26. RSA- Really Simple Algorithm

For this question we will be attempting to go through the entire process of decoding a RSA cipher. We will be using very small primes, but in reality very large primes are often used to prevent the modulus N from being factored and thus having the cipher broken.

In decoding RSA, you are usually given the public key and the modulus N. For this question our N will be 35.

a. Factor the modulus N into its primes. (25 points)

7 and 5 (also known as p and q)

b. Calculate phi(N) (also known as Euler's totient). (75 points)

phi(n)=(p-1)(q-1)=4*6=24

The public key can be any number, but it must be coprime with phi(N).

c. Which number can be used as e in this scenario? (25 points)

   i. 48 shares the factor 2
   ii. 99 shares the factor 3
   iii. 72 shares the factor 2
   iv. 25 shares no factors and thus is coprime to 25

We will select 29 as our public key for this scenario. By factoring N and calculating phi(N), we can now calculate our private key, d. The private key is defined as d*e=1 mod phi(N).

d. Calculate the private key, d. (150 points)

Phi=24 and e=29
We can mod e with phi to simplify
29 mod 24 is 5
Now we can evaluate using extended euclidean, or just realize that 5*5 mod 24 is one.
Therefore d is 5.

Now that we have our private key, we are ready to decode our message. We will stick with a 26 letter alphabet for this question. The message we are trying to decode is
12 # 08 # 21 # 09 # 23 # 24 # 23 # 07 # 00 # 17 # 08 # 12 # 00 # 33 # 16 # 09 # 17 # 00 # 13
(Normally RSA is not expressed like this, however this will simplify the calculations)
The equation of the decryption is (ciphertext)^d mod N.

e. Please decode the message and express the decoded message as numbers and not letters. For example if your output is 0, please express your plaintext as A, if your output is B, please express it as 1, and so forth. The standard two error rule applies here. (300 points)

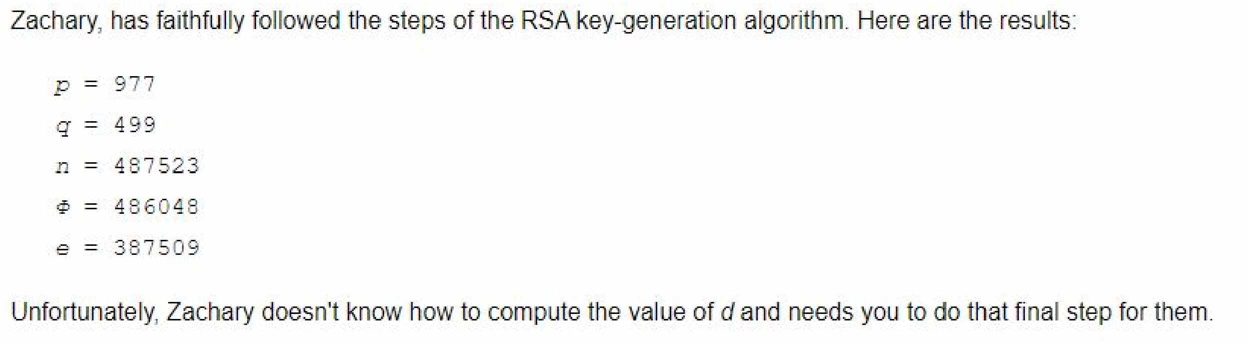
We evaluate 12^5 mod 35. You should be able to do this on a calculator without any extended steps. We get 17, which is the plaintext R. Repeat for all other letters.
Rivest Shamir Adleman (Hey it's RSA!)

Congratulations! You have (hopefully) decoded the contents of the RSA cipher. Here is a bonus question with much larger numbers. I do not recommend using the same process described earlier.
You received the ciphertext 13824. You know that the public key is 3 and the modulus N is 26167. Luckily you managed to already factor 26167 into 137 and 191. Please decrypt the sent message. The answer should be composed of one letter. (200 points)
The letter is Y

The numbers are small enough to use the process above with extended euclidean and rapid modular exponentiation to evaluate with a 4 function calculator. Or you could exploit the fact that the public key is 3. The public key is small enough and the mod is large enough so that when you evaluate even the largest possible plaintext number of 25, 25^3 or 15625 is smaller then our mod 26167. Therefore we can simplify square root 13824, yielding us 24, or the plaintext Y.

While this is all RSA, this isn’t very similar to the standard toebes questions. So let's explore the 5 standard RSA questions you will likely see in competitions. (Yes you do need to be able to evaluate with a 4 function calculator)

Take this toebes question:



Zachary, has faithfully followed the steps of the RSA key-generation algorithm. Here are the results:

```
p = 977
q = 499
n = 487523
Φ = 486048
e = 387509
```

Unfortunately, Zachary doesn't know how to compute the value of *d* and needs you to do that final step for them.

We know that d*e=1 mod phi(N). E is 387509 and phi(N) is 486048.

We will use the extended euclidean algorithm to solve

Format: phi(N)=E(x)+Remainder

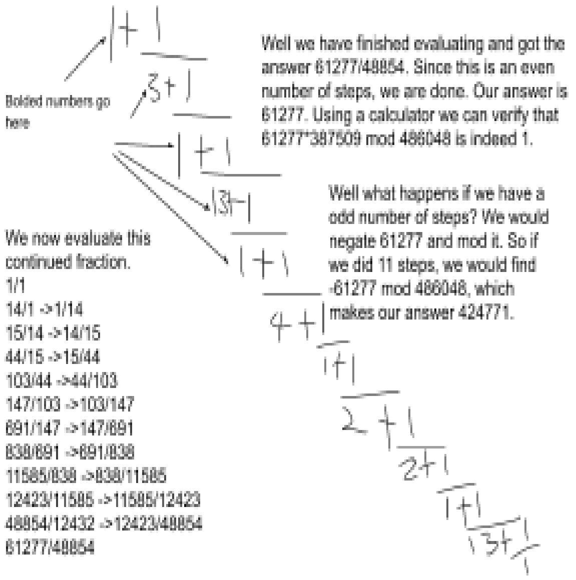
Step 1: 486048=(**1**)387509+98539

Now we shift the values to the left and remove the leftmost number. Keep track of the bolded numbers for later.

387509=(**3**)98539+91892
98539=(**1**)91892+6647
91892=(**13**)6647+5481
6647=(**1**)5481+1166
5481=(**4**)1166+817
1166=(**1**)817+349
817=(**2**)349+119
349=(**2**)119+111
119=(**1**)111+8
111=(**13**)8+7
8=(**1**)7+1

We stop when remainder equals one. Count the number of steps (12). Note this is even.

Now we will evaluate the bolded numbers.



Well we have finished evaluating and got the answer 61277/48854. Since this is an even number of steps, we are done. Our answer is 61277. Using a calculator we can verify that 61277*387509 mod 486048 is indeed 1.

Well what happens if we have a odd number of steps? We would negate 61277 and mod it. So if we did 11 steps, we would find -61277 mod 486048, which makes our answer 424771.

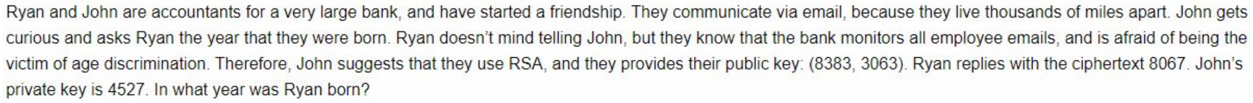
We now evaluate this continued fraction.
1/1
14/1 ->1/14
15/14 ->14/15
44/15 ->15/44
103/44 ->44/103
147/103 ->103/147
691/147 ->147/691
838/691 ->691/838
11585/838 ->838/11585
12423/11585 ->11585/12423
48854/12432 ->12423/48854
61277/48854

d is equal to 61277

Keep in mind this is only one method of evaluating, there are also other slightly different methods that can be used. This is the method I understand best, so I chose to explain it this way.

We now know how to compute the private key, but how do we evaluate large exponents with only a 4 function calculator?

Here's a example question requiring you to do so:



Ryan and John are accountants for a very large bank, and have started a friendship. They communicate via email, because they live thousands of miles apart. John gets curious and asks Ryan the year that they were born. Ryan doesn't mind telling John, but they know that the bank monitors all employee emails, and is afraid of being the victim of age discrimination. Therefore, John suggests that they use RSA, and they provides their public key: (8383, 3063). Ryan replies with the ciphertext 8067. John's private key is 4527. In what year was Ryan born?

The public key is in the format (n,e). Because the private key is given and we are decoding, e can be ignored. The equation for decoding is $(\text{ciphertext})^d$ mod n. Therefore we must evaluate 8067^{4527} mod 8383. We will be using rapid modular exponentiation (the method of repeated squaring) to evaluate this.

First find the binary representation of n, in this case 1000110101111. This will tell you what values are needed and not needed. Next we start to square. Match the corresponding binary to each square starting from the end. Keep track of the values obtained when the binary is 1.

1 8067^1 is 8067. Simple enough. The binary corresponds to 1 so keep track of 8067.

1 8067^2 = 65076489. If this number is larger than n we can mod it by n. 65076489 mod 8383 is 7643. 7643 will move on to the next step and because the binary corresponds to 1, keep track of 7643.

1 7643^2 mod 8383 is 2705
1 2705^2 mod 8383 is 7049
0 7049^2 mod 8383 is 2360. Because the binary is a 0, 2360 does not matter past the next step.
1 2360^2 mod 8383 is 3288
0 3288^2 mod 8383 is 5257
1 5257^2 mod 8383 is 5681
1 5681^2 mod 8383 is 7594
0 7594^2 mod 8383 is 2179
0 2179^2 mod 8383 is 3263
0 3263^2 mod 8383 is 759
1 759^2 mod 8383 is 6037

Now we can take all the results where the binary correspondent is 1 and multiply them together, and mod by n which should give us our answer.

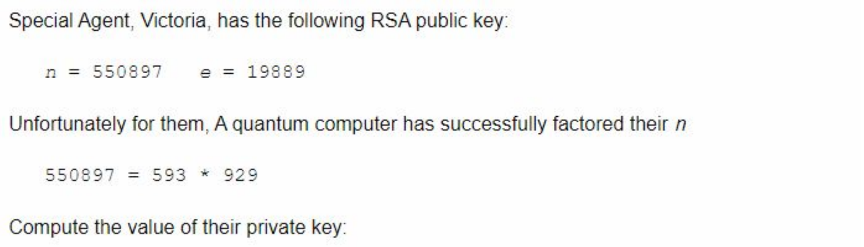
8067*7643*2705*7049*3288*5681*7594*6037 mod 8383. However this expression is too big for our calculators to handle so we will do it step by step.

8067*7643 mod 8383 is 7499
7499*2705 mod 8383 is 6318
6318*7049 mod 8383 is 5086
5086*3288 mod 8383 is 7066
7066*5681 mod 8383 is 4142
4142*7594 mod 8383 is 1332

Finally our answer is 1332*6037 mod 8383 which is 1987

Your answer will always be between 1950 and 2000, so you will know if your answer is correct or not. Additionally, you should always guess a number between 1950 and 2000 if you do not have enough time to finish the question.

Well what do you do with this Toebes question?



Special Agent, Victoria, has the following RSA public key:

```
n = 550897    e = 19889
```

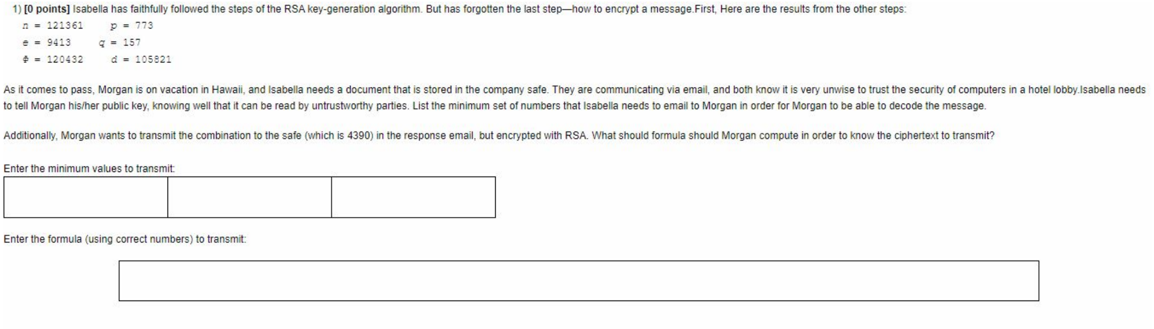
Unfortunately for them, A quantum computer has successfully factored their *n*

```
550897 = 593 * 929
```

Compute the value of their private key:

This is very similar to the compute *d* question earlier. We must find phi(N) which is (p-1)(q-1) or (592)(928) or 549376. We will use the same method of extended euclidean algorithm to solve 19889**d*=1 mod 550897. I will not redo the entire process here, but the answer to this is 482641, and similarly we can verify that (482641)(19889) mod 549376 is indeed 1.

Well what about this?



1) **[0 points]** Isabella has faithfully followed the steps of the RSA key-generation algorithm. But has forgotten the last step—how to encrypt a message.First, Here are the results from the other steps:

```
n = 121361     p = 773
e = 9413     q = 157
Φ = 120432     d = 105821
```

As it comes to pass, Morgan is on vacation in Hawaii, and Isabella needs a document that is stored in the company safe. They are communicating via email, and both know it is very unwise to trust the security of computers in a hotel lobby.Isabella needs to tell Morgan his/her public key, knowing well that it can be read by untrustworthy parties. List the minimum set of numbers that Isabella needs to email to Morgan in order for Morgan to be able to decode the message.

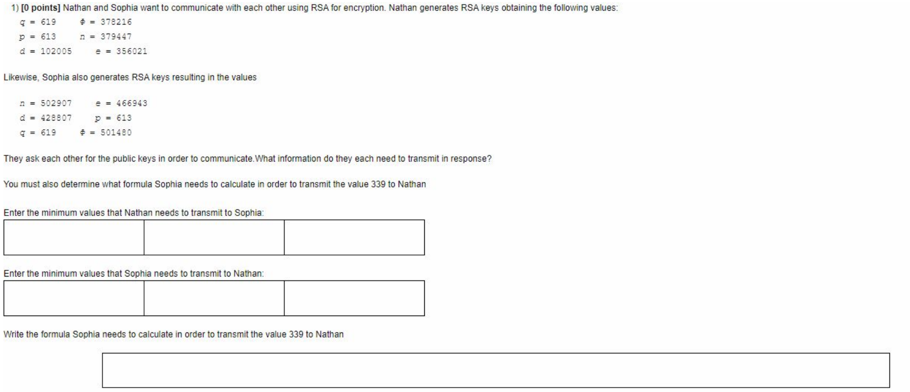
Additionally, Morgan wants to transmit the combination to the safe (which is 4390) in the response email, but encrypted with RSA. What should formula should Morgan compute in order to know the ciphertext to transmit?

Enter the minimum values to transmit:

Enter the formula (using correct numbers) to transmit:

This is a simple memorization problem. Put the values of n and e (121361 and 9413) into the first two boxes in any order. Be sure to leave the third box blank. In the formula box, substitute into the encoding equation (value)^e mod n to encode. For this scenario, the answer is 4390^{9413} mod 121361. Do not solve the equation.

Finally, what about this?



1) **[0 points]** Nathan and Sophia want to communicate with each other using RSA for encryption. Nathan generates RSA keys obtaining the following values:

```
q = 619     Φ = 378216
p = 613     n = 379447
d = 102005     e = 356021
```

Likewise, Sophia also generates RSA keys resulting in the values

```
n = 502907     e = 466943
d = 428807     p = 613
q = 619     Φ = 501480
```

They ask each other for the public keys in order to communicate.What information do they each need to transmit in response?

You must also determine what formula Sophia needs to calculate in order to transmit the value 339 to Nathan

Enter the minimum values that Nathan needs to transmit to Sophia:

Enter the minimum values that Sophia needs to transmit to Nathan:

Write the formula Sophia needs to calculate in order to transmit the value 339 to Nathan

This is basically the same question above. Fill in the n and e value for each person respectively as shown above, and write out the equation to encode using the value the second person wishes to encode with the RSA values of the first person (in this case 339^{356021} mod 379447).