uc3m | Universidad Carlos III de Madrid

CRYPTOGRAPHY AND COMPUTER SECURITY

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | COMPUTER SECURITY LAB (COSEC) GROUP

Mathematical background

Proposed exercises

Exercise 1 :
Computing inverses. Solve ax=1 mod.n, when g.c.d(a,n)=1

a) Applying Fermat's theorem. Solve: 37x = 1 mod.5

b) Applying Euler's theorem. Solve: 7x = 1 mod.12

c) Applying modified Euclid's algorithm. Solve: 32x = 1 mod.5

Exercise 2:
Solve ax=b mod.n equations, when g.c.d(a,n)=1

a) Applying Euler's theorem. Solve 3x = 3 mod.14

b) Applying modified Euclid's algorithm. Solve 19x = 4 mod.49

Exercise 3:
Solve ax=b mod.n equations, when g.c.d(a,n)=m≠1

a) Applying Euler's theorem. Solve 15x = 6 mod. 9

Exercise 4:
Modular arithmetic. Miscellaneous exercises

a) Using your preferred method.

   i) Solve: 2x = 1 mód.4

   ii) Solve: 37x = 1 mód.10

   iii) Solve 3x = 5 mód.8

   iv) Solve 5x = 10 mod. 15

   v) Solve 63x = 2 mod. 110

b) Mathematical proofs on properties:

i) Proof that:

Given M, n such that g.c.d(M,n) =1, and
Given e,d ∈ Z-{0} such that $e \cdot d=1$ mod. $\Phi(n)$, then the following expression holds:
$M^{e \cdot d}$ mod. n =M

ii) Justify whether these statements are true or false:

ii.a) $16^{16} + 16^{17} \bmod 17 = 1 \bmod 17$

ii.b) $16^{17} \cdot 16^{16} \bmod 17 \equiv -1 \bmod 17$

iii) Proof that:

Given a, n integers such that g.c.d. (a,n) = 1, then:
$a^x = a^y$ mod. n ⇨ $x = y$ mod. $\Phi(n)$.

iv) Proof that:

Given a, b, c, n ∈ Z-{0} such that g.c.d(a,n)=d, if $ab \equiv ac$ mod.n ⇨ $b \equiv c$ mod. n/d.

v) Proof that the following system has no solution:

$$\begin{cases} x=2 \text{ mod.}6 \\ x=3 \text{ mod.}9 \end{cases}$$