TD 2 Cryptographie

Introduction

Théorème de Bachet-Bézout (ou Identité de Bézout) — Soient a et b deux entiers relatifs. Si d est le PGCD de a et b, alors il existe deux entiers relatifs x et y tels que ax + by = d.

Théorème de Bézout — Deux entiers relatifs a et b sont premiers entre eux (si et) seulement s'il existe deux entiers relatifs x et y tels que ax + by = 1.

- ⇨ Tout n peut s’écrire sous la forme n = ax + by
- ⇨ Si a et b nom premier entre eux ce n’est pas possible
    - o exemple a = 15, b = 6 comment faire 3 ?
    - o 15 = 3n, 6 = 3m ➔ 15a+6b = 3na+3mb = multiple de 3

Méthode d’Euclide pour le calcul du PGCD de a et b

```
a = k1*b + r1
      b = k2*r1 + r2
            r1 = k2*r2 + r3
                  r2 = k3*r3 + r4
                    … jusqu’à rn = 0 le PGCD est r(n-1)
                    Si r(n-1) = 1 alors a et b premier
entre eux
```

2 Echauffement 2.1 Bachet-Bézout

Le maire de Gotham City souhaite changer de monnaie et réimprimer tous les billets de la ville pour simplifier les transactions. Il souhaiterait savoir s'il est judicieux (ou non) de n'utiliser des billets que de deux valeurs différentes. Il aimerait notamment savoir si les habitants seraient toujours capables d'acheter tous types de produits. Pour chaque proposition du maire, expliquez si oui ou non, les valeurs des billets permettent aux habitants d'acheter des produits de n'importe quelles valeurs :

- 7 et 19
- 29 et 38
- 111 et 53

Solution

C'est possible si les nombres sont premiers entre-eux

- **7 et 19**

```
19 = 2*7 + 5                k1=2, r1=5
    7 = 1*5 + 2             k2=1, r2=2
        5 = 2*2 + 1         k3=2, r3=1
            2 = 2*1 + 0     k4=2, r4=0
                            ➔ r = 1 (r3)
                            ⇨ 19 et 7 premier entre eux
```

- **29 et 38**

```
38 = 1*29 + 9                   k1=1, r1=9
    29 = 3*9 + 8            k2=3, r2=8
        9 = 1*8 + 1         k3=1, r3=1
            8 = 8*1 + 0     k4=8, r4=0
                            ➔ r = 1 (r3)
                            ⇨ 38 et 29 premier entre eux
```

- **111 et 53**

```
111 = 2*53 + 5                      k1=2,  r1=5
    53 = 10*5 + 3                   k2=10, r2=3
        5 = 1*3 + 2             k3=1,  r3=2
             3 = 1*2 + 1        k4=1,  r4=1
                  2 = 2*1 + 0       k5=2,  r5=0
                            ➔ r = 1 (r4)
                            ⇨ 111 et 53 premier entre eux
```

2.2 Calcul d'inverses Algorithme d'Euclide étendu

Le maire de Gotham vous remercie pour vos conseils. Il souhaite maintenant que vous calculiez les inverses de nombres sur des ensembles Z/nZ. Sans raison particulière, il trouve , ca rigolo.

- calculez l'inverse de 5 sur Z/26Z.

• calculez l'inverse de 17 sur Z/46Z.
• calculez l'inverse de 47 sur Z/51Z.

Solution

• calculez l'inverse de 5 sur Z/26Z.

On cherche a tel que : 5*a $\equiv 1[26]$

• 26 et 5

```
26 = 5*5 + 1                k1=5, r1=1
     5 = 5*1 + 0            k2=1, r2=0
                            ⇨ 26 et 5 premier entre eux
```

1 = 1*26 - 5*5 ➔ (-5)*5 $\equiv 1[26]$ ➔ 21*5 $\equiv 1[26]$ **(-5+26=21)**

➔ **a = 21 ou -5**

• calculez l'inverse de 17 sur Z/46Z.

• 46 et 17

```
46 = 2*17 + 12                  k1=2, r1=12
     17 = 1*12 + 5              k2=1, r2=5
          12 = 2*5 + 2      k3=2, r3=2
               5 = 2*2 + 1  k4=2, r4=1
                            ➔ r = 1 (r4)
                            ⇨ 46 et 17 premier entre eux
1 = 5 - 2*2
    = 5 - 2*(12 - 2*5)
    = (17 - 12) - 2*(12 - 2*(17 - 12))
    = (17 - (46 - 2*17)) - 2*((46 - 2*17) - 2*(17 - (46 -
2*17)))
    = (17 - 46 + 2*17) - 2*(46 - 2*17 - 2*(17 - 46 + 2*17))
    = 17 - 46 + 2*17 - 2*(46 - 2*17 - 2*17 + 2*46 - 4*17)
    = 17 - 46 + 2*17 - 2*46 + 4*17 + 4*17 - 4*46 + 8*17
  1 = (1+2+4+4+8)*17 –(1+2+4)*46 = 19*17 – 7*46 = (323-322)
```

➔ (19)*17 $\equiv 1[46]$

➔ **a = 19**

• calculez l'inverse de 47 sur Z/51Z.

```
51 = 1*47 + 4                   k1=1,  r1=7
     47 = 11*4 + 3              k2=11, r2=3
          4 = 1*3 + 1       k3=1,  r3=1
                            ➔ r = 1 (r3)
                            ⇨ 51 et 47 premier entre eux

1 = 4 - 1*3
    = 4 - 1*(47 - 11*4)
    = (51 - 47) - (47 - 11*(51 - 47))
1 = 51 -47 -47 + 11*51 -11*47 = 12*51 – 13*47 = (612-611)
```

➔ (13)*47 $\equiv 1[51]$

➔ **a = 13**

2.3 Exponentiations modulaires

L’adjoint au maire aime également beaucoup l’arithmétique modulaire, il vous demande de calculer (de tête) les exponentiations modulaires suivantes:

- $x \equiv 10^5 \pmod{85}$
- $x \equiv 4^8 \pmod{26}$
- $x \equiv 12^5 \pmod{122}$

Solution

- **$x \equiv 10^5$ (mod 85)**

$10^5 = 10*(85+15)^2 \equiv 10*(15)^2$ **(mod 85)**$\equiv 10*(2*85+55)$ **(mod 85)**

$\equiv 10*55$**(mod 85)** $\equiv 550$ **(mod 85)**$\equiv 6*85+40$ **(mod 85)**)

➔ **$x \equiv 40$ (mod 85)**

- **$x \equiv 4^8$ (mod 26)**

$4^8 = 16*64*64 = (26-10)*(2*26+12)*(2*26+12) = 26k - 10*12*12 = 26k – (5*26-10)*12 = 26n + 120 = 26m - 10$

$x \equiv 4^8 \pmod{26}$ ➔ $x \equiv -10 \pmod{26}$ ➔ **$x \equiv 16$ (mod 26)**

- **$x \equiv 12^5$ (mod 122)**

$12^5 = 12*144*144 = 12*(122+22)*(122+22) = 122n + 12*22*22 = 122n + (2*122+20)*22 = 122m + 20*22$

$x \equiv 12^5 \pmod{122}$ ➔ $x \equiv 440 \pmod{122}$

➔ $x \equiv (3*122+74) \pmod{122}$ ➔ **$x \equiv 74$ (mod 122)**

3 Chiffrement RSA
Batman et Robin souhaitent communiquer discrètement pour que leurs messages ne soient ni lus ni modifies par le Joker. Pour cela, ils décident d'utiliser le bat-ordinateur pour développer un bat-programme utilisant RSA pour chiffrer et déchiffrer des messages. Malheureusement, Batman et Robin n'ont pas eu le temps de se former à la cryptographie. Ils vous demandent de leur donner un exemple du fonctionnement de RSA en chiffrant et déchiffrant le message suivant : LES CAROTTES SONT CUITES.
Pour chiffrer ce message, vous devez d'abord l'encoder sous forme de chiffres en associant chaque lettre à un nombre (A=1, B=2, C=3, etc.).
Puis chaque nombre doit être chiffré puis déchiffre avec RSA de maniéré individuelle.
Les paramètres à sélectionner pour chiffrer et déchiffrer le message sont :
• clef publique : p = 5, q = 17
• exposant : e = 5

RSA

Théorème. Soient p et q deux nombres premiers, et posons n = p × q.
Soit e est un entier premier avec (p – 1) × (q – 1), alors il existe un entier d > 0 et un entier m tels que e × d + m × (p – 1)(q – 1) = 1.
C'est-à-dire e × d = 1 (mod (p – 1)(q – 1))
Notons au passage que si on choisit d positif et inférieur à (p – 1)(q – 1), alors d est unique.
Aussi :
Pour tout entier a < n premier avec n, le reste de la division de $a^{e \times d}$ par n est égal à a.
Voir :
[Nombres premiers et cryptologie : l'algorithme RSA - Interstices](https://interstices.info/nombres-premiers-et-cryptologie-lalgorithme-rsa/)
https://interstices.info/nombres-premiers-et-cryptologie-lalgorithme-rsa/

On choisit 2 nombres premiers entre eux grands n et p
— Calculer : n = p×q
— Calculer l'indicatrice d'Euler : ϕ(n) = (p-1)*(q-1)
— Sélectionner un entier : e ∊ N premier avec ϕ(n)
— Calculer l'inverse modulaire (via l'algorithme d'Euclide étendu)
: d ∊ N tel que : d * e ≡ 1 mod 𝜑(n)
(n,e) est appelée la clé publique
d est la clé privée.

Exemple p = 1009, q =1013, n = 1022117
ϕ(n)=1020096 = (p-1)*(q-1)
e = 101 (on peut vérifier que ϕ(n) et e sont premier entre eux)
[excel 1=PGCD(101;1020096)]
➔ d = 767597 (d * e ≡ 1 mod 𝜑(n)) [excel 1=MOD(767597*101;1020096)}

M = messagge
Message codé = C ≡ M^e (mod n)

Décodage : M ≡ C^d (mod n)

Note $C^d = M^{ed}$

RSA-100 =
1522605027922533360535618378132637429718068114961380688657908494580122963258952897654000350692006139

RSA-100 a été factorisé en avril 1991 :

RSA-100 =
37975227936943673922808872755445627854565536638199

× 40094690950920881030683735292761468389214899724061

e= 65537

Solution
p= 5 q = 17 ➔ n = pq= 85
φ(n) = (p - 1) * (q - 1) = 4*16=64
e = 5
Calcul de la clé privée d tel que : d * e ≡ 1 mod φ(n) = 64
➔Calcul de l'inverse de 5 Mod (64)

• calculez l'inverse de 5 sur Z/64Z.

```
64 = 12*5 + 4                  k1=5,  r1=4
     5 = 1*4 + 1            k2=1, r2=1
                            ➔ r = 1 (r2)
                            ⇨ 64 et 5 premier entre eux
```

```
1 = 5 - 1*4
 = 5 - 1*(64 - 12*5)
 = 5 + 12*5 - 64
```

1 = 13*5 – 64 = (65-64)
➔ (13)*5 $\equiv 1[64]$
➔ **d = 13**

Le message chiffré est $c \equiv m^e (\text{mod } n)$:
Le message déchiffré $m \equiv c^d (\text{mod } n)$
n = 85, e = 5, d = 13

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	26

' ' = 27, '.' = 28
LES CAROTTES SONT CUITES

➔ 12-5-19-27-3-1-18-15-20-20-5-19-27-19-15-14-20-27-3-21-9-5-19-28

On ne peut pas avoir des nombres supérieurs à 64, donc on chiffre caractère par caractère

Ce qui n'est pas optimale car on ne casse pas la fréquence des caractères.

Le message chiffré est $c \equiv m^e (\text{mod } n)$:
12^5 mod (85) = (12*144*144) mod (85) = (12*(85+59)*(85+59) mod (85)

=k*85+(12*59*59) mod (85)

=37 mod (85) ➔ c = 27

Le message déchiffré $m \equiv c^d (\text{mod } n)$
37^{13} mod (85) = 37*(37*37)^6 mod (85) =37*(9)^6 mod (85) =12

37*37 mod (85) = 9
Via excel :

n	**85**			

			n,e = clé publique	
e	**5**			
d	**13**		d= clé privée	
m	c=MOD(m^e ;n)	c*c	c2=mod(c;n)	mMOD(c*c2^6;n)
12	37	1369	9	12
5	65	4225	60	5
19	49	2401	21	19
27	57	3249	19	27
3	73	5329	59	3
1	1	1	1	1
18	18	324	69	18
15	70	4900	55	15
20	5	25	25	20
20	5	25	25	20
5	65	4225	60	5
19	49	2401	21	19
27	57	3249	19	27
19	49	2401	21	19
15	70	4900	55	15
14	29	841	76	14
20	5	25	25	20
27	57	3249	19	27
3	73	5329	59	3
21	21	441	16	21
9	59	3481	81	9
5	65	4225	60	5
19	49	2401	21	19
28	78	6084	49	28

4 Automatisation

Batman et Robin sont surpris de voir à quel point il est long et fastidieux de chiffrer un message avec RSA. Ils souhaitent que vous leur proposiez un pseudocode permettant d'automatiser ce processus.

Proposez 3 fonctions en pseudo-code pour les tâches suivantes :

Conversion message texte M ➔ binaire = MB

Encodage MB (n,e) = CB

Décodage CB (n,d) = MB

Conversion message binaire MB➔ texte = M

Calcul clé privée (p,q,e) = d

Algo inverse (e,phi) avec Euclide

Exemple

Suppose we pick the primes p=3457631 and q=4563413. (In practice we might pick integers 100 or more digits each, numbers which are strong probable primes for several bases.) Suppose we also choose the exponent e=1231239 and calculate d so e d \equic 1 (mod φ(n)). We now publish the key (n, e) = (15778598254603, 1231239).

To encrypt the message "George has green hair" we convert it to an integer. One simple idea (too simple for real use) is to let A be 1, B be 2, ... Then our message is

0705151807052 7080119270718 0505142718010 918.

For each of the four blocks (whose length was chosen so the blocks would represent integers no larger than n) we compute B^e (mod n) (using the binary exponentiation). This gives the encrypted message:

1658228449402 5333403068473 7979527536648 13889903320423.

This message can be decrypted by raising each block to the d = 1315443185039th power modulo n

p=3457631 and q=4563413

(n, e) = (15778598254603, 1231239).

d = 1315443185039