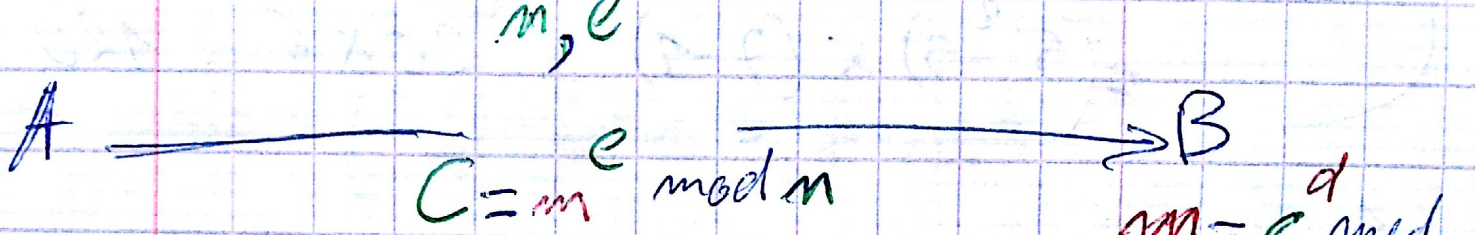
Examen Crypto 2014/2015

PI

Q1:

1- RSA



85 - 86 / 99 copier/coller

2 - 86/99 → cas d'El Gamal

25/99 → réduction

Question 2

PII

Question 3:

1- $n = 5^2 \times 7 = 175$

$\varphi(n) = \varphi(5^2) \times \varphi(7)$

$= (5^2 - 5) \times (7-1) = 20 \times 6 = 120$

2-

Hypothèse d'exposant de signature :

Il existe un inverse pour cet exposant d $\bmod \varphi(n)$

- $d = 12$ il faut que $\text{pgcd}(12, \varphi(120)) = 1 \bmod \varphi(7)$

r_i	120	31	27	4	3	1	0
q_i	/	3	1	6	1	3	
x_i	1	0	1	-1	7	-8	
y_i	0	1	-3	4	-27	31	

$120 \times (-8) + 31 \times 31 = 1$

$x_k = x_{k-2} - q_{k-1} \cdot x_{k-1}$

$y_k = y_{k-2} - q_{k-1} \cdot y_{k-1}$

$31^{-1} \bmod 120$ pgcd $(120, 31)$

3

$$123 \cdot 3 + 23(-16) = 1$$

$$23(-16) = 1 + k\,123$$

$$23(-16) = [1 \bmod 123]$$

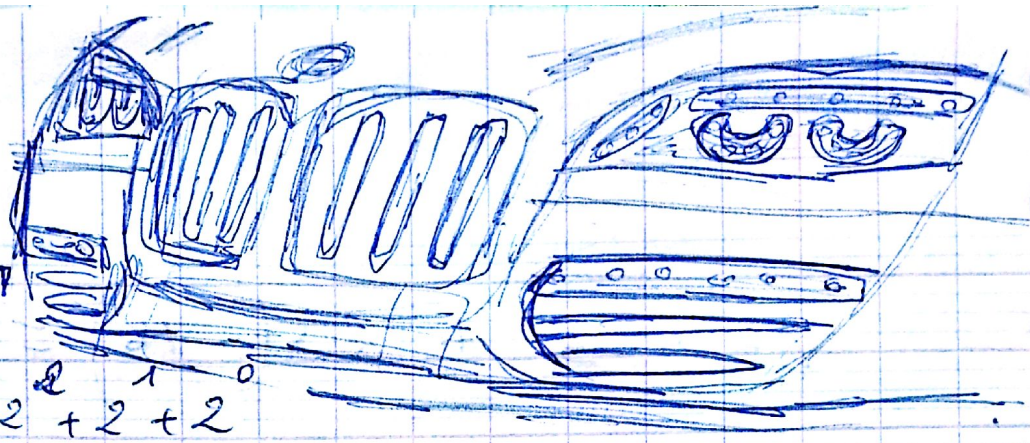
$$-16$$

$$123 \cdot 3 = 1 + k\,23$$

$$123 \cdot 3 = (1 \bmod 23)$$

r_i	120	31	27	4	3	1	0
q_i	/	3	1	6	1	11	
x_i	1	0	1	-1	7	-8	
y_i	0	1	-3	4	-27	31	

3-



$19^{31} \bmod 120$

$31 = 2^4 + 2^3 + 2^2 + 2^1 + 2^0$

~~it 0 d 1~~ $\quad temp := 1 \quad puiss = 19$

it0 : $d_0 = 1$

$temp := 19$

$puiss := 19^2 \bmod 120$

$puiss = 1$

$$\begin{array}{r} 19 \\ \times\ 19 \\ \hline 171 \\ 19 \\ \hline 361 \\ -240 \\ \hline 121 \end{array}$$

it1 : $d_1 = 1$

$temp := 19$

$puiss := 19^2 \bmod 120$

$puiss = 1$

it2 : $d_2 = 1$

$temp := 19$

$puiss := 19$

it3 : $d_3 = 1$

$temp := 19$

$puiss := 1$

it4

$d_4 = 1$

$temp := 19$

$puiss := 19^2 \bmod 120$

$= 1$

$temp = 19$

$19^{31} \bmod 120 = 19$

$31 = 2^4 + 2^3 + 2^2 + 2^1 + 2^0$

temp := 1

~~four~~

$d_4 = 1$

temp := $1^2 = 1$

temp := 1×19

$d_3 = 1$

temp := $1^2 = 1$

temp := 1×19

$d_2 = 1$

temp := $1^2 = 1$

temp := 1×19

$d_1 = 1$

temp := $1^2 = 1$

temp := 1×19

$d_0 = 1$

temp := $1^2 = 1$

temp := 1×19 → 19

Q.4

$n = 77$

$B = \{2, 3, 5, 7\}$

$\{10, 35, 12, 14, 19, 26\}$

$X_1 = 10$: $Y_1 = 10^2 \bmod 77 = 23$ $(0, 0, 0, 0)$ X

$X_2 = 35$: $Y_2 = 35^2 \bmod 77 = 70 = 2 \times 5 \times 7$ $(1, 0, 1, 1)$ —

$X_3 = 12$: $Y_3 = 12^2 \bmod 77 = 67$ $(0, 0, 0, 0)$ X

$X_4 = 14$: $Y_4 = 14^2 \bmod 77 = 42$ $(1, 1, 0, 1)$ —

$X_5 = 19$: $Y_5 = 19^2 \bmod 77 = 53$ $(0, 0, 0, 0)$ X

$X_6 = 26$: $Y_6 = 26^2 \bmod 77 = 60 = 2^2 \times 3 \times 5$ $(0, 1, 1, 0)$ —

$(1, 0, 1, 1)$

$(1, 1, 0, 1)$

$(0, 1, 1, 0)$

$a = X_2 \cdot X_4 \cdot X_6$

$=$

$1000 \mid 1011$

1101

0110

0110

0000

(1,0,1,1)
(1,1,0,1)
(0,1,1,0)

1011
0110
0110

1011
0010
0000

$a = x_2 \cdot x_4 \cdot x_6$ ~~70 x 42 x 60~~ 35 x 14 x 26

$a = 12740$

$b = \sqrt{x_2 \times x_4 \times x_6} =$

pgcd (a+b, n) ⇒ diviseur de 77

pgcd (a-b, n) ⇒ diviseur de 77

$b = \sqrt{176400}$

$b = 420$

42
x42
184
168
176400 → a

12740
420
12320

35
x26
210
70
910
x 14
3640
910
12740

420
x420
184
168
1764

pgcd (13160, 77) = 7

pgcd (12320, 77) = 11

Q5:

$(\mathbb{Z}/p^2\mathbb{Z}, +, \times)$ anneau

G sous ensemble de $\mathbb{Z}/p^2\mathbb{Z}$ avec

$$G = \{[x + p^2\mathbb{Z}] \mid x \equiv 1 \bmod p\}$$

1- L'ensemble des représentants minimaux:

~~$x = 1 + kp$~~

$x_0 = 1 + p^2\mathbb{Z}$

$x_1 = 1 + p + p^2\mathbb{Z}$

$\vdots \quad + 2p$

$\vdots$

$x_{p-1} = 1 + (p-1)p + p^2\mathbb{Z}$

$\Rightarrow x_{p-1} = 1 - p + p^2\mathbb{Z}$

donc

$x = 1 + kp + p^2\mathbb{Z}$ tq $x \in \{0, \dots, p-1\}$

$\Downarrow$

cardinalité $= p$

2- $(G, \times)$ est groupe?

↳ — $\times$ associative?

↳ — $\exists$ e neutre $\in G$?

↳ — tout élément de G est inversible?

- $*$ est associative

$$\left(1+k_1 p+p^2\mathbb{Z}\right) * \left(1+k_2 p+p^2\mathbb{Z}\right) * \left(1+k_3 p+p^2\mathbb{Z}\right)$$

$$= \left[\left(1+k_1 p\right) * \left(1+k_2 p\right) + p^2\mathbb{Z}\right] * k_3 p + p^2\mathbb{Z}$$

élément neutre :

$$1+kp \bmod p^2 * 1 \bmod p^2 = 1*(1+kp) \bmod p^2$$
$$= 1+kp \bmod p^2$$

- tout élément est inversible ? :

$$(1+kp)(1-kp) \bmod p^2$$

$$\equiv 1 \quad ? \; ? \; ?$$

3 - $[p+1+p^2\mathbb{Z}]$ générateur ?

$$(p+1)^0 = 1 \mod p^2$$

$$(p+1)^1 = p+1 \mod p^2$$

$$(p+1)^2 = p^2 + 2p + 1 \mod p^2 = 2(p+1)$$

$$(p+1)^3 = 2(p+1)\times(p+1) \mod p^2 = 2(p+1)^2 \mod p^2$$

$$= 4$$