Maela Nguegang

CSC 333

HW6

Marcus Schaefer

1. (Reading) Done.

2. (Three Pass Protocol Break, 10pt)

$A \to B$: $C_1 = m^a (p)$
$= 28815377349986238948$

$B \to A$: $C_2 = C_1^b (p) \Rightarrow (m^a)^b \ (p)$
$= 32022638409929718780$

$A \to B$: $C_3 = C_2^{a^{-1}(p-1)} (p) \Rightarrow (m^{ab})^{a^{-1}} (p)$
$= 14438564975318228697$

B : $C_3^{b^{-1}(p-1)} (p)$

$p = 91246234312872996521$
$a^*b \ (p) = 52989123124449843069$

Find m;

- knowing a^*b (p) helps find the inverse of a and b to respect to p-1

- From C_3 : $(m^{ab})^{a^{-1}}$
$\Rightarrow C_3 = m^b \ (p)$
$= 14438564975318228697$

we know
- $m = b^{-1} \bmod (p-1)$

From C_2;
$(m^a)^b = (m^b)^a \ (p)$
$= 32022638409929718780$

Using Extended Euclidean;

$x = ab \bmod (p-1) = 52989123124449843069$

we know

$r = p-1$

$= 9124623431287299652 0$

We use, $ab \cdot b^{-1} \equiv 1 \ (p-1)$

$b^{-1}(p-1) = 4093063657970322334 9$

Then $m = (m^b)^{b^{-1}} \mod p$

$m = 6719934502754493897 3$

3. (Chinese Remainder Theorem, 10pt)

(a)

$x = \overset{a}{211}(\overset{m}{2438})$

$x = \overset{b}{3304}(\overset{n}{4247})$

$x = atn + bsm$

we know

$tn = 1 \ (m)$

$sm = 1 \ (n)$

- $t(4247) = 1 \ (2438)$
  $= 4247 \times 1469 = 1 \ (2438)$
  $t = 1469$
- $s(2438) = 1 \ (4247)$
  $= 2438 \times 1688 = 1 \ (4247)$
  $s = 1688$

$x = 211 \times 1469 \times 4247 + 3304 \times 1688 \times 2438$

$= 14913492449$

Reduced modulo

$mn = 2438 \times 4247$

$= 10354186$

This implies, $x = 14913424449 \mod 10354186$

$= 3464609 \ (2438 \cdot 4247)$

(b)

$$x = \overset{a}{211}\ (\overset{w}{2438})$$

$$x = \overset{b}{3304}\ (\overset{y}{4247})$$

$$x = \overset{c}{6614}\ (\overset{z}{7123})$$

we know,

$m = yz \qquad t_1 = m\ (w)$

$n = wz \qquad t_2 = n\ (y)$

$o = wy \qquad t_3 = o\ (z)$

$$x = a t_1 m + b t_2 n + c t_3 o$$

Inverse;

t_1 of $m = 4247 \times 7123\ (2438)$
$= \underline{605}$

t_2 of $n = 2438 \times 7123\ (4247)$
$= \underline{1052}$

t_3 of $o = 2438 \times 4247\ (7123)$
$= \underline{3591}$

Implies;

$$x = 211 \times 605 \times 4247 \times 7123 + 3304 \times 1052 \times 2438 \times 7123 + 6614 \times 3591 \times 2438 \times 4247$$

$$x = 310143150876311$$

Reduce $wyz = 2438 \times 4247 \times 7123$
$= 73752866878$

This implies, $x = 310143150876311 \bmod 73752866878$
$= \underline{\underline{12345654321}}\ (2438 \cdot 4247 \cdot 7123)$

4. (RSA, 10pt)

$(p,q) = (55606958372756897517320 9, 87197861593638608184613 9)$

(a)

(p,q) = (55606958372756897517320 9, 87197861593638608184613 9)
n = p*q
n
484880785998242252005536361908755725678801289005 1
phi = (p-1)*(q-1)
phi
484880785998242252005535434323181389283295587070 4

e = 65537
gcd(e, phi)
1
d = invm(e, phi)
d
401935297315112205051386514564919849157030624886 5

(b)

$m = 122333221$
private key: (d, n)

= (401935297315112205051386514564919849157030624886 5,
484880785998242252005536361908755725678801289005 1)

Public key: (e, n)
=
(65537, 484880785998242252005536361908755725678801289005 1)

Bob → Alice:

$c = m^e (n)$

= 122333221^65537 mod484880785998242252005536361908755725678801289005 1
= 220922577707289073220281121173254002900191972769

Alice:

$$c^d (n) = m$$

=220922577707289073220281121173254002900191972769^4019352973151122050513865145649198491570306248865 mod4848807859982422520055363619087557256788012890051

=122333221

It equals to the same initial key

(c)

Private key: (d, n)

(4019352973151122050513865145649198491570306248865, 4848807859982422520055363619087557256788012890051)

Alice:

$m = 12233321$

$c = m^d (n)$

=122333221^4019352973151122050513865145649198491570306248865 mod4848807859982422520055363619087557256788012890051

= 4406658234538529208177598293845607936264044227295

Bob:

$$c^e (n) = m$$

=4406658234538529208177598293845607936264044227295^65537 mod4848807859982422520055363619087557256788012890051

= 122333221

5. (RSA, 10pt)

Alice public key (e, n):

(e,n) = (394058113086737919967103259422666606189656289102784347215, 7901107608096742141879264256080447840284062885233414253141)

Bob → Alice : ct (Encrypted with Alice Key)

ct = 1888257822447033573882271583151633190707799727592736107956

Alice $\phi(n)$:

phi(n) = 7901107608096742141879264255548389501438834362193040084384 .

1. Find m;

We know

$$c = m^e (n)$$

Also

$$c^d (n) = m$$

Implies $(m^e)^d (n) = m^{ed} (n)$

$$= m^1 (n)$$

$$= m (n)$$

$$ed = 1 (\phi(n))$$

Therefore

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

d = invm(e,phiA)
d
5208431303890053374159037666212862196827913167366525614191

$$m = c^d (n)$$

=1888257822447033573882271583151633190707799727592736107956^790110760809674214187
9264256080447840284062885233414253141
mod5208431303890053374159037666212862196827913167366525614191
m = 889572428773514750203798870141236539835633308007507381732

2.

$$x^2 - (n - \phi(n) + 1)x + n = 0$$

We know n and $\phi(n)$

n = 7901107608096742141879264256080447840284062885233414253141
phi(n) = 7901107608096742141879264255548389501438834362193040084384

Using the formular

$$x = \frac{n - \phi(n) + 1}{2} \pm \sqrt{\left(\frac{n - \phi(n) + 1}{2}\right)^2 - n}$$

(n - phi(n) + 1 / 2):
7901107608096742141879264256080447840284062885233414253141 -
7901107608096742141879264255548389501438834362193040084384 + 1/2
=532058338845228523040374168758/2
n - phi(n) + 1 /2) = 266029169422614261520187084379

(n - phi(n) + 1 / 2))^2
(266029169422614261520187084379)^2
=70771518983686002778130907604009583865746060592724865815641

(n - phi(n) + 1 / 2))^2 - n
70771518983686002778130907604009583865746060592724865815641 -
7901107608096742141879264256080447840284062885233414253141
n = 62870411375589260636251643347929136025461997707491451562500

Sqrt[(n - phi(n) + 1 / 2))^2 - n]
=Sqrt[62870411375589260636251643347929136025461997707491451562500]
=250739728355099843831201221250

Values of p and q

x = 266029169422614261520187084379 + 250739728355099843831201221250
x = 516768897777141053513888305629

x = 266029169422614261520187084379 - 250739728355099843831201221250
x = 15289441067514417688985863129

Test pxq = n

516768897777714105351388305629 x 15289441067514417688985863129 =

7901107608096742141879264256080447840284062885233414253141