Números Inteiros e Criptografia, PLE 2020,Trabalho Final
Aluno: Luiz Rodrigo Lacé Rodrigues
DRE: 118049873

Questão 1)

n = 3 * 2^k + 1, k>1000, para base b<20, n é composto
n-1 = 3*2^k

b^(n-1) ≡/≡ 1 (mod n) para base b<20, caso fosse congruente seria contraditório com o teste de Fermat.

Logo b^(3*2^k) ≡/≡ 1 (mod n)
(b^3) ≡/≡ ± 1 (mod n),

caso b^3 ≡ ± 1 (mod n) haveria a probabilidade de n ser primo, pelo teste de Miller-Rabin

Temos então 256^1536 ≡/≡ -1 (mod n)
(2^8)^1536 ≡/≡ -1 (mod n)
(2)^12288 ≡ (2^3)^2^12 ≡/≡ -1 (mod n)

Como vimos, para base b<20 e (b^3) ≡/≡ ± 1 (mod n), logo (2^3) ≡/≡ -1 (mod n) e (2^3)^2^12 ≡/≡ -1 (mod n)

Questão 2)

Seja n um número inteiro ímpar e composto. Pelo teste de Miller-Rabin vamos ter n-1 = q * 2^k, sendo q a parte impar e k≥1. Escolhendo uma base 1<b<n-1, calculamos então b^q (mod n), caso b^q ≡ 1 mod n,nosso teste será inconclusivo e há 75% de probabilidade do número ser primo, como há também 25% de chance ser composto, chamamos ele de pseudoprimo forte para base b.
Nosso teste será inconclusivo e logo nos retornar um pseudoprimo caso b^q*(2^j) ≡ -1, para k-1 ≥ j ≥ 0

Também pode ser pseudoprimo pelo teste de Fermat quando b^n ≡ b (mod n) e logo b^(n-1) ≡ 1, com n composto.

Voltando para n pseudoprimo forte no teste de Miler-Rabin onde b^q ≡ 1 (mod n) ou b^q*(2^i) ≡ -1 vamos ter

b^n-1 ≡ (b^q)^2^k ≡ 1^(2^k) ≡ 1 mod n
b^n-1 ≡ b^((2^j) * q) ^ k-j ≡ (-1) ^(2^k-j) ≡ 1 mod n

Como temos $k > j$ então logo $k-j \geq 1$, assim (-1) ^(2^k-j) = 1. Observe que vamos chegar em b^n-1 $\equiv$ 1 mod n, que é o nosso teste de Fermat. Assim se um número n é pseudoprimo forte no Teste de Miller, então ele é pseudoprimo no Teste de Fermat.

Questão 3)

O enunciado nos diz que:
$p<q$ e ambos são primos
$n=pq$
$p-1|n-1$
$q-1|n-1$

Se pegamos $n=pq$ em $n-1$ e dividirmos por $q-1$, vamos encontrar:
$pq-1 = (q-1)p + (p-1)$
Ou seja
$pq-1 \equiv p-1 \pmod{q-1}$
$n-1 \equiv p-1 \pmod{q-1}$

Como $p-1<p<q$, então p-1 ≡/≡ 0 mod q-1, encontramos a contradição que q-1 não divide n-1, logo n não é um número de Carmichael

Segundo o Teorema de Korselt temos que: “Um inteiro positivo ímpar n é um número de Carmichael se, e somente se, cada fator primo p de n satisfaz as duas condições seguintes:

- p^2 não divide n;
- p - 1 divide n - 1;

Supomos então, sem perda de generalidade $p>q$.
Pelo Teste de Korselt vamos ter $p-1|n-1$, como $n=pq$ então $p-1|pq-1$

```
   pq-1 |p-1
 -  pq-q |----------
 --------  |q
   -1-q
```

Tendo em mente que n não pode ser um quadrado perfeito pois seria facilmente reconhecido como número composto, logo p=/=q
Vemos então que $p-1|n-1$ torna-se impossível com n ser um número de Carmichael sendo produto dois primos visto que teremos $p>q$ ou $q>p$.

4) $n=938957$

a) $\varphi(n) = 937020$

   Sabemos que:
   $\varphi(n) = (p-1)(q-1)$
   $= pq - p - q + 1$
   $= n - (p+q) + 1$
   Logo: $p+q = n + 1 - \varphi(n)$

   Para acharmos p-q e fazer um sistema, vamos dizer que:
   $(p-q)^2 = p^2 - 2pq + q^2$
   Somamos 2pq e -2pq para não mudarmos a igualdade
   $(p-q)^2 = p^2 + 2pq + q^2 -4pq$
   Como $p^2 + 2pq + q^2 = (p+q)^2$, e $n = pq$ chegamos em:
   $(p-q)^2 = (p+q)^2 - 4n$

   Substituindo os valores que temos, chegamos em:
   $p+q = 1938$
   $p-q = 4$

   Resolvendo por sistema, vamos ter $p = 971$ e $q=967$, logo $n = 967*971$

b) Como podemos encontrar a chave pública "e" sabendo que $mdc(e,\varphi(n))= 1$ e que $e*d \equiv 1 \mod \varphi(n)$, sendo d o inverso multiplicativo de "e" então temos que $mdc(d, \varphi(n)) = 1$

   Precisamos saber agora qual d que divide (970)(966) nos dá resto 1.
   Fazendo a fatoração do número (970)(966) vamos encontrar:
   2*2*3*5*7*23*97, como queremos o menor d possível, vamos pegar o próximo números primo depois de 7 que não está nessa fatoração, que é o 11.
   Como mdc(237020,11)=1,achamos então que o menor d possível pra satisfazer essa divisão é d=11

5)
a)$n=19291$

A raiz quadrada de 19291 é 138,89, ou seja $138^2<19291<139^{\wedge 2}$
Vamos fazer que $n = x^2 - y^2$
$x^2 - n = y^2$

Assim vamos testando x a partir de 139 até encontrarmos um y quadrado perfeito.
temos então que:
$139^2 - 13291 = 1932 - 19291 = 30$, como 30 não é quadrado perfeito, adicionamos 1 em x.
Fazemos isso até chegar em $146^2 - 19291 = 21316 - 19291 = 2025$,
como $2025 = 45^2$, achamos que:
$19291 = 146^2 - 45^2$
$19291 = (146 - 45)(146+45)$
$19291 = 101 * 191$

Temos então $p=101$ e $q=191$
$\varphi(n) = (p-1)(q-1)$
$\varphi(n) = (100)(190)$
$\varphi(n) = 19000$

Para acharmos nossa chave pública, precisamos que $mdc(e,\varphi(n))=1$
Como $mdc(19000,2) = 2$, vamos utilizar $mdc(19000,3) = 1$
Então nossa chave pública $e=3$

Como $e*d \equiv 1 \mod n$, nossa chave secreta d é o inverso multiplicativo de "e"
Pelo algoritmo euclidiano estendido achamos que:
$3(12667) + 19000(-2) = 1$

Então nossa chave secreta é $d=12667$

b)

Como queremos encriptar a senha 12345, vamos fazer
$c(b) = b^{\wedge}e \pmod n$, sendo b nossa senha e n,"e" nossa chaves públicas, assim:
$(12345)^3 \mod (19291)$
$(12345)^2(12345) \mod(19291)$
Como $(12345)^2 \equiv 152399025\ \ 125 \pmod{19291}$, então
$(125)(12345) \equiv 153125 \equiv 19136 \pmod{19291}\equiv$
Logo nossa mensagem encriptada é $c(12345) = 19136$

6)Pelo enunciados nos temos:

$p=3$

$q>3$

$e=3$

Nossa função para encriptar uma mensagem seria $c(b) = b^e \bmod n$.

Temos que b é invariante, então $b^e \equiv b \bmod(n)$. Logo:

$b^e \equiv b \pmod p$

$b^e \equiv b \pmod q$

Temos então:

$b^3 \equiv b \pmod 3$

$b^3 \equiv b \pmod q$

$b^3 \equiv b \pmod 3$ vamos ter 3 soluções.

$0^3 \equiv 0 \pmod 3$

$1^3 \equiv 1 \pmod 3$

$2^3 \equiv 2 \pmod 3$

Perceba que $x^3 \equiv x \pmod y$ sendo $y \neq 2$ só terá 3 soluções para qualquer primo pois $x \not\equiv 0 \pmod y$ então $x^2 \equiv 1 \pmod y$

Logo pelo teorema chines do resto, $b^3 \equiv b \pmod{3q}$ tem 9 blocos invariantes

7)

Precisamos que $mdc(e,\varphi(n)) = 1$, como temos $\varphi(n) = (p-1)(q-1)$, sendo p e q números primos, logo teremos que $\varphi(n)$ é um número par. Assim, o $mdc(2,\varphi(n)) = 2$. Logo não seria possível achar o inverso multiplicativo de "e", que é a nossa chave secreta d.

8) $x \equiv (a.q.q') + (b.p.p')$.

a) Congruente a mod p

Temos $x \equiv a*q*q' \equiv a$

Sabendo que $q*q' \equiv 1$, visto que um é o inverso multiplicativo do outro.

E $b*q*q' \equiv 0 \bmod p$.

Congruente a mod q

Temos novamente que $p*p' \equiv 1$, mas agora $a*p*p' \equiv 0$

Temos então que $x \equiv a \pmod p$ e $x \equiv b \pmod q$

Nossa solução “n” atende a nossa expectativa mas ainda falta mostrar que é uma solução unica. Vamos supor que existam outras soluções, na qual não houvessem tais congruências. Vamos começar dizendo que $n \not\equiv y$

$n \equiv A \pmod p$
$Y \equiv A \pmod p$
$n - Y \equiv 0 \pmod p$
$p \mid n - Y$

$n \equiv A \pmod q$
$Y \equiv A \pmod q$
$n - Y \equiv 0 \pmod q$
$q \mid n - Y$

Sabendo que p e q são primos e dividem n - Y ($p \mid n - Y$ e $q \mid n - Y$),
logo $p*q \mid n - Y$ e $(n - Y) \equiv \pmod{pq}$. Perceba que temos $n \equiv Y \bmod (pq)$, o que é um falso visto que começamos supondo que n e Y não eram congruentes.

b) Do enunciado podemos tirar que o sistema possui uma única solução n, e que é dada por $x \equiv (a1*q1*q1') + (a2*q2*q2') + \ldots + (ak*qk*qk')$.
Sabendo que $q1 = Q2*Q3*...*QK$, $q2 = Q1*Q3*...*Qk$ até $qk= Q1*Q2*Q(k-1)$.

Vamos escrever a solução como $x \equiv (a1*q1*q1') + (a2*q2*q2')$ em relação a mod p

- mod p1
  $x \equiv (a1*q1*q1') \equiv a1$
  Sabendo que $(a2*q2*q2') \equiv 0 \bmod p1$ e $(ak*qk*qk') \equiv 0 \bmod p1$. Visto que temos $q1*q1 \equiv 1$,por serem inversos multiplicativos.

- mod p2
  $x \equiv (a2*q2*q2') \equiv a2$
  Como:
  $(a1*q1*q1') \equiv 0 \bmod p2$
  $(ak*qk*qk') \equiv 0 \bmod p2$
  Visto que $q2*q2' \equiv 1$

- mod pk
  $x \equiv (ak*qk*qk') \equiv ak$
  Como:
  $(a1*p1*p1') \equiv 0$
  $(a2*p2*p2') \equiv 0$
  $pk*pk' \equiv 1$

Assim como na letra a), vamos agora mostrar que tais soluções são únicas e provar isso supondo que existam outras soluções das quais não são congruentes a solução n, e assim, demonstrar um absurdo.
Vamos começar supondo que n ≡/≡ Y

n ≡ a1 (mod p1)
Y ≡ a1(mod p1)
n - Y ≡ 0 (mod p1)
p1 | n-Y

n ≡ a2(mod p2)
Y ≡ a2(mod p2)
n - Y ≡ 0 (mod p2)
p2 | n - Y

n ≡ ak (mod pk)
Y ≡ ak (mod pk)
n - y ≡ 0 (mod pk)
pk | n - Y

Como temos p1,p2 até pk coprimos, temos que o produtório entre eles divide n-Y. Como (p1*p2*...*pk) | n - Y ≡ 0 (mod p1*p2*...*pk) e n ≡ Y mod(p1*p2*...*pk). Como supomos no início que n e y não eram congruentes, essa congruência se demonstra falsa.

Assim temos que existe apenas uma única solução.

10) n = 7597, e = 4947, Φ = 7420

Primeiro temos que achar a nossa chave secreta d para decriptar as mensagens. Como d é o inverso multiplicativo de e mod(Φ), calculamos e*d ≡ 1 (mod Φ)

4947*d ≡ 1 (mod 7420)
Através do Algoritmo euclidiano estendido encontramos:
4947(3) + 7420(-2) = 1
Logo temos que d = 3

Podemos começar a decriptar nossa mensagem: tendo em vista que uma função para encriptar a mensagem como c(b) = b^e(mod n), sendo e b a nossa mensagem. Para decriptar vamos precisar de uma função que D(c(b)) = b, essa função será (c(b))^d ≡ b (mod n)

$(6803)^3 \equiv (6803)^2(6803) \equiv (46280809)(6803) \equiv (7482)(6803) \equiv 50900046 \equiv 146 \pmod{7597}$

$(205)^3 \equiv (42025)(205) \equiv (4040)(205) \equiv 828200 \equiv 127 \pmod{7597}$

$(1126)^3 \equiv (1267876)(1126) \equiv (6774)(1126) \equiv 7627524 \equiv 136 \pmod{7597}$

$(1421)^3 \equiv (2019241)(1421) \equiv (6036)(1421) \equiv 8577156 \equiv 143 \pmod{7597}$

$(1658)^3 \equiv (2748964)(1658) \equiv (6447)(1658) \equiv 10689126 \equiv 147 \pmod{7597}$

Utilizando a tabela no final da lista pra traduzir os números, temos que a mensagem é “raios”

11)

Temos e,n e d. Queremos encontrar as chave p e q

Sabendo que $e*d \equiv 1 \mod \Phi$ e que $mdc(e,\Phi) = mdc(d,\Phi) = 1$, conseguimos encontrar um Φ.

Sabemos que:

$\varphi(n) = (p-1)(q-1)$
$= pq - p - q + 1$
$= n - (p+q) + 1$

Logo: $p+q = n + 1 - \varphi(n) =$ soma

Para acharmos p-q e fazer um sistema, vamos dizer que:

$(p-q)^2 = p^2 - 2pq + q^2$

Somamos 2pq e -2pq para não mudarmos a igualdade

$(p-q)^2 = p^2 + 2pq + q^2 -4pq$

Como $p^2 + 2pq + q^2 = (p+q)^2$, e $n = pq$ chegamos em:

$(p-q)^2 = (p+q)^2 - 4n$

$p-q= ((p+q)^2 - 4n)^{(1/2)} =$ subtração

Assim podemos fazer um sistema onde:

p = soma/2

q = subtração/2

E assim encontramos as chaves p e q