Catargiu Georgiana - Ecaterina
info - engleză, 332/1

Assignment 2

CATARGIU $\longrightarrow$ CATA

$k = 2, \quad \ell = 3$

$27^k < n < 27^\ell \Leftrightarrow 729 < n < 19683$

$n = 1655 = 331 \cdot 5 \quad \Rightarrow \begin{cases} p = 331 \\ q = 5 \end{cases}$

$\varphi(n) = (p-1)(q-1) = 330 \cdot 4 = 1320$

$\left.\begin{array}{l} 1 < e < \varphi(n) \Leftrightarrow 1 < e < 1320 \\ \gcd(e, \varphi(n)) = \gcd(e, 1320) = 1 \end{array}\right| \Rightarrow e = 71$

$K_E = (n, e) = (1655, 71)$ – public key

$K_D = d$, where $d = e^{-1} \bmod \varphi(n) = 71^{-1} \bmod 1320$

We compute d by using the Euclidean algorithm.

$1320 = 71 \cdot 18 + 42$

$71 = 42 \cdot 1 + 29$

$42 = 29 \cdot 1 + 13$

$29 = 13 \cdot 2 + 3$

$13 = 3 \cdot 4 + 1$

$3 = 3 \cdot 1 \quad \Rightarrow (1320, 71) = 1$, hence $\exists\, 71^{-1} \bmod 1320$

$1 = 13 - 4 \cdot 3 = 13 - 4 \cdot (29 - 2 \cdot 13) = 13 - 4 \cdot 29 + 8 \cdot 13 = 9 \cdot 13 - 4 \cdot 29$

$= 9(42 - 1 \cdot 29) - 4 \cdot 29 = 9 \cdot 42 - 9 \cdot 29 - 4 \cdot 29 = 9 \cdot 42 - 13 \cdot 29$

$= 9 \cdot 42 - 13 \cdot (71 - 42 \cdot 1) = 9 \cdot 42 - 13 \cdot 71 + 13 \cdot 42 = 22 \cdot 42 - 13 \cdot 71$

$= 22(1320 - 18 \cdot 71) - 13 \cdot 71 = 22 \cdot 1320 - 396 \cdot 71 - 13 \cdot 71$

$= 22 \cdot 1320 - 409 \cdot 71$

$\hookrightarrow 71^{-1} \bmod 1320 = -409 = 911$

$\Rightarrow K_D = d = 911$ – private key.

C	A	T	A
3	1	20	1

- plaintext : CATA
- split the plaintext : CA / TA

$$CA \longmapsto 3\cdot 27+1 = 82$$
$$TA \longmapsto 20\cdot 27+1 = 541$$

- encrypt : $m^e \bmod n$ – we will use the repeated squaring modular exponentiation method

$$e = 71 = 2^6+2^2+2^1+2^0$$

$82^{71} \bmod 1655$

$82^{(2^0)} = 82^1 = 82$
$82^{(2^1)} = 82^{(2^0)}\cdot 82^{(2^0)} = 82\cdot 82 = 104 \pmod{1655}$
$82^{(2^2)} = 82^{(2^1)}\cdot 82^{(2^1)} = 104\cdot 104 = 886 \pmod{1655}$
$82^{(2^3)} = 82^{(2^2)}\cdot 82^{(2^2)} = 886\cdot 886 = 526 \pmod{1655}$
$82^{(2^4)} = 82^{(2^3)}\cdot 82^{(2^3)} = 526\cdot 526 = 291 \pmod{1655}$
$82^{(2^5)} = 82^{(2^4)}\cdot 82^{(2^4)} = 291\cdot 291 = 276 \pmod{1655}$
$82^{(2^6)} = 82^{(2^5)}\cdot 82^{(2^5)} = 276\cdot 276 = 46 \pmod{1655}$
$\Rightarrow 82^{71} = 82^{(2^6+2^2+2^1+2^0)} = 46\cdot 886\cdot 104\cdot 82 = 618 \pmod{1655}$

$541^{71} \bmod 1655$

$541^{(2^0)} = 541^1 = 541$
$541^{(2^1)} = 541^{(2^0)}\cdot 541^{(2^0)} = 541\cdot 541 = 1401 \pmod{1655}$
$541^{(2^2)} = 541^{(2^1)}\cdot 541^{(2^1)} = 1401\cdot 1401 = 1626 \pmod{1655}$
$541^{(2^3)} = 541^{(2^2)}\cdot 541^{(2^2)} = 1626\cdot 1626 = 841 \pmod{1655}$
$541^{(2^4)} = 541^{(2^3)}\cdot 541^{(2^3)} = 841\cdot 841 = 596 \pmod{1655}$
$541^{(2^5)} = 541^{(2^4)}\cdot 541^{(2^4)} = 596\cdot 596 = 1046 \pmod{1655}$
$541^{(2^6)} = 541^{(2^5)}\cdot 541^{(2^5)} = 1046\cdot 1046 = 161 \pmod{1655}$
$\Rightarrow 541^{71} = 541^{(2^6+2^2+2^1+2^0)} = 161\cdot 1626\cdot 1401\cdot 541 = 391 \pmod{1655}$

• equivalents:

$$618 = \boxed{0}\cdot 27^2 + \boxed{22}\cdot 27 + \boxed{24} \longmapsto \text{–VX}$$
$$391 = \boxed{0}\cdot 27^2 + \boxed{14}\cdot 27 + \boxed{13} \longmapsto \text{–NM}$$

• ciphertext : –VX –NM

• split the ciphertext: –VX / –NM

• equivalents :

$$\text{–VX} \longmapsto \boxed{0}\cdot 27^2 + \boxed{22}\cdot 27 + \boxed{24} = 618$$
$$\text{–NM} \longmapsto \boxed{0}\cdot 27^2 + \boxed{14}\cdot 27 + \boxed{13} = 391$$

• decrypt : $c^d \bmod n$ – we will use the repeated squaring modular exponentiation method.

$$d = 911 = 2^9+2^8+2^7+2^3+2^2+2^1+2^0$$

$618^{911} \bmod 1655$

$$618^{(2^0)} = 618^1 = 618$$
$$618^{(2^1)} = 618^{(2^0)}\cdot 618^{(2^0)} = 618\cdot 618 = 1274 \pmod{1655}$$
$$618^{(2^2)} = 618^{(2^1)}\cdot 618^{(2^1)} = 1274\cdot 1274 = 1176 \pmod{1655}$$
$$618^{(2^3)} = 618^{(2^2)}\cdot 618^{(2^2)} = 1176\cdot 1176 = 1051 \pmod{1655}$$
$$618^{(2^4)} = 618^{(2^3)}\cdot 618^{(2^3)} = 1051\cdot 1051 = 716 \pmod{1655}$$
$$618^{(2^5)} = 618^{(2^4)}\cdot 618^{(2^4)} = 716\cdot 716 = 1261 \pmod{1655}$$
$$618^{(2^6)} = 618^{(2^5)}\cdot 618^{(2^5)} = 1261\cdot 1261 = 1321 \pmod{1655}$$
$$618^{(2^7)} = 618^{(2^6)}\cdot 618^{(2^6)} = 1321\cdot 1321 = 671 \pmod{1655}$$
$$618^{(2^8)} = 618^{(2^7)}\cdot 618^{(2^7)} = 671\cdot 671 = 81 \pmod{1655}$$
$$618^{(2^9)} = 618^{(2^8)}\cdot 618^{(2^8)} = 81\cdot 81 = 1596 \pmod{1655}$$

$$618^{911} = 618^{(2^9+2^8+2^7+2^3+2^2+2^1+2^0)}$$
$$= 1596\cdot 81\cdot 671\cdot 1051\cdot 1176\cdot 1274\cdot 618 = 82 \pmod{1655}$$

$391^{911} \bmod 1655$

$391^{(2^0)} = 391^1 = 391$
$391^{(2^1)} = 391^{(2^0)} \cdot 391^{(2^0)} = 391 \cdot 391 = 621 \pmod{1655}$
$391^{(2^2)} = 391^{(2^1)} \cdot 391^{(2^1)} = 621 \cdot 621 = 26 \pmod{1655}$
$391^{(2^3)} = 391^{(2^2)} \cdot 391^{(2^2)} = 26 \cdot 26 = 676$
$391^{(2^4)} = 391^{(2^3)} \cdot 391^{(2^3)} = 676 \cdot 676 = 196 \pmod{1655}$
$391^{(2^5)} = 391^{(2^4)} \cdot 391^{(2^4)} = 196 \cdot 196 = 351 \pmod{1655}$
$391^{(2^6)} = 391^{(2^5)} \cdot 391^{(2^5)} = 351 \cdot 351 = 731 \pmod{1655}$
$391^{(2^7)} = 391^{(2^6)} \cdot 391^{(2^6)} = 731 \cdot 731 = 1451 \pmod{1655}$
$391^{(2^8)} = 391^{(2^7)} \cdot 391^{(2^7)} = 1451 \cdot 1451 = 241 \pmod{1655}$
$391^{(2^9)} = 391^{(2^8)} \cdot 391^{(2^8)} = 241 \cdot 241 = 156 \pmod{1655}$

$\Rightarrow 391^{911} = 391^{(2^9+2^8+2^7+2^3+2^2+2^1+2^0)}$
$= 156 \cdot 241 \cdot 1451 \cdot 676 \cdot 26 \cdot 621 \cdot 391 = 541 \pmod{1655}$

- decrypt : 82 541
- literal equivalents :

$82 = \boxed{3} \cdot 27 + \boxed{1} \longmapsto CA$
$541 = \boxed{20} \cdot 27 + \boxed{1} \longmapsto TA$

- plaintext : CATA ✓