I provide solutions for study.

This homework is being checked off (100% for turning it in. You get a separate check for participation in the message exchange.

1 Homework 15, assigned Wednesday 11/29/2023 and due next Wednesday

1. In this problem you should do all calculations by hand and show all details, only using the spreadsheets to check.

   Work through the entire process of setting up your RSA key using $p = 11, q = 17, r = 7$.

   You need to state what N is, verify that r has the correct property.

   If I send you the message $M = 42$, what is the M' you will receive?

   If you receive from me the message $M' = 76$, what was the message I sent?

$N = 11 \cdot 17 = 187$

$(p-1)(q-1) = 160$

$\gcd(7, 160) = 1$ so this works as required

160	1	0	
7	0	1	
6	1	-22	23
1	-1	(23)	1

Here is the computation of $7^{-1} \bmod 160 = 23$

$5 = 23$

The spreadsheet should help you check hand calculation.

$42^7 \bmod 187$:

7	15 ← result
3	36
1	42

encoded message to you is 15

$15^{23} \bmod 187$:

23	(42)
11	26
5	155
2	38
1	15

1

checked the decryption

$76^{23} \bmod 187$

23 → 11 → 5 → 2 → 1

87 → 43 → 166 → 76

decryption of message 76 is 32

2. Longer messages

   Messages expressed in the usual alphabet can be coded as numbers in various ways. One method is to replace each letter by two digits, A = 01, B = 02 up to Z = 26 and then space = 27.

   Then the numbers may be larger than M. So break the numbers into chunks, all of the same length and all less than M, and encrypt them one by one.

   The key $N = 28907 = (137)(211), r = 11$ which I used in class could be used to encrypt 4 digit (2 letter) blocks. Encrypt the message "RUN FOR YOUR LIFE" as a series of numbers. Show all work, but you may copy from the spreadsheet (or include snapshots of your spreadsheet calculations).

   Cryptographically of course this is very weak: a cipher encoding two digit blocks is easy to solve using statistical analysis. But a larger N will allow encryption of much longer blocks of text which will not be likely to be repeated.

RUN_FOR_YOUR_LIFE_

1821 1427 0615 1827 2515 2118 2712 0906 0522

91, 22631, 24563, 27423, 12588, 7276, 11362, 21015, 8423

if I made a mistake do tell me!

			28907	<---modulus
			1821	<----base of exponentation
11	<---exponent	1	91	<- result

- Sample calculation of first block - the spreadsheet pasted funny into my PDF editor

3. Message exchange

   I supply you with the key $N = 10403; r = 7$. Send me a coded message, a brief text sentence as in the previous problem, coding four digits at a time.

   You prepare an RSA key of your own with N at least 10000. Make sure that it is not too large to work with my spreadsheet (do some practice encryption and decryption). Send me your RSA key at the same time you send me your encrypted message for the first par and I will send you a reply to your message.

   In both parts of this problem, it makes sense to retain your work (which may use the spreadsheet of course) but you do not need to send it to me: just send me the message and your public key. I talked about this in class. You aren't going to lose points if you send work to me, but cryptographically that is your private stuff :-)

   Be aware that a point on this problem depends on replying when I send you a message using the key I send you, with the decryption of the message.

This is handled separately in email and gets a separate check

4. Verify that 49 is not a prime by finding a such that $a^{48} \texttt{mod} 49 \neq 1$.

   Find an $a < 49$ which lies and claims in effect that 49 is a prime. This indicates why you have to repeat the test with many random values of a to be certain (in practical terms) that you have a prime. But it doesn't happen often.

   Verify that 3293 is not a prime in the same way.

```
                                                    49      <---modulus

                                                    2       <----base of exponentation

48      <---exponent    0       15      <- result
```

• The very first number I try, 2 has $2^{48} \equiv_{49} 15$, not 1 so we see and 49 is not a prime

```
                                                    49      <---modulus

                                                    18      <----base of exponentation

48      <---exponent    0       1       <- result
```

• 18 is lying to you! 19 does too.

If 3293 were prime, we would have $2^{3292} \equiv 1 \bmod 3293$ and we do not.

```
                                                    3293    <---modulus

                                                    2       <----base of exponentation

3292    <---exponent    0       453
 1646                   0       484
  823                   1       3093
  411                   1       3131
  205                   1       1463
  102                   0       1343
   51                   1       2798
   25                   1       2055
```

← result is 453, not 1

box went off end of page, sigh

5. Compute $3^{1000} \texttt{mod} 23$ by repeated squaring.

   You can use the spreadsheet to check, but this might be a good drill for reliably doing these calculations on an exam.

   Then do this calculation using Fermat's little theorem. Depending on how good your calculator is, you might have to do a wee amount of repeated squaring, but not very much.

1000	<---exponent	0	8
500		0	13
250		0	6
125		1	12
62		0	2
31		1	18
15		1	12
7		1	2
3		1	4
1		1	3

← the result

1000 mod 22 = 10

3^{10} mod 23 =

10	<---exponent	0	8
5		1	13
2		0	9
1		1	3

You might not need repeated squaring at all. Same answer.

Try determining by experiment a similarly efficient method of computing powers mod 49. 49 is of course not a prime, so the exact approach of Fermat's theorem doesn't work. But there is a modulus you can apply to reduce the exponent in any calculation of an $a^n \texttt{mod} 49$. Find out what it is. You can use the spreadsheet to quickly compute powers mod 49 for your experimental investigation.

Holmes: not scored, but I'll explain, some of you might have explored this.