Congruences - 2 : Cryptographie, etc.

NOM et PRENOM : ..... *Il faut tout justifier et expliquer !*

1. Un message a été chiffré avec la matrice de Hill

$$\begin{pmatrix} 1 & 2 & 0 \\ 3 & 1 & 4 \\ 5 & 3 & 5 \end{pmatrix}$$

Le destinataire a reçu : **VWF** . Déchiffrez ce message.

2. Pour chacune des paires suivantes, dites si elle correspond à une clé publique RSA. Justifiez !

a. $(E, n) = (31, 527)$ b. $(E, n) = (9; 1083)$.

3. Amélie possède la clé publique $(E_A, n_A) = (35, 221)$. Ben possède la clé publique $(E_B, n_B) = (5, 323)$.

Partie A – Amélie veut envoyer le message **W3** à Ben.

a. Pourquoi ne peut-elle pas signer-chiffrer directement la paire de caractères ?

b. Amélie **signe-chiffre** ce message caractère par caractère ; quels seront les deux blocs envoyés ?

Partie B – Amélie a envoyé un caractère **chiffré** à Ben qui a reçu le bloc **2** . Quel était le caractère en clair ?

FORMULAIRE

Table alpha-numérique.

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

Vigenère $y_i = x_i + k_{i(mod\, r)}\, (mod\, m)$

Inverses modulo 26

a	:	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	:	1	9	21	15	3	19	7	23	11	5	17	25

RSA $C = P^E \bmod n \quad , \quad D = E^{-1} \bmod \phi(n)$

a	b	c	d	e	f	g	h	i	j	k	l	m
00	01	02	03	04	05	06	07	08	09	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

A	B	C	D	E	F	G	H	I	J	K	L	M
26	27	28	29	30	31	32	33	34	35	36	37	38

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
39	40	41	42	43	44	45	46	47	48	49	50	51

0	1	2	3	4	5	6	7	8	9		.	,
52	53	54	55	56	57	58	59	60	61	62	63	64

;	?	-	...
65	66	67	...