Exercise on Implementing RSA: Group A

As a group create a series of spreadsheets for implementing the techniques we have learned so far. You will use the following public keys for encrypting messages.

Team	Mike	A	B	C	D
m	4417571	3815969	78112883	44938309	65445929
k	101	101	107	77	107

You are Group A, and your value of m factors as

$$m = pq, \qquad p = 16301, \quad q = 271.$$

(The numbers p and q are primes.)

Use the following table for converting from letters to numbers

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	21	22	23	24
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
25	26	27	28	29	31	32	33	34	35	36	37	38

(a) Create a spreadsheet that will implement the Euclidean algorithm. Try to set it up so that it will find solutions to

$$ax + by = \gcd(a, b)$$

for a given input (a, b).

(b) Use your spreadsheet from part (b) to find a solution to the equation

$$ku - \phi(m)v = 1$$

for *your* public key; you are Group A. (Remember that your solution must have $u > 0$.) Recall that if $m = pq$ is a product of distinct primes then

$$\phi(m) = \phi(p)\phi(q) = (p-1)(q-1).$$

(c) Find the binary expansion of the value of u you found in part (a).

(d) Create a spreadsheet that will make a table of successive squares $a^{2^j} \pmod m$.

(e) Using *your* public key, I have created the following encrypted message:

$$b_1 = 3685682, \quad b_2 = 173200, \quad b_3 = 380465, \quad b_4 = 2942389, \quad b_5 = 2215525$$

Use your spreadsheet from part (d) to decrypt the code. (Recall, this means you calculate $b_i^u \pmod m$ for the values of b_i above, *your* value of m and the u you found in part (a).)

(f) Find the binary expansion of the value $k = 101$ (this is the k from *my* public key).

(g) Use *my* public key $(m, k) = (4417571, 101)$ to encrypt a short (about 1 sentence long) message to send me. (This means you need to convert your message to numbers using the scheme above, and then break it up into a sequence of numbers $a_1, a_2, \ldots$ each smaller than $m = 4417571$. Now calculate $a_i^{101} \pmod{4417571}$ for $i = 1, 2, \ldots$. Give me your results.

(h) Repeat parts (f) and (g) using the public key from Group B and give the encrypted message to them.

(i) Once you receive an encrypted code from Group D, decrypt it using your public key. (In other words, repeat what you did in part (e) with the new sequence of numbers.)

Exercise on Implementing RSA: Group B

As a group create a series of spreadsheets for implementing the techniques we have learned so far. You will use the following public keys for encrypting messages.

Team	Mike	A	B	C	D
m	4417571	3815969	78112883	44938309	65445929
k	101	101	107	77	107

You are Group B, and your value of m factors as

$$m = pq, \qquad p = 37, \quad q = 2111159.$$

(The numbers p and q are primes.)

Use the following table for converting from letters to numbers

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	21	22	23	24
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
25	26	27	28	29	31	32	33	34	35	36	37	38

(a) Create a spreadsheet that will implement the Euclidean algorithm. Try to set it up so that it will find solutions to

$$ax + by = \gcd(a, b)$$

for a given input (a, b).

(b) Use your spreadsheet from part (b) to find a solution to the equation

$$ku - \phi(m)v = 1$$

for *your* public key; you are Group B. (Remember that your solution must have $u > 0$.) Recall that if $m = pq$ is a product of distinct primes then

$$\phi(m) = \phi(p)\phi(q) = (p-1)(q-1).$$

(c) Find the binary expansion of the value of u you found in part (a).

(d) Create a spreadsheet that will make a table of successive squares $a^{2^j} \pmod m$.

(e) Using *your* public key, I have created the following encrypted message:

$$b_1 = 41985523, \quad b_2 = 67851544, \quad b_3 = 30387266, \quad b_4 = 42359611, \quad b_5 = 7965343$$

Use your spreadsheet from part (d) to decrypt the code. (Recall, this means you calculate $b_i^u \pmod m$ for the values of b_i above, *your* value of m and the u you found in part (a).)

(f) Find the binary expansion of the value $k = 101$ (this is the k from *my* public key).

(g) Use *my* public key $(m, k) = (4417571, 101)$ to encrypt a short (about 1 sentence long) message to send me. (This means you need to convert your message to numbers using the scheme above, and then break it up into a sequence of numbers $a_1, a_2, \ldots$ each smaller than $m = 4417571$. Now calculate $a_i^{101} \pmod{4417571}$ for $i = 1, 2, \ldots$. Give me your results.

(h) Repeat parts (f) and (g) using the public key from Group C and give the encrypted message to them.

(i) Once you receive an encrypted code from Group A, decrypt it using your public key. (In other words, repeat what you did in part (e) with the new sequence of numbers.)

Exercise on Implementing RSA: Group C

As a group create a series of spreadsheets for implementing the techniques we have learned so far. You will use the following public keys for encrypting messages.

Team	Mike	A	B	C	D
m	4417571	3815969	78112883	44938309	65445929
k	101	101	107	77	107

You are Group C, and your value of m factors as

$$m = pq, \qquad p = 13, \quad q = 3456793.$$

(The numbers p and q are primes.)

Use the following table for converting from letters to numbers

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	21	22	23	24
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
25	26	27	28	29	31	32	33	34	35	36	37	38

(a) Create a spreadsheet that will implement the Euclidean algorithm. Try to set it up so that it will find solutions to

$$ax + by = \gcd(a, b)$$

for a given input (a, b).

(b) Use your spreadsheet from part (b) to find a solution to the equation

$$ku - \phi(m)v = 1$$

for *your* public key; you are Group C. (Remember that your solution must have $u > 0$.) Recall that if $m = pq$ is a product of distinct primes then

$$\phi(m) = \phi(p)\phi(q) = (p-1)(q-1).$$

(c) Find the binary expansion of the value of u you found in part (a).

(d) Create a spreadsheet that will make a table of successive squares $a^{2^j} \pmod m$.

(e) Using *your* public key, I have created the following encrypted message:

$$b_1 = 9258973, \quad b_2 = 30020225, \quad b_3 = 6250561, \quad b_4 = 36824565, \quad b_5 = 31724353$$

Use your spreadsheet from part (d) to decrypt the code. (Recall, this means you calculate $b_i^u \pmod m$ for the values of b_i above, *your* value of m and the u you found in part (a).)

(f) Find the binary expansion of the value $k = 101$ (this is the k from *my* public key).

(g) Use *my* public key $(m, k) = (4417571, 101)$ to encrypt a short (about 1 sentence long) message to send me. (This means you need to convert your message to numbers using the scheme above, and then break it up into a sequence of numbers $a_1, a_2, \ldots$ each smaller than $m = 4417571$. Now calculate $a_i^{101} \pmod{4417571}$ for $i = 1, 2, \ldots$. Give me your results.

(h) Repeat parts (f) and (g) using the public key from Group D and give the encrypted message to them.

(i) Once you receive an encrypted code from Group B, decrypt it using your public key. (In other words, repeat what you did in part (e) with the new sequence of numbers.)

Exercise on Implementing RSA: Group D

As a group create a series of spreadsheets for implementing the techniques we have learned so far. You will use the following public keys for encrypting messages.

Team	Mike	A	B	C	D
m	4417571	3815969	78112883	44938309	65445929
k	101	101	107	77	107

You are Group D, and your value of m factors as

$$m = pq, \qquad p = 31, \quad q = 2111159.$$

(The numbers p and q are primes.)

Use the following table for converting from letters to numbers

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	21	22	23	24
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
25	26	27	28	29	31	32	33	34	35	36	37	38

(a) Create a spreadsheet that will implement the Euclidean algorithm. Try to set it up so that it will find solutions to

$$ax + by = \gcd(a, b)$$

for a given input (a, b).

(b) Use your spreadsheet from part (b) to find a solution to the equation

$$ku - \phi(m)v = 1$$

for *your* public key; you are Group D. (Remember that your solution must have $u > 0$.) Recall that if $m = pq$ is a product of distinct primes then

$$\phi(m) = \phi(p)\phi(q) = (p-1)(q-1).$$

(c) Find the binary expansion of the value of u you found in part (a).

(d) Create a spreadsheet that will make a table of successive squares $a^{2^j} \pmod m$.

(e) Using *your* public key, I have created the following encrypted message:

$$b_1 = 41985523, \quad b_2 = 25628364, \quad b_3 = 51498856, \quad b_4 = 33914975, \quad b_5 = 60744318$$

Use your spreadsheet from part (d) to decrypt the code. (Recall, this means you calculate $b_i^u \pmod m$ for the values of b_i above, *your* value of m and the u you found in part (a).)

(f) Find the binary expansion of the value $k = 101$ (this is the k from *my* public key).

(g) Use *my* public key $(m, k) = (4417571, 101)$ to encrypt a short (about 1 sentence long) message to send me. (This means you need to convert your message to numbers using the scheme above, and then break it up into a sequence of numbers $a_1, a_2, \ldots$ each smaller than $m = 4417571$. Now calculate $a_i^{101} \pmod{4417571}$ for $i = 1, 2, \ldots$. Give me your results.

(h) Repeat parts (f) and (g) using the public key from Group A and give the encrypted message to them.

(i) Once you receive an encrypted code from Group C, decrypt it using your public key. (In other words, repeat what you did in part (e) with the new sequence of numbers.)