide étendu. Mentionner toutes les étapes.

c) Alain reçoit le message chiffré $(251, 286)$. Déchiffrer ce message à l'aide de sa clé privé.

a) $P_1 = (1 \cdot 53) \bmod 120 = 53$

$P_2 = (2 \cdot 53) \bmod 120 = 106$

$P_3 = (4 \cdot 53) \bmod 120 = 92$

$P_4 = (10 \cdot 53) \bmod 120 = 50$

$P_5 = (20 \cdot 53) \bmod 120 = 100$

$P_6 = (40 \cdot 53) \bmod 120 = 80$

Clé publique : $(53, 106, 92, 50, 100, 80)$ ✓

Chiffrement : 10 11 01 → $53 + 92 + 50 + 80 = 275$ ✓

0 11 11 → $106 + 92 + 50 + 100 + 80 = 427$ -1k

Message chiffré : $(275, 427)$

b) $120 = 1 \cdot 120 + 0 \cdot 53$

$53 = 0 \cdot 120 + 1 \cdot 53$

$14 = 1 \cdot 120 - 2 \cdot 53$

$11 = 1 \cdot 53 - 3 \cdot 14$

$3 = 1 \cdot 14 - 1 \cdot 11$

$2 = 1 \cdot 11 - 3 \cdot 3$

$1 = 1 \cdot 3 - 1 \cdot 2 = (1 \cdot 14 - 1 \cdot 11) - (1 \cdot 11 - 3 \cdot 3)$

$= (1 \cdot 120 - 2 \cdot 53 - 1 \cdot 53 + 3 \cdot 14) - (1 \cdot 53 - 3 \cdot 14) - 3 \cdot 14 + 3 \cdot 11)$

$= (1 \cdot 120 - 3 \cdot 53 + 3 \cdot 120 - 6 \cdot 53) - (1 \cdot 53 - 6 \cdot 120 + 12 \cdot 53 + 3 \cdot 53 - 9 \cdot 14)$

$= (4 \cdot 120 - 9 \cdot 53) - (16 \cdot 53 - 6 \cdot 120 - 9 \cdot 120 + 18 \cdot 53)$

$= 4 \cdot 120 - 9 \cdot 53 - 34 \cdot 53 + 15 \cdot 120$

$= 19 \cdot 120 - 43 \cdot 53 = 1$ ✓

$-43 \equiv_{120} 77 = 53^{-1} \bmod 120$

c) $251 \rightarrow 251 : 77 \equiv_{120} 7 = 1+2+4 \rightarrow$ "11 10 00"

$286 \rightarrow 286 : 77 \equiv_{120} 62 = 40+20+2 \rightarrow$ "01 00 11"

Exercice 5 (3 pts)

1.5/3

Dans cet exercice, tous les calculs peuvent se faire avec la calculatrice. Veillez cependant à mentionner toutes les étapes de calcul.

a) Achim se crée un code RSA avec les nombres premiers $p = 89$ et $q = 41$, ainsi que l'exposant $e = 101$. Déterminer quelles sont les clés publique resp. privé de Achim.

b) Blanche envoie le message suivant à Achim (chiffré avec sa clé publique): "2585 3244 3359 1662". Déchiffrez ce message (A=1, B=2, ...) via la clé privée d'Achim et donnez votre réponse sous la forme d'un texte/mot.

a) $p = 89$ $q = 41$ $n = p \cdot q = 3649$ ✓

$\varphi(n) = 88 \cdot 40 = 3520$ $e = 101$ ✓

$\text{pgcd}(\varphi(n), e) = 1$

$e \cdot d \equiv_{\varphi(n)} 1$

→ $3520 = 1 \cdot 3520 + 0 \cdot 101$

$101 = 0 \cdot 3520 + 1 \cdot 101$

$86 = 1 \cdot 3520 - 34 \cdot 101$

$15 = 1 \cdot 101 - 1 \cdot 86$

$11 = 1 \cdot 86 - 5 \cdot 15$

$4 = 1 \cdot 15 - 1 \cdot 11$

$3 = 1 \cdot 11 - 2 \cdot 4$

$1 = 1 \cdot 4 - 1 \cdot 3 = 1 \cdot 15 - 1 \cdot 11 - 1 \cdot 11 + 2 \cdot 4$

$= 1 \cdot 101 - 1 \cdot 86 - 2 \cdot 86 + 10 \cdot 15 + 2 \cdot 15 - 2 \cdot 11$

$= 1 \cdot 101 - 3 \cdot 3520 + 102 \cdot 101 + 12 \cdot 101 - 12 \cdot 86 - 2 \cdot 86 + 10 \cdot 15$

$= 115 \cdot 101 - 3 \cdot 3520 - 14 \cdot 3520 + 476 \cdot 101 + 10 \cdot 101 - 10 \cdot 86$

$= -17 \cdot 3520 + 601 \cdot 101 - 10 \cdot 3520 + 340 \cdot 101$

$= -27 \cdot 3520 + 941 \cdot 101 = 1$

$d = 941$ ✓

1

Clé privée $(p, q, d) = (89, 41, 941)$ ✓ Clé publique $(3649, 101) = (n, e)$

b)

2585 :

$m \equiv_{3649} 2585^{941}$

méthode des facteurs de 2 car module est inconnu à ma calculatrice :

$2585^2 \equiv_{3649} 906$ ✓

$2585^4 \equiv_{3649} 906^2 \equiv_{3649} 3460$ ✓

~~$2585^8 \equiv_{3649} 936^2 \equiv_{3649} 336$~~

$2585^8 \equiv_{3649} 3460^2 \equiv_{3649} 2880$ ✓

$2585^{16} \equiv_{3649} 2880^2 \equiv_{3649} 223$ ✓

$2585^{32} \equiv_{3649} 223^2 \equiv_{3649} 2292$ ✓

$2585^{64} \equiv_{3649} 2292^2 \equiv_{3649} 2353$ ✓

$\equiv^{128} \equiv_n 2352^2 \equiv_n$ ~~20~~

$\equiv^{256} \equiv_n 400$

$\equiv^{512} \equiv_n 400^2 \equiv_n 3093$ ...

idée de

$941 = 512 + 256 + 128 + 32 + 8 + 4 + 1$

→ $2585^{941} \equiv_n 3093 \cdot 400 \cdot 20 \cdot 2292 \cdot 2880 \cdot 3460 \cdot 2585$

$\equiv_n 189 \cdot 2052 \cdot 3030 \cdot 2585$

$\equiv_n 1034 \cdot 1796$

$\equiv_n 3372$ ← ~~il y a une erreur de calcul qui traîne à quelque part~~

1h

3244 :

$3244^2 \equiv_n 3469$

$\equiv^4 \equiv_n 3208$

$\equiv^8 \equiv_n 1084$

$\equiv^{16} \equiv_n 78$

$\equiv^{32} \equiv_n 2435$

$\equiv^{64} \equiv_n 3249$

$\equiv^{128} \equiv_n 3093$

$\equiv^{256} \equiv_n 2620$

$\equiv^{512} = 631$ ✓

idem

→ $3244^{941} \equiv_n 631 \cdot 2620 \cdot 3093 \cdot 2435 \cdot 1084 \cdot 3208 \cdot 3241$

$\equiv_n 223 \cdot 3568 \cdot 3624 \cdot 3241$

$\equiv_n 182 \cdot 2902$

$\equiv_n 2708$ ← ~~Je~~ J'imagine que j'ai encore échoué ~~et que~~ ou que mon J est faux.

Exercice 6 (2 pts)

2/2

~~Crypter~~ Chiffrer le message "Le plastique est partout" par la méthode de l'alphabet désordonné avec le mot–clé JE SUIS TON PROF.

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

Le plastique est partout

→ ~~AI GAJKLPHQI IKL GJ~~

→ AI GAJLMPHQI ILM GJKMOQM ✓