Popa Alex Ovidiu 20.11.2020

936

# PKC Assignment C

## RSA encryption + decryption

- plain text : POPA
- $k=2$, $l=3$
- $p=29$, $q=31 \Rightarrow n=899$

$\varphi(n) = 28 \cdot 30 = 840$

- take $e=71$, $1 < e < 840$ and $(71, 840) = 1$

$\Rightarrow K_E = (899, 71)$

- 27 letters alphabet, $27^2 < 899 < 27^3$ is true
- split the plain text into blocks of $k=2$ length:

PO/PA

- Write the numerical equivalent of each block:

$PO = \underline{\underline{16}} \cdot 27 + \underline{\underline{15}} \cdot 1 = 447$

$PA = \underline{\underline{16}} \cdot 27 + \underline{\underline{1}} \cdot 1 = 433$

- Encrypt each number ($m^e \bmod n$)

$447^{71} \bmod 899 = ?$ - repeated sq. mod. exp.

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

$$447^{(2^0)} = 447$$

$$447^{(2^1)} = 447^{(2^0)} \cdot 447^{(2^0)} = 231$$

$$447^{(2^2)} = 447^{(2^1)} \cdot 447^{(2^1)} = 320$$

$$447^{(2^3)} = 447^{(2^2)} \cdot 447^{(2^2)} = 813$$

$$447^{(2^4)} = 447^{(2^3)} \cdot 447^{(2^3)} = 204$$

$$447^{(2^5)} = 447^{(2^4)} \cdot 447^{(2^4)} = 262$$

$$447^{(2^6)} = 447^{(2^5)} \cdot 447^{(2^5)} = 320$$

$$447^{71} = 447^{(2^0+2^1+2^2+2^6)} = 447 \cdot 231 \cdot 320 \cdot 320$$

$$= 220 \pmod{899}$$

$$433^{71} \bmod 899 = ?$$

$$433^{2^0} = 433$$

$$433^{(2^1)} = 433^{(2^0)} \cdot 433^{(2^0)} = 497$$

$$433^{(2^2)} = 433^{(2^1)} \cdot 433^{(2^1)} = 683$$

$$433^{(2^3)} = 433^{(2^2)} \cdot 433^{(2^2)} = 807$$

$$433^{(2^4)} = 433^{(2^3)} \cdot 433^{(2^3)} = 373$$

$$433^{(2^5)} = 433^{(2^4)} \cdot 433^{(2^4)} = 683$$

$$433^{(2^6)} = 433^{(2^5)} \cdot 433^{(2^5)} = 807$$

$$433^{71} = 433^{(2^0+2^1+2^2+2^6)} = 433 \cdot 497 \cdot 683 \cdot 807$$

$$= 495 \pmod{899}$$

- Write the literal equivalents after encrypting:

$220 = \underline{0} \cdot 27^2 + \underline{8} \cdot 27 + \underline{4} \cdot 1 \Rightarrow$ _HD

$495 = \underline{0} \cdot 27^2 + \underline{18} \cdot 27 + \underline{9} \cdot 1 \Rightarrow$ _Ri

-> the ciphertext is: _HD_Ri

## Decryption

$n = 899, \ \varphi(n) = 840$

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

$d = 71^{-1} \bmod 840$ - compute using the Extended Euclidean Algorithm

$840 = 71 \cdot 11 + 59$

$71 = 1 \cdot 59 + 12$

$59 = 4 \cdot 12 + 11$

$12 = 1 \cdot 11 + 1$

$11 = 11 \cdot 1 \quad \Rightarrow (840, 71) = 1 \Rightarrow$ there exists $d = 71^{-1} \bmod 840$

We compute:

$1 = 12 - 1 \cdot 11 = 12 - 1 \cdot (59 - 4 \cdot 12) =$

$= 5 \cdot 12 - 1 \cdot 59$

$= 5 \cdot (71 - 1 \cdot 59) - 1 \cdot 59$

$= 5 \cdot 71 - 6 \cdot 59$

$= 5 \cdot 71 - 6 \cdot (840 - 11 \cdot 71)$

$= 5\cdot 71 - 6\cdot 840 + 66\cdot 71$

$= \underline{\underline{71\cdot 71}} - 6\cdot 840$

$\Rightarrow \underline{\underline{d = 71}} = 71^{-1} \bmod 840$

- Split the ciphertext: _HD / _RI
- Write the numerical equivalents:

$-HD = 0\cdot 27^2 + 8\cdot 27 + 1\cdot 4 = 220$

$-RI = 0\cdot 27^2 + 18\cdot 27 + 1\cdot 9 = 495$

- Decrypt each number ($c^d \bmod n$)

$220^{71} \bmod 899$

$220^{2^0} = 220$

$220^{(2^1)} = 220^{(2^0)} \cdot 220^{(2^0)} = 753$

$220^{(2^2)} = 220^{(2^1)} \cdot 220^{(2^1)} = 639$

$220^{(2^3)} = 220^{(2^2)} \cdot 220^{(2^2)} = 175$

$220^{(2^4)} = 220^{(2^3)} \cdot 220^{(2^3)} = 59$

$220^{(2^5)} = 220^{(2^4)} \cdot 220^{(2^4)} = 784$

$220^{(2^6)} = 220^{(2^5)} \cdot 220^{(2^5)} = 639$

$220^{71} = 220^{(2^0+2^1+2^2+2^6)} = 220\cdot 753\cdot 639\cdot 639$

$= 447 \pmod{899}$

$495^{71} \bmod 899$

$495^{(2^0)} = 495$

$495^{(2^1)} = 495^{(2^0)} \cdot 495^{(2^0)} = 497$

$495^{(2^2)} = 495^{(2^1)} \cdot 495^{(2^1)} = 683$

$495^{(2^3)} = 495^{(2^2)} \cdot 495^{(2^2)} = 807$

$495^{(2^4)} = 495^{(2^3)} \cdot 495^{(2^3)} = 373$

$495^{(2^5)} = 495^{(2^4)} \cdot 495^{(2^4)} = 683$

$495^{(2^6)} = 495^{(2^5)} \cdot 495^{(2^5)} = 807$

$495^{71} = 495^{(2^0+2^1+2^2+2^6)} = 495 \cdot 497 \cdot 683 \cdot 807$

$= 433 \pmod{899}$

- Write the literal equivalents after decrypting:

$447 = \underline{\underline{16}} \cdot 27 + \underline{15} \cdot 1 \Rightarrow$ PO

$433 = \underline{\underline{16}} \cdot 27 + 1 \cdot 1 \Rightarrow$ PA

$\Rightarrow$ plaintext is POPA



Scanned with CamScanner