

Stinson:

Paginas: 1 definicion de criptosistema.

3,4 ~~7/12~~ anillo.

Shift cipher, substitution cipher.
(definir permutacion)

Pag 9: definicion de φ y teorema
 $ax \equiv b \pmod{m}$

Pag 10: Inverso

Pag 12 monoalfabetico Vignere cipher
no lo damos, ni el siguiente de
Hill cipher.

Saltamos las paginas 12-160

Ejercicios: 1-11

Capítulo 5 PKC un enorme avance.

Pag 162 trapdoor oneway function.

Seguridad Siempre es condicional ya que la key es pública. Cogemos todos los x hacemos $E_x(x)$ y cuando salga la y , esa sera la x .

Ejemplo de one way $n=pq$ $b \bmod n$
 $x^b \bmod n$ es one way.

¿Cómo se sabe lo difícil que es calcular?

pag 163 trapdoor one way function.

163-173

- Algorithm de Euclides
- Lagrange
- Fermat
- Chinese remainder theorem
- primitive root

pag. 173 definici3n de RSA.

pag 175 definici3n de big O.

Como calcular el tiempo de
coste. k10bits

pag 1 • bases change pag 2 ex. 4.

- Number of digits
- bit operation.

- Adding 2 of w bits $\rightarrow w$ bit operation

. Multiplication

$$\begin{array}{r} 11101 \\ 1101 \\ \hline 11101 \\ 111010 \\ 1101 \\ \hline 10010001 \\ 1101 \\ \hline 10111001 \end{array}$$

Sumo fila por fila cuando tengo
2 unos y me llevo 1 de po un
uno y me llevo 1 a la siguiente
columna

$$\begin{array}{r}
 1110000 \\
 10100 \\
 \hline
 111000000 \\
 11100 \\
 \hline
 100611000000
 \end{array}$$

Tiempo para multiplicar dos números de w y l bits. Sumare l filas de w bits cada una.

Example: compute $n!$

Multiplico $n-1$ números cada uno tiene $\lg i$ bits

$a_i \cdot (i+1)$
 $1.2.3.4.5$
 a_i tiene $\sum_{j=2}^i \lg j$ bits

$$\sum_{j=2}^i \lg j = i \lg i \text{ bits}$$

luego $a_i \cdot (i+1) = i \lg^2 i$ bit operations

$$\text{luego } n! = \sum_{i=2}^n i \lg^2 i = n^2 \lg^2 n \text{ bits}$$

Multiplicar polinomios

$$\sum_{i=0}^d a_i x^i \sum_{j=0}^d b_j x^j = \sum_{k=0}^{2d} \left(\sum_{j+i=k} a_i b_j \right) x^k$$

Coefficientes con n bits $\sum_{k=1}^{2d} K \cdot n^2 = n^2 d^2$

División y resta tienen el mismo coste.

Ejercicios: 9, 11, 14, 15, 16

En la pagina 11, vuelvo a
Shinson.

pag 178 Primality.

- Legendre symbol
- Jacobi symbol (propiedades QR
on mod n)
- Quadratic residues
- Solovay Strassen Fermat test.
- Miller-Rabin

Pag 189 Factoring algorithms
pollard ρ harte

Pag 194

Saltemos hasta pg 233

pg 233 logaritmo discreto.

Algoritmos

Cuerpos finitos

Cuerpos elípticos

No con la 6.5.4 point
compression.

o sea hasta pg 262

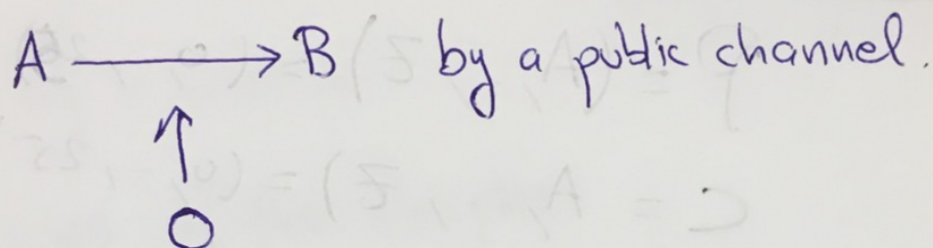
Ejerc en 265, 266, 267

No 268 Saltemos guías a 273

Mandar trabajo para los alumnos. Por ejemplo las secciones del capítulo 1 que no daremos, y otros capítulos

Introducción

¿Qué es un criptosistema?



Definition: A cryptosystem is a 5-tuple

$$(P, C, K, E, D)$$

Given $k \in K$ $E_k: P \rightarrow C$ injective
 $D_k: C \rightarrow P$

$$D_k(E_k(x)) = x$$

Select $w \in K$ randomly (they are together)

• If $C = P$ permutation

Examples Modular arithmetic. (mis notas)

Definition of division, gcd, lcm

congruence, set $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^*$ operations, ring.

- How many $(g, m) = 1 \quad p(m)$.

Shift cipher

$$\mathcal{P} = (A, \dots, Z) = (0, \dots, 25)$$

$$\mathcal{C} = (A, \dots, Z) = (0, \dots, 25)$$

$$K = (\dots, 25)$$

$$e_K(x) = x + K \pmod{26}$$

$$d_K(y) = y - K \pmod{26}$$

examples • To encrypt page 5 stinson
• to cryptanalyze, page 6

Substitution

$$e_\pi(x) = \pi(x)$$

$$d_\pi(y) = \pi^{-1}(y)$$

example

how to build d_π from e_π .
Final page 7.

Affine: $e(x) = ax + b \pmod{26}$

$ax \not\equiv b \pmod{26}$ only 1 solution

- How many $(g, m) = 1 \quad \varphi(m)$.

- Inverse of a mod m .

Exercises of the chapter.

4 hours. (First day).

Dia 2 PKC.

In order to send a message, A, B need to get in touch at least once.

But imagine that each of us need to send our credit card info to a shop in a

secure way. E_K should be public in such a way that

$E_K(x) = c$ cannot be decrypt but only by Bob.

Definition: One-way function is

$f: P \rightarrow C$ such that

$f(P) = C$ is easy but $f^{-1}(C) = P$
is hard to compute.

For example is polynomial time
to compute C but is exponential
to compute $f^{-1}(C)$.

Example: let $n = 135761$

Compute $x^2 \bmod n$ is polynomial

$$x = 23 \quad 23 \times 23 = \frac{2300}{4} = 575 = 23 \times 25$$
$$23 \times 23 = 23 \times (25 - 2) = 575 - 46 = 529$$

given 24239 encontrar $x^2 \equiv 36501$.

$$433 \times 433 = (410^2 + 310 + 3)(410^2 + 310 + 3)$$

$$= 1610^4 + 2410^3 + (12 + 9 + 12)10^2 + 1810 + 9$$

$$= 10^5 + 610^4 + 210^4 + 410^3 + 310^3 + 310^2 + 10^2 + 810 + 9$$

$$= 10^5 + 810^4 + 710^3 + 410^2 + 810 + 9$$

$$= 187489 \pmod{135761}$$

$$= 51728.$$

$$187489 = 135761 + 51728$$

$$24239 \text{ find } x^2 \equiv 24239 \pmod{135761}$$

How to compute the time?

Definition: A number $n \in \mathbb{Z}$ written in base b is

$$n = \sum_{j=0}^d a_j b^j \quad 0 \leq a_j < b.$$

To change basis we divide by b subtract and divide again

$n = 345$ in base 3

$$\begin{aligned} 345 &= 115 \cdot 3 = 3[38 \times 3 + 1] \\ &= 9[12 \times 3 + 2] + 3 = 27[3 \times 4] + 2 \cdot 9 + 3 \\ &= 81[3 + 1] + 2 \cdot 9 + 3 = 3^5 + 3^4 + 2 \cdot 3^2 + 3 \\ &= (110210)_3 \end{aligned}$$

We compute in base 2. Binary

Definition: A bit operation is

1) Look up and down and if carry

2) $(0, 0, 0) \rightarrow (0, 0)$

$(0, 0, 1) \rightarrow (1, 0)$

$(0, 1, 0) \rightarrow (1, 0)$

$(1, 0, 0) \rightarrow (1, 0)$

$(0, 1, 1) \rightarrow (0, 1)$

$(1, 0, 1) \rightarrow (1, 1)$

$(1, 1, 0) \rightarrow (1, 1)$

$(1, 1, 1) \rightarrow (1, 1)$

Addition of 2 w bits $\rightarrow w$ bits operation

Multiplication $w \times l \rightarrow w.l$ " "

Subtraction = Addition, Multiplication = division

Examples.

big O notation

polynomial time

Exponenciación como ejemplo y su inversa se cree que no.

Seguir, comparando capítulo 2 de Wobitz, con mis notas, y con Johnson.

ya sabemos que factorizar no es polinómico

RSA.

Examples: multiply k by l bits

- Put at most l rows of k bits
- Add $l-1$ times, which is k bit operations
- In total $k \cdot l$.

Example: Compute $n!$

• Let $a_j = \prod_{i=2}^j i$

How many bits has a_j ?

$$2^{w-1} \leq n < 2^w$$

has w bits

Example: Multiply $n \cdot m$ mod b $(\lg b)^2$ mult.
and 2 reductions $(\lg n + \lg m) \lg b$

$$2^{\lceil \lg_2 n \rceil} \leq n = 2^{\lg_2 n} < 2^{\lceil \lg_2 n \rceil + 1}$$

so, has $\lceil \lg_2 n \rceil + 1$ bits

$$\begin{aligned} \lceil \lg_2 a_j \rceil &\leq \sum_{i=2}^j \lg_2 i \\ &= \frac{1}{\lg 2} \sum_{i=2}^j \lg i < \frac{1}{\lg 2} \int_1^{j+1} \lg t \, dt \\ &= \frac{1}{\lg 2} \left(t \lg t - t \right) \Big|_1^{j+1} = \frac{(j+1) \lg(j+1) - 1}{\lg 2} \\ &= \frac{(j+1) \lg(j+1) - j}{\lg 2} \end{aligned}$$

To get $a_{j+1} = a_j \cdot (j+1)$

$$j+1 \text{ has } \lceil \lg_2(j+1) \rceil \leq \frac{\lg(j+1)}{\lg 2} + 1$$

$$\leq 4j \lg^2 j \text{ bits}$$

So, to get a_n we get

$$\sum_{j=2}^n j \lg^2 j \leq 4 \lg^2 n \cdot n^2.$$

Example: Polynomial of degree d_1 ,
and degree $d_2 \leq d_1$ coefficients $\leq m$.

$$\begin{aligned} & \left(\sum_{i=0}^{d_1} a_i x^i \right) \left(\sum_{j=0}^{d_2} b_j x^j \right) = \\ &= \sum_{k=0}^{d_1+d_2} \left(\sum_{\substack{i+j=k \\ 0 \leq i \leq d_1 \\ 0 \leq j \leq d_2}} a_i b_j \right) x^k \end{aligned}$$

We have for $k \leq d_2$, k
possible $i+j=k$ $j=0, \dots, k$, $i=k-j$.

and for $w > d_2$, we have d_2 possible

$$j = 0, \dots, d_2, \quad i = w - j.$$

In particular we have $d_2 + 1$ multiplications and d_2 additions

Multiplications are of numbers $\leq m$

so requires $(\lg m)^2$ we add the partial sums which are $\leq d_2 m^2$ or

$\lg d_2 + 2 \lg m$ each

$$\text{so } (d_2 (\lg m)^2 + d_2 (\lg d_2 + 2 \lg m)) (d_1 + d_2)$$

$$\text{If } d_1 = d_2 \quad d_2^2 \lg^2 m \text{ if } m > \sqrt{d_2}$$

Example: Modular reduction $O(\lg^2 m)$
mod m

division of two integers.

111001101101

$$a = kb + r$$

$$\bullet \left[\begin{array}{l} r \geq a - b \geq 0 \end{array} \right] \quad k = k + 1$$

$$\bullet \quad a - b < b \Rightarrow a = kb + r$$

We did $\frac{a}{b}$ subtractions so

$$\text{it is } \frac{a}{b} \cdot \lg_2 a$$

or

$$\begin{array}{r}
 11011011 \quad \overline{111} \\
 1110000 \quad 1111 \\
 \hline
 1101011 \\
 111000 \\
 \hline
 110011 \\
 11100 \\
 \hline
 10111 \\
 1110 \\
 \hline
 1001 \\
 111 \\
 \hline
 010
 \end{array}$$

$$11011011 = (11111) \times 111 + 10$$

on each subtraction a remove one digit so there are

$w-l$ substructures each of l integer so it is $w.l$.

Example: compute $\binom{n}{m}$

$$\frac{n(n-1)\dots(n-m+1)}{m!} \quad \left(m < \frac{n}{2}\right)$$

$m!$ requires $m^2 \lg^2 m$

bits of $\prod_{j=(n-m+1)}^w j$ is $\sum_{n-m+1}^w \lg j =$

$$= \int_{n-m+1}^w \lg t \, dt = t \lg t \Big|_{n-m+1}^w = w \lg w - (n-m+1) \lg(n-m+1)$$

multiply by $\lg n$ bits gets

$$\sum_{w=n-m+1}^n w \lg n \lg w - (n-m) \lg^2 n = \lg^2 n m^2$$

Big O notation

Definition: $f(n) = O(g(n))$ if

$$|f(n)| \leq C g(n) \quad \forall n.$$

valid for $n \in \mathbb{N}^w$.

Example: • A polynomial of degree d is $O(n^d)$.

$$\bullet \lg n = O(n^\epsilon) \quad \forall \epsilon > 0.$$

$$\bullet f(n) = \text{number of bits of } n \text{ is } f(n) = O(\lg n)$$

Exercise: Explain Remark on page 8 of Wollitz.

We can express with O all the computations done so far.

Definition: An algorithm is in polynomial time if is

$$O(w_1^{d_1} \dots w_r^{d_r}) \text{ for}$$

integers $n_1, \dots, n_r$ of bits $w_1, \dots, w_r$.

Important: The notion of asymptotic.

Exponentiation: $b^n \bmod m$

- write n in base 2

$$n = \sum_{j=0}^k u_j 2^j$$

requires: $O(\lg^2 n)$.

$$b^{\sum u_j 2^j} = \underbrace{b^{2^0}}_{a} \underbrace{b^{2^1}}_{B} \underbrace{b^{2^2}}_{B^2} \dots b$$

$$\begin{aligned} a &= 1 \\ B &= b \end{aligned}$$

- $u_j = 1$ $a = a \cdot B \pmod{m}$ b^8

- $u_j = 0$ $a = a$

- $B = B^2 \bmod m$

$$b^7 = b^4 b^2 b$$

at most 1 multiplication and 1 square
always $\lg m$ bits $(\lg m)^2 \lg n$

It is believed that the inverse is not polynomial time.

Know the inverse^{of 3} is equivalent to factoring.

$$ad = 1 + k \varphi(n)$$

$$\begin{aligned} \frac{ad-1}{n} &= k \frac{\varphi(n)}{n} = k \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right) \\ &= k \left(1 - \left(\frac{1}{p} + \frac{1}{q}\right) + \frac{1}{n}\right) \end{aligned}$$

$$3 \varphi(n) > 2(n-2)$$

$$3n - 3(p+q) + 3 > 2n - 2$$

$$p(q-3) > 3q-5$$

si $p > 3$ y $q > 7$

$$n > 3(p+q) - 5$$

once we know $\varphi(n)$, then

$$\begin{aligned} A = \varphi(n) &= (x-1)(y-1) = xy - (x+y) + 1 \\ &= n - (x+y) + 1 \end{aligned}$$

$$\text{so } \begin{cases} x+y = n - A + 1 \\ xy = n \end{cases}$$

and we solve x and y .

Factoring is difficult.

In fact knowing the inverse of
anybody is equivalent to factoring:

Given May 2007.

Pollard - rho for factoring.

Day 3: Number theory

- Euclidean algorithm
- Chinese remainder theorem
- Lagrange
- Fermat
- $\mathbb{Z}_p^*$ is cyclic
- Theorem 5.8 Shinson

α is primitive $\Leftrightarrow \alpha^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$

$\forall q \mid p-1, q \text{ prime.}$

(Pocklington-Lehmer)

176 Shinson inverse mod m
in $(\lg m)^3$, and exponentiation

RSA HQV1 PAGE 178 ST1

generar números en RSA.

Después de Teorema 5.8

Teorema 5.9 a is quadratic residue $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

$$a = b^2 \Rightarrow b^{p-1} = 1 \pmod{p}$$

$$\text{if } a^{\frac{p-1}{2}} \equiv 1 \text{ and } b^i = a \pmod{p}$$

$$\Rightarrow i = 2w + 1 \Rightarrow$$

$$b^{w(p-1)} b^{\frac{p-1}{2}} = 1 \pmod{p}$$

Which is not by theorem 5.8.

In order to know if it is a quadratic residue we introduce

Legendre Symbol and Jacobi symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \in \mathbb{R}_p \\ -1 & a \in \mathbb{N}_p \\ 0 & p \mid a \end{cases}$$

Jacobi symbol

$$\left(\frac{a}{n}\right) = \prod_{p \mid n} \left(\frac{a}{p}\right)^{\alpha_p} \quad n = \prod_{p \mid n} p^{\alpha_p} \quad (n \text{ odd})$$

Solovay-Strassen

$$2 \leq a < n$$

$$\text{If } a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \Rightarrow n \text{ prime}$$

$$a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \Rightarrow n \text{ composite}$$

$$\left(\frac{a}{n}\right) = 0 \Rightarrow n \text{ composite}$$

Exercises to see the probability.
5.22 pag 231

It is polynomial time algorithm

Quadratic reciprocity law.

DIFFICULT

What to do next?

Pocklington-Lehmer $n-1=rs$ $r > \sqrt{n}$

$$\forall p \mid r$$

$$(a_p^{\frac{n-1}{p}} - 1, n) = 1$$

$$a_p^{n-1} \equiv 1 \pmod{n}$$

then n is prime $p^e \mid r$

Proof: $b_p = a_p^{\frac{n-1}{p^e}}$

$$b_p^{p^{e-1}} \not\equiv 1 \pmod{p}$$

$$b_p^{p^e} \equiv 1 \pmod{p}$$

$$\Rightarrow \text{ord}(b_p) = p^e \mid p-1 \Rightarrow p > \sqrt{n} \quad \square$$

Examples 11351

Solovay-Strassen $1 \leq a \leq n-1$ random.

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \text{ prime}$$

$$\left(\frac{a}{n}\right) \equiv 0 \text{ composite}$$

$$a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \text{ composite}$$

Example conrad para alumnos

—

|

$$\sum_{k=1}^{p-1} \left(\frac{w}{p}\right) \zeta_p^k = g_p \quad \zeta_p = e^{\frac{2\pi i}{p}}$$

$$\begin{aligned} g_p^2 &= \sum_{w,l} \left(\frac{w}{p}\right) \left(\frac{l}{p}\right) \zeta_p^{w+l} \\ &= \sum_{w=1}^{p-1} \sum_{l=1}^{p-1} \left(\frac{w}{p}\right) \left(\frac{l}{p}\right) \zeta_p^{w(1+l)} \\ &= \sum_{u=1}^{p-1} \left(\frac{u}{p}\right) \left(\sum_{w=0}^{p-1} \left[\left(\zeta_p\right)^{1+u} \right]^w - 1 \right) \\ &= \left(\frac{-1}{p}\right) p - \sum_{u=1}^{p-1} \left(\frac{u}{p}\right) \\ &= \left(\frac{-1}{p}\right) p \end{aligned}$$

$$g^q_p = \left(g^{\frac{q-1}{2}}_p \right) g_p = p^{\frac{q-1}{2}} g_p = \left(\frac{p^*}{q} \right) g_p$$

$$g^q_p = \left(\sum_{k=1}^{p-1} \left(\frac{k}{p} \right) \sum_p^k \right)^q = \sum_{k=1}^{p-1} \left(\frac{k}{p} \right) \sum_p^{qk}$$

$$= \left(\frac{q}{p} \right) \sum_{k=1}^{p-1} \left(\frac{k}{p} \right) \sum_p^k = \left(\frac{q}{p} \right) g_p$$

$$\left(\frac{p^*}{q} \right) = \left(\frac{q}{p} \right)$$

$$\left(\frac{p^*}{q} \right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{q} \right) \left(\frac{p}{q} \right)$$

$$(-1)^{\frac{p-1}{2} \frac{q-1}{2}} = \left(\frac{p}{q} \right) \left(\frac{q}{p} \right)$$

To see whether a is a quadratic residue we see that

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{b-1}{2}\frac{a-1}{2}}$$

$$\left(\frac{a}{b}\right) = \prod_{p|b} \left(\frac{a}{p}\right)^{\alpha_p} = \prod_{p|b} \prod_{q|a} \left(\frac{q}{p}\right)^{\beta_q \alpha_p}$$

$$= \prod_{q|a} \prod_{p|b} \left(\frac{p}{q}\right)^{\beta_q \alpha_p}$$

$$= \left(\frac{b}{a}\right) (-1)^{\frac{b-1}{2}\frac{a-1}{2}} \prod_{q|a} \prod_{p|b} \left((-1)^{\frac{q-1}{2}\frac{p-1}{2}}\right)^{\beta_q \alpha_p}$$

exercise

Corollary: Solovay-Strassen is polynomial. With what probability?
pay 185 (quizzes).

A previous primality test is

Fermat's: $a^{n-1} \not\equiv 1 \pmod{n} \Rightarrow$
 n is composite.

If $a^{n-1} \equiv 1 \pmod{n}$ then

n is a pseudoprime base a
there are n which are
pseudoprimes for all $(a, n) = 1$

n is Carmichael: $a^n \equiv a \pmod{n} \forall a$ Example
221 38,
24

Pocklington - Lehmer

Proposition: $\forall l \mid r \quad rs = n-1$
 $r > \sqrt{n}$

$$\exists \left(a_l^{\frac{n-1}{l}}, n \right) = 1, \quad a_l^{n-1} \equiv 1 \pmod{n}$$

$\Rightarrow n$ is prime. $p^e \parallel r$

$$\forall p \mid n \quad b_p = a_p^{\frac{n-1}{p^e}} \quad b_p^{p^e} \equiv 1 \pmod{p}$$

$$b_p^{p^{e-1}} \not\equiv 1 \pmod{p} \Rightarrow \text{ord } b_p = p^e \mid p-1$$

$$\Rightarrow \forall l \mid r \Rightarrow r \mid p-1 \Rightarrow p > \sqrt{n} \quad \square$$

Example 153533 page 195 Washington

Miller Rabin

$$n-1 = 2^w m$$

random a

$$b = a^m \quad b \equiv 1 \pmod{n} \Rightarrow n \text{ is prime}$$

$$\text{if } b^{2^j} \equiv -1 \quad \text{for } j=0 \dots w-1 \Rightarrow$$

n is prime

$$b^{2^{w-1}} \not\equiv -1 \Rightarrow n \text{ is composite.}$$

Proof

$$a^m \neq 1$$

$$a^{2^{w-1}m} \neq -1 \Rightarrow a^{2^{w-1}m} = 1$$

$$\Rightarrow a^{2^{w-2}m} = 1 \dots a^m = 1 \quad \square$$

How many

$$x^{m 2^i} \equiv 1 \pmod{p^a}$$

$$(m 2^i, p-1) < \frac{p-1}{2} \quad i < p$$

Example I have a file full of
examples in prof-coast file

A cabannes a pag 188 squares not

no

Algorithms para factorizar: ejercicios
alumnos

School $\frac{1}{4}$ de Miller para alumnos

other attacks RAS pag. 201
alumnos

Nada de las secciones 5.8 y 5.9

Finite fields of my notes
and Sherson

Discrete logarithm, Finite fields
and elliptic curves is chapter 6.
Section 6.7 no except maybe
6.7.3 only the definitions



Primality test

Fermat If $a^{n-1} \not\equiv 1 \pmod{n}$
then n is composite.

If n is composite and $a^{n-1} \equiv 1 \pmod{n}$
 n is a pseudoprime for the base a .

There are infinitely many integers
which are pseudoprimes for all a .
Carmichael numbers.

Example for Fermat

Discrete logarithms

Problem: $\langle \alpha \rangle$ a multiplicative group given $\beta \in \langle \alpha \rangle$ find a s.t. $\alpha^a = \beta$ $a = \log_{\alpha} \beta$

El gamal $K = \{ p, \alpha, a, \beta : \beta = \alpha^a \}$

p, α, β public
 a secret w secret

$$e_w(x, w) = (y_1, y_2)$$

$$y_1 = \alpha^x \text{ mod } p$$

$$y_2 = x \beta^w \text{ mod } p$$

$$d_{12} = \frac{y_2}{y_1^a} = x$$

Example page 234

How to solve the DLP

- Trivial $O(n)$
- Shanks Baby step Giant step
- Pollard rho
- Index-Calculus
- Pohlig-Hellman

Mo la section 6.3

Faster Miller-Rabin

x at random $n-1 = 2^k m$

$$x^m \equiv 1 \pmod{n} \Rightarrow x \text{ prime}$$

$$x^{2^i m} \equiv -1 \pmod{n} \text{ for } i < k$$

$\Rightarrow n$ is prime

$$x^{2^{k-1} m} \not\equiv -1 \pmod{n} \Rightarrow$$

n is composite.

Suppose n is prime then

$$x^2 \equiv 1 \pmod{n}$$

has 2 solutions $\Rightarrow x^{2^{k-1} m} \equiv 1 \pmod{n}$

$$\Rightarrow x^{2^{k-2} m} \equiv 1 \Rightarrow \dots \Rightarrow x^m \equiv 1 \pmod{n} \quad \square$$

EXAMPLES.

Section 6.5 elliptic curves
hasta 6.5.4 luego explica
el cap. 5 de whashington
solo

6.5.5 si es doubling.

mi introducción con el círculo
a curvas elípticas.

Shanks algorithm

$$\beta \in \langle \alpha \rangle \quad |\langle \alpha \rangle| = n$$

$$m = \lceil \sqrt{n} \rceil + 1$$

$$L_1 (\alpha^m, \alpha^{2m}, \dots, \alpha^{(m-1)m})$$

$$L_2 (\beta \alpha^{-1}, \dots, \beta \alpha^{-(m-1)})$$

$$\begin{aligned} a = u + vm &= (m-1) + (m-1)m \\ &= m^2 - 1 \geq n-1 \quad \square \end{aligned}$$

$$\beta \alpha^{-u} = \alpha^{jm} \text{ is the answer}$$

$O(m)$ and $O(m)$ string.

$$\lg_3 525 \text{ in } \mathbb{Z}_{809}^*$$

$$2^9 \equiv 99 \pmod{809}$$

$$29 = \left\lceil \sqrt{809} \right\rceil$$

Rockhingham-Lehmer

$$808 = 8(101)$$

$$100 = 10 \cdot 10 \quad 2, 5$$

$$(2^{50} - 1, 101)$$

$$2^7 = 27$$

$$2^{50} = (2^7)^7 \cdot 2 = 27^7 \cdot 2$$

$$= 22 \cdot 22 \cdot 22 \cdot 27 \cdot 2 = 22 \cdot 80 \cdot 27 \cdot 2 \quad (*)$$

$$27^2 = (25+2)^2 = 25^2 + 4 + 100$$

$$= 729 = 707 + 22$$

$$22^2 = (20+2)^2 = 400 + 4 + 80 = 484$$

$$= 404 + 80$$

$$(*) \Rightarrow 22 \cdot 21 \cdot 27 \cdot 2 = -4$$

$$= -22.21.27.2$$

$$22.21 = 462 = 404 + 58$$

$$= -58.27.2 = -15.27 = -405$$

$$= -1$$

$$2^{30} - 1 = -2 + 101 \quad \text{so} \quad (2^{30} - 1, 101) = 1.$$

$$2^{100} \equiv 1 \pmod{101}$$

$$5^{20} = 5^{6 \cdot 3} \cdot 5 = 24^6 \cdot 5$$

$$24^2 = (25-1)^2 = 625 + 1 - 50 = -30$$

$$(24)^6 = -30^2 \cdot 30 = -900 \cdot 30 = 270 = 68$$

$$= 68 \cdot 5 = 37 \quad 5^{50} - 1 = (37, 101) = 1$$

101 es primo

First, we compute the ordered pairs $(j, 99^j \bmod 809)$ for $0 \leq j \leq 28$. We obtain the list

(0, 1)	(1, 99)	(2, 93)	(3, 308)	(4, 559)
(5, 329)	(6, 211)	(7, 664)	(8, 207)	(9, 268)
(10, 644)	(11, 654)	(12, 26)	(13, 147)	(14, 800)
(15, 727)	(16, 781)	(17, 464)	(18, 632)	(19, 275)
(20, 528)	(21, 496)	(22, 564)	(23, 15)	(24, 676)
(25, 586)	(26, 575)	(27, 295)	(28, 81)	

which is then sorted to produce L_1 .

The second list contains the ordered pairs $(i, 525 \times (3^i)^{-1} \bmod 809)$, $0 \leq j \leq 28$. It is as follows:

(0, 525)	(1, 175)	(2, 328)	(3, 379)	(4, 396)
(5, 132)	(6, 44)	(7, 554)	(8, 724)	(9, 511)
(10, 440)	(11, 686)	(12, 768)	(13, 256)	(14, 355)
(15, 388)	(16, 399)	(17, 133)	(18, 314)	(19, 644)
(20, 754)	(21, 521)	(22, 713)	(23, 777)	(24, 259)
(25, 356)	(26, 658)	(27, 489)	(28, 163)	

Exportar archi...

Crear archivo F...

Adobe PDF Pack

Convertir archivos a PDF
con otros tipos de archivo
de pago

Seleccionar archivo para c...

Selección

Editar PDF

Comentar

Combinar archivos

Rellenar y firmar

Almacene y comparta arch...

Más inform...

Una vez que sabemos que 809 es primo, ahora intentamos resolver el logaritmo con la table o un ordenador.

Pollard- ρ for factoring

Trivial which cost?

The idea is to find $x \not\equiv x' \pmod{n}$
but $x \equiv x' \pmod{p}$ then $(x-x', n) > 1$

$$\begin{array}{c} \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \end{array} \quad x_{i+1} = f(x_i)$$

if p is the length of the circle,
then $x_i \equiv x_{2i} \pmod{p} \nexists i$.

If we have p possible values
 $p < \sqrt{n}$, then $x_1, \dots, x_{n^{1/4}}$
there is a collision so take

x_1 and x_2

x_2 " x_4

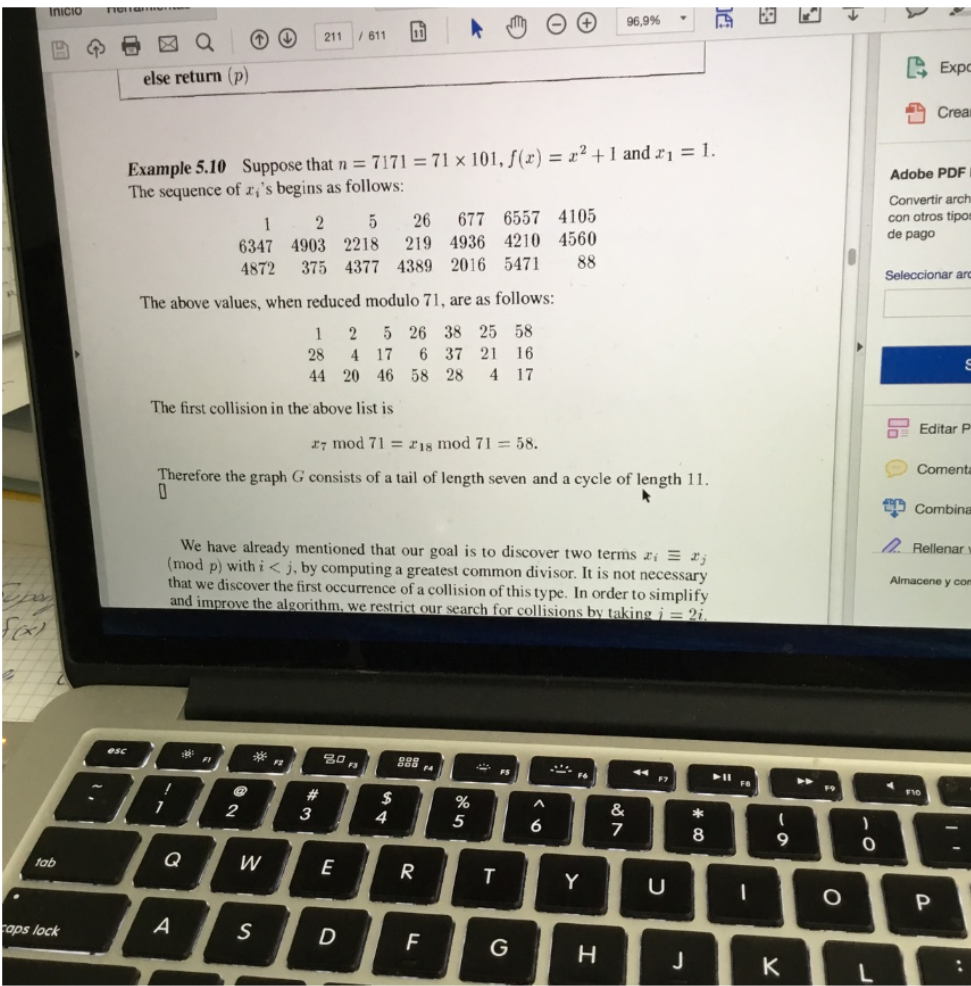
x_3 " x_6

$\vdots$

x_j " x_{2j}

and in $n^{1/4}$ we find a collision.

x_{7171} and x_{71}^2



$$88^2 \cdot 71 = 574 \bmod 7171$$

en long $x_{22} - x_{11} = 574 - 219 = 355$

$$(355, 7171) = 71$$

$$5 \times 71 = 355$$

$$71 \times 101 = 7171 \quad \square$$

For discrete logarithm $\log_{\alpha} \beta$

$$a_0 P + b_0 Q = P_0$$

$$a_1 P + b_1 Q = M_1$$

$$a_2 P + b_2 Q = M_2$$

$$a_3 P + b_3 Q = M_3$$

$$f(P) = P + M_i$$

When there is a match

$$\alpha^a \beta^b = X_0$$

$$S_1 = \alpha^{a_1} \beta^{b_1}$$

$$S_2 = \alpha^{a_2} \beta^{b_2}$$

$$S_g = \alpha^{a_g} \beta^{b_g}$$

$$f(X_0) = X_0 \cdot S_i = \alpha^{a+a_i} \beta^{b+b_i}$$

$$f(X_j) = f(X_i)$$

$$\alpha^{a_j+c b_j} \beta^{a_i+c b_i}$$



$$p = 809$$

$$\alpha = 89$$

$$\langle 89 \rangle = 101$$

$$\beta = 618$$

S_1

$$1 < x < 269$$

$$270 \leq x < 540$$

$$540 \leq x \leq 809$$

$$a_0 = 1 \quad b_0 = 1$$

$$a_1 = 2 \quad b_1 = 3 \quad a_2 = 2 \quad b_2 = 1$$

$$a_3 = 1 \quad b_3 = 2$$

$$x_0 = 89 \cdot 618 = 799$$

$$x_1 = 799 \cdot 292 = 316 \rightarrow 292 \rightarrow 618$$

$$\rightarrow 49 \cdot 113 \rightarrow 1127605$$

$$\rightarrow 298 \rightarrow 1327453$$

$$M_1 = 89^2 \cdot 618^3 = 316$$

$$\rightarrow 521 \rightarrow 676$$

$$\rightarrow 805 \rightarrow 480$$

$$M_2 = 89^2 \cdot 618 = 728$$

$$\rightarrow 764 \rightarrow 613$$

$$\rightarrow 207 \rightarrow 692$$

$$M_3 = 89 \cdot 618^2 = 292$$

$$\rightarrow 578 \rightarrow 504$$

$$\rightarrow 435 \rightarrow 361$$

$$\rightarrow 692$$

$$\left(\frac{7k}{7k}\right)^*$$

$$1.2 \ 3 \ 4 \ 5 \ 6$$

$$\alpha = 3$$

$$\beta = 4$$

$$a_0 = 1 = b_0$$

$$a_1 = 2 = b_1$$

$$a_2 = 1; b_2 = 2$$

$$a_3 = 2 \quad b_3 = 3$$

$$M_1 = 3^2 \cdot 4^2 = 4$$

$$1 \leq 2$$

$$M_2 = 3 \cdot 4^2 = 6$$

$$3 \leq 4$$

$$M_3 = 3^2 \cdot 4^3 = 2$$

$$5 \leq 1$$

$$p_0 = 5 \quad 3^3 \cdot 4^4 = p_1 = 5 \cdot 2 = 3$$

$$3^4 \cdot 4^6 = p_2 = 3 \cdot 6 = 4$$

$$3^5 \cdot 4^8 = p_3 = 3$$

$$3^5 \cdot 4^8 = 3^3 \cdot 4^4$$

$$5 + 8a = 3 + 4a \pmod{6}$$

$$4a = -2 \pmod{6}$$

$$\boxed{a = 1 \pmod{3}}$$

Index calculus $p_1 \dots p_B$

$$\left. \begin{aligned} \alpha^{a_1} &= p_1^{\alpha_{11}} \dots p_B^{\alpha_{B1}} \\ &\vdots \\ \alpha^{a_C} &= p_1^{\alpha_{1C}} \dots p_B^{\alpha_{BC}} \end{aligned} \right\} \text{ solve } \lg \alpha^i$$

the $\beta \alpha^S = p_1^{\beta_1} \dots p_B^{\beta_B}$ and solve. $\boxtimes$

Example $p = 10007$

$\alpha = 5$ $B = \{2, 3, 5, 7\}$

$$a_1 = 4063$$

$$5^{4063} = 2 \cdot 3 \cdot 7$$

$$a_2 = 5136$$

$$5^{5136} = 2 \cdot 3^3$$

$$a_3 = 9865$$

$$5^{9865} = 3^3 \cdot 7$$

$$\lg_5 9451$$

$$S = 7736 \text{ vale}$$

$$5^{4063} \bmod 10007 = 42 = 2 \times 3 \times 7.$$

This yields the congruence

$$\log_5 2 + \log_5 3 + \log_5 7 \equiv 4063 \pmod{10006}.$$

Similarly, since

$$5^{5136} \bmod 10007 = 54 = 2 \times 3^3$$

and

$$5^{9865} \bmod 10007 = 189 = 3^3 \times 7,$$

we obtain two more congruences:

$$\log_5 2 + 3 \log_5 3 \equiv 5136 \pmod{10006}$$

and

$$3 \log_5 3 + \log_5 7 \equiv 9865 \pmod{10006}.$$

We now have three congruences in three unknowns, and there happens to be a unique solution modulo 10006, namely $\log_5 2 = 6578$, $\log_5 3 = 6190$ and $\log_5 7 = 1301$.

Now, let's suppose that we wish to find $\log_5 9451$. Suppose we choose the "random" exponent $s = 7736$, and compute

$$9451 \times 5^{7736} \bmod 10007 = 8400.$$

Since $8400 = 2^4 3^1 5^2 7^1$ factors over $\mathcal{B}$, we obtain

$$\begin{aligned} \log_5 9451 &= (4 \log_5 2 + \log_5 3 + 2 \log_5 5 + \log_5 7 - s) \bmod 10006 \\ &= (4 \times 6578 + 6190 + 2 \times 1 + 1301 - 7736) \bmod 10006 \\ &= 6057. \end{aligned}$$

To verify, we can check that $5^{6057} \equiv 9451 \pmod{10007}$.

Exportar archivo

Crear archivo PDF

Adobe PDF Pack

Convertir archivos a PDF y otros tipos de archivos de pago

Seleccionar archivo para con

Seleccionar

Editar PDF

Comentar

Combinar archivos

Rellenar y firmar

Almacene y comparta archivo

Más informa

Elliptic curves

We want to find solutions to

$$x^2 + y^2 = z^2$$

• trivial

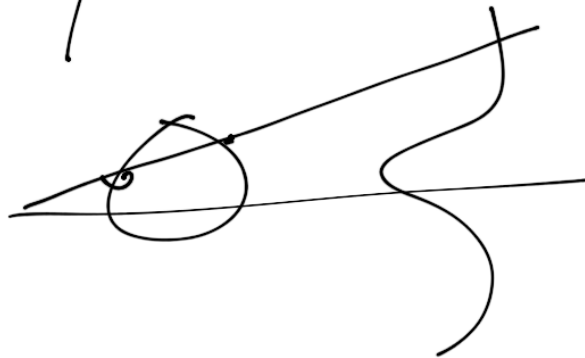
• non trivial $\Rightarrow z \neq 0 \Rightarrow$

$$x^2 + y^2 = 1$$



$$x = \frac{m^2 - n^2}{m^2 + n^2} \quad y = \frac{2mn}{m^2 + n^2}$$

Cubic equation $3z^2 + 1$



how did we make the picture?

then we need two points and
we get a group abelian.

$E_{\text{tors}}(\mathbb{Q})$ known

$$E(\mathbb{Q}) \simeq E_{\text{tors}} \oplus \mathbb{Z}^r$$

r highly unknown.

if $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ then

$$\overline{E}_p = y^2 = x^3 + \overline{a}x + \overline{b} \text{ is}$$

an elliptic curve and $\overline{E}_p(\mathbb{F}_p)$
a finite group

over the complex we take

$$P(z) = \sum_{a \in \Lambda} \left(\frac{1}{(z+a)^2} - \frac{1}{a^2} + \frac{1}{z^2} \right)$$

double periodic

$P'(z)$ also, and one can

prove

$$(P'(z))^2 = (P(z) - \omega_1)(P(z) - \omega_2)(P(z) - \omega_3)$$

An isomorphism from



so

$$E[\mathbb{C}] = \mathbb{C}/\omega_1\mathbb{C} + \mathbb{C}/\omega_2\mathbb{C}$$

$$E_q(\mathbb{F}_q) \cong \mathbb{F}_q/\omega_1\mathbb{F}_q + \mathbb{F}_q/\omega_2\mathbb{F}_q \quad e|d$$

we get many different groups by selecting only one curve.

Examples of elliptic curves in ^{Page} 259
Stinson, and we can add points

Example in Woblitz.

points over finite fields Harsh

pag 177 Woblitz.

Squir Stinson.

Birthday paradox

$$\frac{364}{365} \cdot \frac{363}{365} \dots$$

$$\prod_{j=1}^n \frac{365-j}{365} = \prod_{j=1}^n \left(1 - \frac{j}{365}\right)$$

$$\lg p = \sum_{j=1}^n \lg\left(1 - \frac{j}{365}\right) + \frac{j}{365}$$

$$\lg(1-x) \approx -x - \frac{x^2}{2}$$

$$-\frac{1}{365} \sum_{j=1}^n j \sim -\frac{n^2/2}{365}$$

$$e^{-\frac{n^2}{365}} < \frac{1}{2}$$

$$\frac{n^2}{365} > \lg 2$$

$$n > \sqrt{365 \lg 2}$$

is like the square root collision

Pollard rho.

Definition of RSA

Mis notes.

Finite fields Mobius

• Group

• Ring

• Field

irreducible, prime

$$g \mid a \mid b \quad \mathbb{Z}/n\mathbb{Z} \quad \text{evaluation}$$

$$a(b+c) = ab+ac \quad \text{integral, homo}$$

$$a^{-1} \quad \forall a \neq 0 \quad \text{contains } \mathbb{Q} \text{ or } \mathbb{F}_p$$

extension. Vector spaces

$$a(u+v) = au + av$$

$$(ab)u = a(bu)$$

$$1 \cdot u = u$$

$$(a+b)u = au + bu$$

$(V, +)$ is a group

$u = [v: \mathbb{F}]$ vector space dimension

definition of polynomials in K

$$\deg(pq) = \deg p + \deg q$$

$$q = qb + r \quad \deg r < \deg b$$

polynomials over K have deg roots

$$p(\alpha) = 0 \Leftrightarrow (x - \alpha) \mid p(x)$$

a finite field is $|\mathbb{F}| = p^r$

is a vector space over $\mathbb{F}_p$ $\square$

$$[L:W] = [L:M][M:W]$$

$$\boxed{K(x)/p(x) \sim W(\alpha)}$$

$$x \longrightarrow \{1, \alpha, \dots, \alpha^d\}$$

$$x \longrightarrow \alpha$$

$$\text{If } d(p(x)) = d \Rightarrow \mathbb{F}_p[x]/p(x) \simeq \mathbb{F}_{p^d}$$

$$| \quad | = p^d \quad \square$$

and it is a field.

$$f(x) \in K[x] \quad \exists \quad [L:K] : f(\alpha) = 0 \quad \alpha \in L$$

$$p(x) \mid f(x) \text{ irred.} \Rightarrow$$

$$K[x]/p(x) \text{ field} \quad [x] = 0$$

$$p(x) = 0 \Rightarrow f(x) = 0$$

$$f(x) \in \mathbb{F}_p[x] \text{ irreducible of degree } d =$$

$$f(x) \mid \underbrace{x^{p^d} - x}_{\text{is a field of } p^d \text{ elements}}$$

$$\mathbb{F}_{p^d} = \mathbb{F}_p[x]/f(x) \cong \mathbb{F}_p(\alpha) = \{ \alpha^d - \alpha = 0 \}$$

$$f(\alpha) = 0$$

per f is irreducible

$$\Rightarrow (f(x), x^{p^d} - x) = f(x)$$

$$N(\alpha) = \frac{1}{n} \sum_{h|h} p^{\frac{n}{h}} \mu(h)$$

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & d=1 \\ 0 & \text{others} \end{cases}$$

because is multiplicative
 and inverse formula

Construction of $\mathbb{F}_p$.

Discrete logarithm

$\beta \in \langle \alpha \rangle$ find $a: \alpha^a = \beta$

Elgamal p, α, β public a secret

$$(\alpha^w, x\beta^w)$$

$$y_2 / y_1^a = x$$

pollard-ghw, index columns