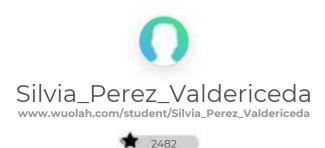
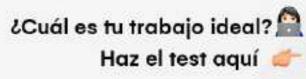
WUOLAH



Examen-1-2016-Enunciadosv3.pdf *Examenes*

- 2° Criptografía y Seguridad Informática
- **Grado en Ingeniería Informática**
- Escuela Politécnica Superior
 Universidad Carlos III de Madrid







http://bit.ly/necesitouncambio

Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA GRADO EN INGENIERÍA INFORMÁTICA

Examen 1 Parcial Evaluación Continua

Leganés/Colmenarejo – Semana 3 – 2016

Apellidos:

Nombre:

Grupo Modelo 1

EJERCICIO 1 (0,2 puntos)

Cálculo de inversos: Aplicando el Teorema de Euler:

- A) $7 \cdot x \mod 22 = 1$
- B) $3 \cdot x \mod 165 = 1$

EJERCICIO 2 (0,2 puntos)

Cálculo de inversos: Aplicando el método de Euclides modificado:

 $61 \cdot x \mod 197 = 1$

EJERCICIO 3 (0,1 puntos)

Resuelva:

 $11^{4200} \mod 6125 = x$

EJERCICIO 4 (0,2 puntos)

Resolución de ecuación de congruencia $a \cdot x \equiv b \mod n$

- A) $7 \cdot x = 21 \mod 28$
- B) $31 \cdot x = 12 \mod{79}$

EJERCICIO 5 (0,1 puntos)

Indique si 7 es raíz primitiva del módulo 23.

EJERCICIO 6 (0,2 puntos)

Calcule la operación que sigue con polinomios pertenecientes a $CG(2^4)$ siendo el mod (p(x)), donde $p(x) = x^4 + x + 1$.

Siendo $a(x) = (x^3+x^2)$, calcule $a(x)^2 \mod p(x)$



na I

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA GRADO EN INGENIERÍA INFORMÁTICA

Examen 1 Parcial Evaluación Continua

Leganés/Colmenarejo – Semana 3 – 2016

Apellidos:

Nombre:

Grupo Modelo 2

EJERCICIO 1 (0,2 puntos)

Cálculo de inversos: Aplicando el Teorema de Euler:

- A) $9 \cdot x \mod 41 = 1$
- B) $7 \cdot x \mod 72 = 1$

EJERCICIO 2 (0,2 puntos)

Cálculo de inversos: Aplicando el método de Euclides modificado:

 $23 \cdot x \mod 47 = 1$

EJERCICIO 3 (0,1 puntos)

Razone si existe algún número "s" tal que

 $3^{s} \mod 13 = 1$

En caso de existir, indique cuántos podrían existir. A la vista de lo anterior, ¿es 3 raíz primitiva de 13?

EJERCICIO 4 (0,2 puntos)

Resolución de ecuación de congruencia $a \cdot x \equiv b \mod n$

- A) $19 \cdot x = 20 \mod 37$
- B) $15 \cdot x = 12 \mod 21$

EJERCICIO 5 (0,1 puntos)

¿Cuántos números positivos, menores que 3267, son primos relativos con él?

EJERCICIO 6 (0,2 puntos)

Sean los polinomios $a(x)=x^2+1$ y $b(x)=x^2$ pertenecientes a $CG(2^3)$ siendo el mod (p(x)), donde $p(x)=x^3+x+1$. Calcule el polinomio $c(x)=a(x)^2 \cdot b(x)$ mód p(x)



ıana

CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA GRADO EN INGENIERÍA INFORMÁTICA

Examen 1 Parcial Evaluación Continua

Leganés/Colmenarejo – Semana 3 – 2016

Apellidos:

Nombre:

Grupo

Modelo 3

EJERCICIO 1 (0,2 puntos)

Cálculo de inversos: Aplicando el Teorema de Euler:

- A) $6 \cdot x \mod 42 = 1$
- B) $3 \cdot x \mod 77 = 1$

EJERCICIO 2 (0,2 puntos)

Cálculo de inversos: Aplicando el método de Euclides modificado:

 $26 \cdot x \mod 113 = 1$

EJERCICIO 3 (0,1 puntos)

Calcule

21960 mód 131

EJERCICIO 4 (0,2 puntos)

Resolución de ecuación de congruencia $a \cdot x \equiv b \mod n$

- A) $7 \cdot x = 21 \mod 91$
- B) $6 \cdot x = 5 \mod 43$

EJERCICIO 5 (0,1 puntos)

Encuentre dos raíces primitivas respecto al módulo 11.

EJERCICIO 6 (0,2 puntos)

Sean los polinomios a(x)=x+1 y b(x)=x pertenecientes a $CG(2^3)$ siendo el mod (p(x)), donde $p(x)=x^3+x+1$. Calcule el polinomio $c(x)=a(x)^2 \cdot b(x)^3$ mód p(x)

WUOLAH



Centro preparador y examinador www.thatsfun.es

Ordonez, 38, Leganes

8 911 03 58 00

609 52 40 92

Gaztambide 61, 1° 4 Madrid

@ 911 27 32 04

911 27 32 04

CRYPTOGRAPHY AND COMPUTER SECURITY BACHELOR IN INFORMATICS ENGINEERING

Test 1 Continuous assessment

Leganés – Week 3 – 2016

Name:

Group Model 1

EXERCISE 1 (0.2 marks)

Inverse calculation using Euler's Theorem

A) $7 \cdot x \mod 22 = 1$

Surname:

B) $3 \cdot x \mod 165 = 1$

EXERCISE 2 (0.2 marks)

Inverse calculation using Euclides' extended algorithm:

 $61 \cdot x \mod 197 = 1$

EXERCISE 3 (0.1 marks)

Solve:

 $11^{4200} \mod 6125 = x$

EXERCISE 4 (0.2 marks)

Equations of type $a \cdot x \equiv b \mod n$

A) $7 \cdot x = 21 \mod 28$

B) 31·x=12 mod79

EXERCISE 5 (0.1 marks)

Explain in detail whether the following statement is true or false:

There are 8 primitive roots mod 31

Compute one primitive root respect to modulo 31.

EXERCISE 6 (0.2 marks)

Carry out the following operations with polynomials belonging to $GF(2^4)$, in which the irreducible polynomial is $p(x) = x^4 + x + 1$. Considering $a(x) = (x^3 + x^2)$, calculate $a(x)^2$ mod p(x)

4 horas de speaking gratis a la semana

Simulacros de examen todos los viernes GRATIS

OXFORD
PET
FIRST
CAE
TOELF
TOEIC
IELTS

Flexibilidad horaria

Grupos reducidos



Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

Reservados todos los derechos. No se permite la explotación económica ni la transformación de esta obra. Queda permitida la impresión en su totalidad.

CRYPTOGRAPHY AND COMPUTER SECURITY BACHELOR IN INFORMATICS ENGINEERING

Test 1 Continuous assessment

Leganés – Week 3 – 2016

Surname:

Name:

Group Model 2

EXERCISE 1 (0.2 marks)

Inverse calculation using Euler's Theorem

- A) $9 \cdot x \mod 41 = 1$
- B) $7 \cdot x \mod 72 = 1$

EXERCISE 2 (0.2 marks)

Inverse calculation using Euclides' extended algorithm:

$$23 \cdot x \mod 47 = 1$$

EXERCISE 3 (0.1 marks)

Explain if there is a number "s" such that

$$3^{s} \mod 13 = 1$$

If "s" exists, explain how many of them may exist. Based on the previous facts, is 3 primitive root of 13?

EXERCISE 4 (0.2 marks)

Equations type $a \cdot x \equiv b \mod n$

- A) $19 \cdot x = 20 \mod 37$
- B) $15 \cdot x = 12 \mod 21$

EXERCISE 5 (0.1 marks)

How many positive numbers, below 3267, are relatively primes to it?

EXERCISE 6 (0.2 marks)

Let $a(x)=x^2+1$ and $b(x)=x^2$ from $GF(2^3)$, with mod (p(x)), where $p(x)=x^3+x+1$. Calculate the polynomial $c(x)=a(x)^2 \cdot b(x)$ mod p(x)

