Group 2: Kyle, Jesus, Ying, Mason, Connor, Gage, Adam

Homework6 – Group 2

3.8

A) N = pq = 352717 and (p - 1) (q - 1) = 351520

Using (3.5) to compute,

(p + q) = N + 1 - (p - 1) (q - 1)

(p + q) = 352718 - 351520

p + q) = 1198

X^2 - (p + q)X + N = X^2 - 1198 X + 352717

= (X - 677) (X - 521)

This gives the factorization N = 352717 = 677, 521

B) N = pq = 77083921 and (p - 1) (q - 1) = 77066212

Using (3.5) to compute,

(p + q) = N + 1 - (p - 1) (q - 1)

(p + q) = 77083922 - 77066212

(p + q) = 17710

X^2 - (p + q)X + N = X^2 - 17710 X + 77083921

= (X - 10007) (X - 7703)

This gives the factorization N = 77083921 = 10007, 7703

C) N = pq = 109404161 and (p - 1) (q - 1) = 109380612

Using (3.5) to compute,

(p + q) = N + 1 - (p - 1) (q - 1)

(p + q) = 109404162 - 109380612

(p + q) = 23550

X^2 - (p + q)X + N = X^2 - 23550 X + 109404161

= (X - 17183) (X - 6367)

This gives the factorization N = 109404161 = 17183, 6367

D) N = pq = 172205490419 and (p - 1) (q - 1) = 172204660344

Group 2: Kyle, Jesus, Ying, Mason, Connor, Gage, Adam

Using (3.5) to compute,

(p + q) = N + 1 - (p - 1) (q - 1)

(p + q) = 172205490420 - 172204660344

(p + q) = 830076

X^2 - (p + q)X + N = X^2 - 830075 X + 172205490419

= (X - 422183) (X - 407893)

This gives the factorization N = 352717 = 422183, 4078

3.12

Group 2: Kyle, Jesus, Ying, Mason, Connor, Gage, Adam

$\because C_1 \equiv M^{e_1} \bmod N$

$C_2 \equiv M^{e_2} \bmod N$

$\because \gcd(e_1, e_2) = 1$

$\therefore e_1 x + e_2 y = 1$

$C_1^x C_2^y = M^{e_1 x + e_2 y} \bmod$

$C_1^x C_2^y \equiv M \bmod N$

$x = 252426389$

$y = -496549570$

$(C_1^x * C_2^y) \bmod N = (m') \bmod N$

$\because m < N$

$\therefore (C_1^x * C_2^y) \bmod N = m$

$C_1^x \bmod N = 1031756109$

$C_2^y \bmod N = 603385073 \quad (C_2^x \bmod N) = ((C_2^{-1})^{-x} \bmod N)$

$m = (C_1^x \bmod N * C_2^y \bmod N) \bmod N$

$m = 1054592380$

3.14

a) $n = 1105$

$n - 1 = 2^4 * 69$

Let a = 10

$10^{69}\ (mod\ 1105) \equiv 805$

$10^{69^2}\ (mod\ 1105) \equiv 495$

$10^{69^4}\ (mod\ 1105) \equiv 560$

$10^{69^5}\ (mod\ 1105) \equiv 885$

Since none of these congruencies equals 1 or -1 10 is a Miller-Rabin witness for 1105 and 1105 is composite by the MRT.

b) $n = 294409$

$n - 1 = 2^3 * 36801$

Let a = 69

$69^{36801}\ (mod\ 294409) \equiv 32776$

$69^{36801^2}\ (mod\ 294409) \equiv 262144$

$69^{36801^3}\ (mod\ 294409) \equiv 1$

Since $69^{36801^3}\ (mod\ 294409) \equiv 1$, by the MRT 69 is a witness for 294409 and 294409 is composite.

c) The book had b and c as the same n.

d) $n = 118901509$

$n - 1 = 2^2 * 29725377$

Let a = 2

$2^{29725377}\ (mod\ 118901509) \equiv 7906806$

$2^{29725377}\ (mod\ 118901509) \equiv -1$

Let a = 3

$3^{29725377}\ (mod\ 118901509) \equiv -1$

Let a = 5

$5^{29725377}\ (mod\ 118901509) \equiv -1$

Let a = 7

$7^{29725377}\ (mod\ 118901509) \equiv 7906806$

$7^{297253^277}\ (mod\ 118901509) \equiv -1$

Let a = 11

$11^{29725377}\ (mod\ 118901509)\ \equiv -1$

Let a = 13

$13^{29725377}\ (mod\ 118901509)\ \equiv 1$

Let a = 17

$17^{29725377}\ (mod\ 118901509)\ \equiv 7906806$

$17^{29725377^2}\ (mod\ 118901509)\ \equiv -1$

Let a = 19

$19^{29725377}\ (mod\ 118901509)\ \equiv 110994703$

$19^{29725377^2}\ (mod\ 118901509)\ \equiv -1$

Let a = 23

$23^{29725377}\ (mod\ 118901509)\ \equiv 7906806$

$23^{29725377^2}\ (mod\ 118901509)\ \equiv -1$

Let a = 29

$29^{29725377}\ (mod\ 118901509)\ \equiv 1$

Thus, by the MRT 118901509 is probably prime.

e) $n = 118301521$

$n - 1 = \ 2^4 * 7431345$

Let a = 82

$82^{7431345}\ (mod\ 118301521)\ \equiv 4527074$

$82^{7431345^2}\ (mod\ 118301521)\ \equiv 1758249$

$82^{7431345^3}\ (mod\ 118301521)\ \equiv 1$

Since $82^{7431345^3}\ (mod\ 118301521)\ \equiv 1$, by the MRT 82 is a witness for 118301521 and 118301521 is composite.

f) $n = 118901527$

$n - 1 = 2^1 * 59450763$

Let a = 2

$2^{59450763}\ (mod\ 118901527)\ \equiv 1$

Let a = 3

$3^{59450763}\ (mod\ 118901527)\ \equiv -1$

Let a = 5

$2^{59450763}\ (mod\ 118901527)\ \equiv -1$

Let a = 7

$2^{59450763}\ (mod\ 118901527)\ \equiv 1$

Let a = 11

$2^{59450763}\ (mod\ 118901527)\ \equiv 1$

Let a = 13

$2^{59450763}\ (mod\ 118901527)\ \equiv 1$

Let a = 17

$2^{59450763}\ (mod\ 118901527)\ \equiv 1$

Let a = 19

$2^{59450763}\ (mod\ 118901527)\ \equiv 1$

Group 2: Kyle, Jesus, Ying, Mason, Connor, Gage, Adam

Let a = 23

$2^{59450763}\ (mod\ 118901527)\ \equiv 1$

Let a = 29

$2^{59450763}\ (mod\ 118901527)\ \equiv -1$

Thus, by the MRT 118901527 is probably prime.

g) $n = 118915387$

$n - 1 = \ 2^1 * 59457693$

Let a = 2

$2^{59457693}\ (mod\ 118915387)\ \equiv 113834375$

$2^{594576932^{2}}\ (mod\ 118915387)\ \equiv 33511057$

$2^{594576932^{3}}\ (mod\ 118915387)\ \equiv 46684018$

$2^{594576932^{4}}\ (mod\ 118915387)\ \equiv 40120772$

$2^{594576932^{5}}\ (mod\ 118915387)\ \equiv 90181692$

Since none of these congruencies equals 1 or -1 2 is a Miller-Rabin witness for 118915387 and 118915387 is composite by the MRT.

3.21

a) n = 1739

$2^{2!} - 1 = 3$ (mod 1739)	GCD(3, 1739) = 1
$2^{3!} - 1 = 63$ (mod 1739)	GCD(63, 1739) = 1
$2^{4!} - 1 = 1082$ (mod 1739)	GCD(1082, 1739) = 1
$2^{5!} - 1 = 1394$ (mod 1739)	GCD(1394, 1739) = 1
$2^{6!} - 1 = 1443$ (mod 1739)	GCD(1443, 1739) = 37

1739 / 37 = 47

$(37 - 1) = 36 = 2^2 * 3^3$

Factors are 37 and 47, 37 has the property that p – 1 is a product of small primes

Group 2: Kyle, Jesus, Ying, Mason, Connor, Gage, Adam

b) n = 220459

$2^{2!} - 1 = 3 \pmod{220459}$	GCD(3, 220459) = 1
$2^{3!} - 1 = 63 \pmod{220459}$	GCD(63, 220459) = 1
$2^{4!} - 1 = 22331 \pmod{220459}$	GCD(22331, 220459) = 1
$2^{5!} - 1 = 85053 \pmod{220459}$	GCD(85053, 220459) = 1
$2^{6!} - 1 = 4045 \pmod{220459}$	GCD(4045, 220459) = 1
$2^{7!} - 1 = 43102 \pmod{220459}$	GCD(43102, 220459) = 1
$2^{8!} - 1 = 179600 \pmod{220459}$	GCD(179600, 220459) = 449

220459 / 449 = 491

$(449 - 1) = 448 = 2^6 * 7$

Factors are 449 and 491, 449 has the property that p – 1 is a product of small primes

c) n = 48356747

$2^{2!} - 1 = 3 \pmod{220459}$	GCD(3, 48356747) = 1
$2^{3!} - 1 = 63 \pmod{220459}$	GCD(63, 48356747) = 1
$2^{4!} - 1 = 16777215 \pmod{220459}$	GCD(16777215, 48356747) = 1
$2^{5!} - 1 = 29007255 \pmod{220459}$	GCD(29007255, 48356747) = 1
$2^{6!} - 1 = 6497325 \pmod{220459}$	GCD(6497325, 48356747) = 1
$2^{7!} - 1 = 11540769 \pmod{220459}$	GCD(11540769, 48356747) = 1
$2^{8!} - 1 = 13320679 \pmod{220459}$	GCD(13320679, 48356747) = 1
$2^{9!} - 1 = 2119446 \pmod{220459}$	GCD(2119446, 48356747) = 1
$2^{10!} - 1 = 32129513 \pmod{220459}$	GCD(32129513, 48356747) = 1
$2^{11!} - 1 = 4931911 \pmod{220459}$	GCD(4931911, 48356747) = 1
$2^{12!} - 1 = 35410323 \pmod{220459}$	GCD(35410323, 48356747) = 1
$2^{13!} - 1 = 46845550 \pmod{220459}$	GCD(46845550, 48356747) = 1
$2^{14!} - 1 = 45774460 \pmod{220459}$	GCD(45774460, 48356747) = 1
$2^{15!} - 1 = 46983890 \pmod{220459}$	GCD(46983890, 48356747) = 1
$2^{16!} - 1 = 8398520 \pmod{220459}$	GCD(8398520, 48356747) = 1
$2^{17!} - 1 = 9367159 \pmod{220459}$	GCD(9367159, 48356747) = 1
$2^{18!} - 1 = 17907955 \pmod{220459}$	GCD(17907955, 48356747) = 1
$2^{19!} - 1 = 13944672 \pmod{220459}$	GCD(13944672, 48356747) = 6917

48356747 / 6917 = 6991

$(6917 - 1) = 6916 = 2^2 * 7 * 13 * 19$

Factors are 6917 and 6991, 6917 has the property that p – 1 is a factor of small primes

Group 2: Kyle, Jesus, Ying, Mason, Connor, Gage, Adam

3.25

a.) N = 61063

1882^2 = 270 mod 61063 and 270 = 2 * 3^3 * 5

1898^2 = 60750 mod 61063 and 60750 = 2 * 3^5 * 5^3

So,

1882^2 * 1898^2 = (2 * 3^3 * 5) (2 * 3^5 * 5^3) = (2 * 3^4 *5^2)^2 = (4050)^2 mod 61063 ← 4050 = b

And,

1882 * 1898 = 3572036 = 30,382 mod 61063 ←30,382 = a

GCD(N, a-b) = GCD(61063, (30,382 – 4,050)) = GCD(61063, 26332) = **227**

b.) N = 52907

339^2 = 480 mod 52907 = 2^5 * 3 * 5

763^2 = 192 mod 52907 = 2^6 * 3

773^2 = 52907 mod 52907 = 2^6 * 3^5

976^2 = 250 mod 52907 = 2 * 5^3

So, 339^2 *763^2*773^2*976^2 = (2^5 * 3 * 5)(2^6 * 3)(2^6 * 3^5)(2 * 5^3) = 2^18 * 3^7 *5^4 however this is not a power of 2 so we have to find a new combo. This combo is:

339^2*773^2*976^2 = (2^5 * 3 * 5)(2^6 * 3^5)(2 * 5^3) = 2^12 * 3^6 *5^4 = (2^6 * 3^3 * 5^2)^2 = 43200^2 ← 43200 = b

And,

339 * 773 * 976 = 301024752 = 36829 mod 52907 ← 36829 = a

GCD(N, b- a) = GCD(52907, (43200, 36829)) = GCD(52907, 6371) = **277**

c.) N = 198103

1189^2 = 27000 mod 198103 = 2^5 * 3 * 5

1605^2 = 27000 mod 198103 = 2 * 7^3

2378^2 = 108000 mod 198103 = 2^5 * 3^3 * 5^3

2815^ 2 = 105 mod 198103 = 3 * 5 * 7

So,

Group 2: Kyle, Jesus, Ying, Mason, Connor, Gage, Adam

$1189^2 * 1605^2 * 2378^2 * 2815^2 = (2^5 * 3 * 5)(2 * 7^3)(2^5 * 3^3 * 5^3)(3 * 5 * 7)$

$= 2^3 * 3^2 * 5^2 * 7^2$ however this is not a power of two so another combination so I find a new combination which is:

$1605^2 * 2378^2 * 2815^2 = (2 * 7^3)(2^5 * 3^3 * 5^3)(3 * 5 * 7) = (2^6 * 3^4 * 5^4 * 7^4) = (2^3 * 3^2 * 5^2 * 7^2)^2 = (88200)^2 \bmod 198103 \leftarrow b$

So,

$1605 * 2378 * 2815 \bmod 198103 = 64248 \leftarrow a$

$GCD(N, b - a) = GCD(198103, (88200 - 64248)) = GCD(198103, 23952) = 499$

d.) $N = 2525891$

$1591^2 = 5390 \bmod 2525891 = 2 * 5 * 7^2 * 11$

$3182^2 = 21560 \bmod 2525891 = 2^3 * 5 * 7^2 * 11$

$4773^2 = 48150 \bmod 2525891 = 2 * 3^2 * 5 * 7^2 * 11$

$5275^2 = 40824 \bmod 2525891 = 2^3 * 3^6 * 7$

$5401^2 = 13860000 \bmod 2525891 = 2^4 * 3^2 * 5^3 * 7 * 11$

$1591^2 * 3182^2 * 4773^2 * 5275^2 * 5401^2 = (2 * 5 * 7^2 * 11)(=2^3 * 5 * 7^2 * 11)(2 * 3^2 * 5 * 7^2 * 11)(2^3 * 3^6 * 7)(2^4 * 3^2 * 5^3 * 7 * 11) = (2^6 * 3^4 \text{ \^{} } 5^3 * 7^4 * 11^2)^2 = (18825760800)^2$

So,

$1591 * 3182 * 4773 * 5275 * 5401 = 739064$

$GCD(N, b - a) = GCD(2525891, 18825686936) = 1$