Chapitre Cryptographie :

prenons a = 100
a = 2 x 50
a = 4 x 25
a = 5 x 20
a = 10 x 10

Exercice 1 :
Nombre premier : nombre qui possède seulement 2 diviseurs : 1 et lui-même
25 = 5x5 : pas premier
345 = 5x69 pas premier

659 :
$\sqrt{659} \simeq 25{,}6$
Nombres premiers inférieurs à 25 : 2, 3, 5, 7, 11, 13, 17, 19, 23
659 n'est divisible par aucun nombre premier inférieur à sa racine : c'est un nombre premier.

1023 = 3 x 341 : pas premier

Exercice 2 :
A = 1080
A = 2 x 540
A = 2 x 2 x 270
A = 2 x 2 x 2 x 135
A = 2 x 2 x 2 x 3 x 45
A = 2 x 2 x 2 x 3 x 3 x 15
A = 2 x 2 x 2 x 3 x 3 x 3 x 5
$A = 2^3 \times 3^3 \times 5$

B = 63 x 37
$B = 3^2 \times 7 \times 37$

36 = 2 x 18 = 2 x 2 x 9 = 2 x 2 x 3 x 3 = $2^2 \times 3^2$
38 = 2 x 19
$C = (2^2 \times 3^2)^2 \times (2 \times 19)^2$
$C = 2^4 \times 3^4 \times 2^2 \times 19^2$
$C = 2^6 \times 3^4 \times 19^2$

$(x^a)^b = x^{ab}$
$x^a \times x^b = x^{a+b}$

$D = (2 \times 3^2 \times 17)^2 \times (25 \times 24)^5$
$25 = 5^2$
$24 = 2^3 \times 3$
$D = (2 \times 3^2 \times 17)^2 \times (5^2 \times 2^3 \times 3)^5$
$D = (2^2 \times 3^4 \times 17^2) \times (5^{10} \times 2^{15} \times 3^5)$
$D = 2^2 \times 3^4 \times 17^2 \times 5^{10} \times 2^{15} \times 3^5$
$D = 2^{17} \times 3^9 \times 5^{10} \times 17^2$

$x = 2^4 \times 3^5 \times 5 \times 7^2 \times 11$
$x = y \times q\,?$

$x = 2^3 \times 2 \times 3^2 \times 3^3 \times 7 \times 7 \times 11$
$x = (2^3 \times 3^2 \times 7 \times 11) \times 2 \times 3^3 \times 7$
$x = y \times 2 \times 3^3 \times 7$
Donc x est divisible par y
et $q = 2 \times 3^3 \times 7$

BrainStorming : diviseurs de 4116 ?
2, 3, 7,
4, 6, 12, 14, 21, 28, 49

Combien de diviseurs : (3+1)x(2+1)x(1+1) = 4x3x2 = 24

Algorithme d'Euclide :
1636 = 1128 x 1 + 508
1128 = 508 x 2 + 112
508 = 112 x 4 + 60
112 = 60 x 1 + 52
60 = 52 x 1 + 8
52 = 8 x 6 + 4
8 = 4 x 2 + 0

Exercice 3 :
$246 = 2 \times 3 \times 41$
il y a (1+1) x (1+1) x (1+1) = 8 diviseurs
Diviseurs de 246 : {1.2.3.6, 41, 82,123, 246}
$348 = 2^2 \times 3 \times 29$
il y a (2+1)x(1+1)x(1+1) = 12 diviseurs
Diviseurs 348 : {1.2.3.4.6,12,29,58,87,116,174, 348}
Car 6 est le dernier nombre pour les deux chiffres qui quand on divise le nombre on obtient un chiffre sans virgules.
PGCD (246,348) = 6

Exercice 4 :
825 :
825 = 3*275
275 = 5*55
55 = 5*11
11 = 11*1
$825 = 3 \times 5^2 \times 11$

168 :
168 = 3*56
56 = 7*8
$168 = 3 \times 7 \times 8$
Leurs PGCD commun est 3

Exercice 5 :
Emploi de l'algorithme d'Euclide:
Soustraire les deux nombres qu'on cherche et réutiliser le plus petit nombre et le reste.
PGCD(712 ,128) ?
712-128=584->reste
584-128=456

456-128=328
328-128=200

200-128=72
128-72=56
72-56=16
56-16=40
40-16=24

24-16=8
16-8=8
8-8=0

dividende	diviseur	quotient	0 <= reste < diviseur
712	128	5	72
128	72	1	56
72	56	1	16
56	16	3	8
16	8	2	0

Leurs PGCD commun est 8.

Nombre premier : **un** nombre qui a seulement deux diviseurs : 1 et lui-même
Nombres premiers entre eux : **deux** nombres dont le PGCD vaut 1
Ces deux définitions n'ont rien à voir !

Soient deux nombres premiers différents :
Ex : 13 et 29 :
13 = 13 x 1
29 = 29 x 1
donc PGCD(13,29) = 1 => 13 et 29 sont premiers entre eux !
deux nombres sont premiers => les deux sont premiers entre eux

A-t-on la réciproque ?
Prenons deux nombres premiers entre eux :
36 et 25 :
$36 = 6^2$
$25 = 5^2$
PGCD(25,36) = 1, mais 25 et 36 ne sont pas premiers ni l'un ni l'autre !
La réciproque est donc fausse :
Si deux nombres sont premiers entre eux, cela ne veut pas forcément dire qu'ils sont premiers.

Exercice 6 :
PGCD(4,9) = 1 premiers entre eux
4 = 2^2
9 = 3^2

$44 = 2^2 \times 11$
$32 = 2^5$
PGCD(44, 32) = 4 => pas premiers entre eux

30 et 25 :
$30 = 5 \times 6 = 5 \times 2 \times 3$
$25 = 5^2$
PGCD(30, 25) = 5 => 30 et 25 ne sont pas premiers entre eux

23 et 36 :
23 est premier : 23 = 23 x 1
$36 = 6^2 = 2^2 \times 3^2$
PGCD(23,36) = 1 => 23 et 36 sont premiers entre eux

Exemple :
PGCD(345, 425) = PCGD(5x69, 5x85) = 5 x PGCD(69, 85)

PGCD(30, 25) = 5 = d
30 = d x 6
25 = d x 5
et PGCD(6,5) = 1

Exercice 7 :
PGCD(30,36) = PGCD(5x6, 6x6)
= 6 x PGCD(5,6)
= 6 x 1
= 6

Congruences :
prenons a = 26, b = 15 et n = 11
$26 = 2 \times 11 + 4$
$15 = 1 \times 11 + 4$
26 et 15 ont le même reste (4) dans la division par 11 => 26 et 15 sont congrus modulo 11 :
$26 \equiv 15 \quad [11]$
$26 \equiv 4 \quad [11]$
$26 \equiv -7 \quad [11]$

11h 23h
$23 = 1 \times 12 + 11$
$23 \equiv 11 \quad [12]$

vendredi 30, 23, 16, 9, 2
$30 = 4 \times 7 + 2$
$23 = 3 \times 7 + 2$
$30 \equiv 23 \quad [7]$
ces nombres sont congrus modulo 7
$30 \equiv 16 \quad [7] \Leftrightarrow 30 - 16 = 14 = 2 \times 7$

Simplifier la congruence : réduire la congruence au reste :
$30 \equiv 2 \quad [7]$

message à chiffrer : ASTERIX à chiffrer avec clé = 3
DVWHULA

message à déchiffrer : VOQKEVYSC avec clé = 10
LEGAULOIS

On a pour le chiffre de César 25 clés possibles (on ne compte la clé = 0)

Chiffre affine :
T : x = 19
On chiffre avec la clé (a, b) = (7, 12)
$y \equiv ax + b \quad [26]$
$y \equiv 7 \times 19 + 12 \quad [26]$
$y \equiv 145 \quad [26]$
$145 = 5 \times 26 + 15$
$y \equiv 15 \quad [26]$ et $0 \leq 15 < 26$
y = 15 correspond à la lettre P
T est chiffrée en P

Chiffrons le message : OK avec la clé (7,12)

'O' : x=14
$y \equiv 7 \times 14 + 12 \quad [26]$
$y \equiv 110 \quad [26]$
Division de 110 par 26 :
$110 = 26 \times 4 + 6$
$y \equiv 6 \quad [26]$ avec $0 \leq 6 < 26$
lettre chiffrée : G

K : x = 10
$y \equiv 7 \times 10 + 12 \quad [26]$
$y \equiv 82 \quad [26]$
Division de 82 par 26 :
$82 = 26 \times 3 + 4$
$y \equiv 4 \quad [26]$ avec $0 \leq 4 < 26$
lettre chiffrée : E

« OK » est chiffré en « GE »

Il faut déchiffrer ONOO. La clé de chiffrement est (7,12)
$y \equiv ax + b \quad [26]$
ça ressemble à une équation du type $y = ax + b$
On veut déchiffrer, donc trouver x à partir de y :
$ax = y - b$

$x = \frac{1}{a}(x - b)$ (on multiplie par l'inverse de a pour trouver x)
En travaillant sur les entiers, nous n'avons pas le droit de diviser
Il faudrait trouver l'équivalent de 1/a, autrement dit, l'inverse de a, mais modulo 26
l'inverse de a, c'est le nombre qui multiplié à a donne 1 :

$$a \times \frac{1}{a} = 1$$

il faudrait trouver un nombre c tel que :

$$a \cdot c \equiv 1 \quad [26]$$

c	ac	ac [26]	
1	7	7	
2	14	14	
3	21	21	
4	28	2	
5	35	9	
6	42	16	
7	49	23	
8	56	4	
9	63	11	
10	70	18	
11	77	25	
12	84	6	
13	91	13	
14	98	20	
15	105	1	
16	112	8	
17	119	15	
18	126	22	
19	133	3	
20	140	10	
21	147	17	
22	154	24	
23	161	5	
24	168	12	

$15 \times 7 = 105 \equiv 1 \quad [26]$
105 = 26*4 + 1

l'inverse de 7 modulo 26 est 15 : c = 15

Le chiffrement était :
$y \equiv 7x + 12 \quad [26]$
Pour déchiffrer, il faut trouver x en fonction de y:
$7x \equiv y - 12 \quad [26]$
$15 \times 7x \equiv 15 \times (y - 12) \quad [26]$
Or $15 \times 7 \equiv 1 \quad [26]$
Donc :
$x \equiv 15 \times (y - 12) \quad [26]$
$x \equiv 15y - 15 \times 12 \quad [26]$
$x \equiv 15y - 180 \quad [26]$
$180 = 26 \times 6 + 24$
$x \equiv 15y - 24 \quad [26]$
$x \equiv 15y - 24 + 26 \quad [26]$
$x \equiv 15y + 2 \quad [26]$
La clé de déchiffrement est donc (15,2). Elle est différente de la clé de chiffrement

Déchiffrer le message ONOO qui a été chiffré avec la clé (7,12).
O : y=14
$x \equiv 15 \times 14 + 2 \quad [26]$
$x \equiv 212 \quad [26]$
362 = 26 x 8 + 4
$x \equiv 4 \quad [26]$
lettre déchiffrée : E
ONOO => EPEE

Analyse détaillée :
1. message : ASTERIX
clé (a, b) = (0, 17)
$y \equiv 0 \cdot x + 17 \quad [26]$
A : 0 => $y \equiv 17 \quad [26]$ => R
S : 18 => $y = 0 \cdot 18 + 17 \equiv 17 \quad [26]$ => R
T : 19 => $y = 0 \cdot 19 + 17 \equiv 17 \quad [26]$ => R
…
message chiffré : RRRRRRR... indéchiffrable !

2. message : ASTERIX
clé (a, b) = (13, 6)
$y \equiv 13 \cdot x + 6 \quad [26]$
A : 0 => $y = 13 \times 0 + 6 \equiv 6 \quad [26]$ => G
S : 18 => $y = 13 \times 18 + 6 = 240 \equiv 6 \quad [26]$ => G
car $240 = 9 \times 26 + 6$

T : 19 => $y = 13 \times 19 + 6 = 253 \equiv 19 \quad [26]$ => T
car $253 = 9 \times 26 + 19$

E : 4 => $y = 13 \times 4 + 6 = 58 \equiv 6 \quad [26]$ => G
…

il va aussi y avoir un problème pour déchiffrer : au moins 3 lettres se codent par G.

x	13x+6	13x+6 [26]
0	6	6
1	19	19
2	32	6
3	45	19
4		6
5		19

Le problème est que 13 n'est pas premier avec 26 !

Liste des nombres a premiers avec 26 <=> PGCD(a, 26) = 1.
$26 = 2 \times 13$

1 3 5 7 9 11 15 17 19 21 23 25

nombre de clés donnant un codage acceptable : 12*26 = 312
12 possibilités pour a
26 possibilités pour a
311 en enlevant la clé (1,0)

Chiffre de vigenère :
Texte : ASTERIX
clé : IDEFIX
chiffré : IVXJ…

Echange de clés Diffie-Hellman
Alice et Bob choisissent des nombres communs (peinture en commun):
p = 13
g = 5

Peintures secrètes :
Alice choisit a = 2
Bob choisit b = 3

Mélange :
Alice calcule $A \equiv 5^2 \quad [13]$
$A \equiv 25 \quad [13]$
$A \equiv 12 \quad [13]$

Bob calcule $B \equiv 5^3 \quad [13]$
$B \equiv 125 \quad [13]$
$125 = 4 \times 13 + 8$
$B \equiv 8 \quad [13]$

Alice reçoit B = 8 et calcule :
$K \equiv 8^2 \quad [13]$
$K \equiv 64 \quad [13]$
$64 = 4 \times 13 + 12$
$K \equiv 12 \quad [13]$

Bob reçoit A = 12 et calcule :
$K \equiv 12^3 \quad [13]$
$K \equiv 1728 \quad [13]$
$1728 = 132 \times 13 + 12$
$K \equiv 12 \quad [13]$

Exercice 8 :
$A \equiv 14^3 \quad [2741]$
$A \equiv 2744 \quad [2741]$
$A \equiv 3 \quad [2741]$

$B \equiv 14^{12} \quad [2741]$
$B \equiv 56693912375296 \quad [2741]$
56693912375296 = 2741 * 20683660115 + 81
$B \equiv 81 \quad [2741]$

$K \equiv 81^3 \quad [2741]$
531441 = 2741 * 193 + 2428
$K \equiv 2428 \quad [2741]$