Feuille de TD1 :

Sandra Marcello

25 février 2022

1 Exercice : GCD, Bézout's coefficients and modular inverse

1. GCD(315,540)
2. Bézout's coefficients (122, 246)
3. $99^{-1} = 101$

2 Exercice :Chinese Remainder Theorem

Solve the folllowing systems :

1.

$$x = 12[25]$$
$$x = 9[26]$$
$$x = 23[27]$$

2.

$$13x = 4[99]$$
$$15x = 56[103]$$

3 Exercice :CRT and RSA

The goal is to improve the RSA decryption algorithm. This can be done thanks to the CRT. Let $n = pq$, consider $Dec(y) = y^d[n]$. We define $d_p = d[p-1]$ and $d_q = d[q-1]$. Let $M_p = q^{-1}[p]$ et $M_q = p^{-1}[q]$.

Consider the following algorithm :

Input $(n, d_p, d_q, M_p, M_q, y)$

$x_p \leftarrow y^{d_p}[q]$

$x_q \leftarrow y^{d_q}[p]$
$x \leftarrow M_p q x_p + M_q p x_q[n]$
Return (x)
— Show that the ouptput of the algrotihm is the plain text x.
— Let $p = 11, q = 13$ and $d = 5$ compute : d_p, d_q, M_p, M_q
— Consider $y = 21$ find the associated plain message.

4 Exercice : Elliptic curve1/2

Let E be an elliptic curve over F_{11} defined by $y^2 = x^3 + x + 6$.
Find the points of this curve.