Math 4440/5440 Homework 1

Ian Martiny
Thao Bui
Colin Sidey
Bharadwaj Thirumal

Task 1:

What to replace IxNay's ciphertext of `LXFIXKNUBLNUNUB` with?

Solution: In order to replace this text with a proper text we need to find the key it was encrypted under. Since we know this was a Caesar shift cipher we can just brute force the key, by trying all 26 possible keys. Thus we find that this was the encryption of `SEMPERUBISUBUBI` (Always wear your undewear) under the key of 19. We decided to change this to `ALEAIACTAEST` (The die is cast). Once this is encrypted we get `TEXTBTVMTXLM`.

Task 2:

Determine the key and plaintext from a Vinenère cipher

Solution: The key is `XSU` and the plaintext is:

```
ATTENTION HEADQUARTERS WE ARE PLANNING THE NEXT OPERATION IT WILL TAKE PLACE IN WHEN
WE PLAN TO ASSASSINATE FRIEDRICH KASISKI ACCORDING TO WIKIPEDIA HE IS IN THE ARMY
EXCEPT HE HAD ALREADY RETIRED FROM THE ARMY IT IS CONFUSING ANYWAY WE PLAN TO GO BACK
AND FIGURE IT OUT AND ASSASSINATE HIM SO HE CANT CRACK THE VIGENERE CIPHER IF THAT IS
OK WITH YOU LET US KNOW ALSO WE ARE SENDING THIS VIGENERE CIPHER AND WE THINK IT IS
PROBABLY HARDER TO BREAK IF WE SEND LOTS OF EXTRA NONSENSE IN THE MESSAGE SO IM GOING
TO QUOTE FROM SCIENTIFIC AMERICAN ON THE VIGINERE CIPHER IN NINETEEN SEVENTEEN THE
METHOD USED FOR THE PREPARATION AND READING OF CODE MESSAGES IS SIMPLE IN THE EXTREME
AND AT THE SAME TIME IMPOSSIBLE OF TRANSLATION UNLESS THE KEY IS KNOWN THE EASE WITH
WHICH THEY KEY MAY BE CHANGED IS ANOTHER POINT IN FAVOR OF THE ADOPTION OF THIS CODE
BY THOSE DESIRING TO TRANSMIT IMPORTANT MESSAGES WITHOUT THE SLIGHTEST DANGER OF THEIR
MESSAGES BEING READ BY POLITICAL OR BUSINESS RIVALS ETC
```

To get this solution we used the methods from the textbook. To find the key we wrote a simple program that shifted the ciphertext looking for coincidental line ups (with the original, unshifted ciphertext) and kept track of which shifts had the most coincidences. The multiples of three had the most coincidences and we decided to assume the key was of length three first, our idea was that if the key was of length three that would also create the coincidences occurring from the shifts of six and nine etc.

Once we had decided to use a key of length three we use "Method 2" from the book. That is we looked at every third letter and did frequency analysis on this. And stored this as a vector W. Then we used the frequency of English alphabet from the book and stored it as a vector A. We then did the dot product of W with all the shifts of A and saw which was the largest. We did this for every third character starting with the first, then starting with the second and then starting with the third. The largest usually had a value of around 0.07 and gave us the value of our key. Then we simply decrypted under this key. Though we were initially stumped by the key itself, not being a word threw us off.

Task 3:

Explain why the Affine key is bad, then decrypt anyway.

Solution: Using $\alpha = 2$ as a key is a bad choice because $\gcd(2, 26) = 2$ so, 2 is not invertible $\texttt{mod}\ 26$. Thus when attempting to decrypt each ciphertext character has two possible plaintext characters it could have come from.

As for finding the actual plaintext we just looked at both possible decryptions for each letter. We could shift each letter by -1 (to negate β) and then we had a choice. Since our character value was even (having been multiplied by 2) we could either simply halve the value, or the value could have wrapped around 26. So we printed both options, assuming no character wrapped around and assuming all characters wrapped around. This gave us an output such as:

no wrap:	G	E	F	G	I	A	G	B	A	E	G	J	B	G	H	E	E	E
wrap:	T	R	S	T	V	N	T	O	N	R	T	W	O	T	U	R	R	R

Then we could simply attempt to reason what the phrase was. Starting with the end, we know that `RRR` and `EEE` were both bad ways to end a word but looking at the previous two letters we could either form the word `THERE` or `THREE`. Before that word was clearly the word `TWO` which led us to the word `ONE` before that. From there we were able to reason that the plaintext was `TESTING ONE TWO THREE`.

Task 4:

Where are they headed next and how do we plan to stop them?

Solution: They are headed to Baghdad (in the past) to influence Muhammad Ibn Musa Al-Khwarizmi to stop him from inventing algebra since it is so much work. In order to stop them we could stop them from getting a time machine.

To discover this we needed to decrypt their message. To do this we initially did a frequency analysis on the message. From this we discovered that it had (roughly) the same distribution as the English language. This suggested that the encrypted message was just a rearrangement of the plaintext. After this we noticed that the first couple letters resembled the word "Eviladia" and this lead us to recognize that this message was encrypted by swapping the order of pairs of letters. Allowing us to decrypt the full message.

The decryption is:

```
  Eviladia was here all your base are belong to us we are planning to take over the
 world since you have no hope of reading this message we may as well mention that our
next target is Baghdad around year we plan to influence Muhammad Ibn Musa Al-Khwarizmi
  not to invent algebra because we are getting tired of having to learn so much of it
```

Task 5:

Write a small Sage that will print out a multiplication table modulo n for any n.

Solution: Our code is as follows:

```
num = int(raw_input("Enter n: "))
column = "   |  "
seperator = "   |  "
for i in range(0, num):
    column += str(i) + "   "
```

```
print column
print seperator
for i in range(0,num):
    row = ""
    for j in range(0, num):
        product = i * j
        if product >= num:
            product %= num
        row += str(product) + "   "
    print str(i) + "  |  " + row
```

Some sample output, $n = 3$:

```
Enter n: 3
   |  0   1   2
   |
0  |  0   0   0
1  |  0   1   2
2  |  0   2   1
```

and for $n = 6$:

```
Enter n: 6
   |  0   1   2   3   4   5
   |
0  |  0   0   0   0   0   0
1  |  0   1   2   3   4   5
2  |  0   2   4   0   2   4
3  |  0   3   0   3   0   3
4  |  0   4   2   0   4   2
5  |  0   5   4   3   2   1
```

You can tell that a residue is not invertible if there are any non-zero, zero divisors; that is if two non-zero numbers which multiply to be zero. Equivalently if there is no inverse for a number. Some examples, in the above $n = 6$ case we can see that 2 is not invertible, because $2 \cdot 3 \equiv 0 \pmod{6}$ so there are zero divisors, and it has no inverse. Similarly for $n = 8$:

```
Enter n: 8
   |  0   1   2   3   4   5   6   7
   |
0  |  0   0   0   0   0   0   0   0
1  |  0   1   2   3   4   5   6   7
2  |  0   2   4   6   0   2   4   6
3  |  0   3   6   1   4   7   2   5
4  |  0   4   0   4   0   4   0   4
5  |  0   5   2   7   4   1   6   3
6  |  0   6   4   2   0   6   4   2
7  |  0   7   6   5   4   3   2   1
```

we can see that 6 is not invertible for the same reasons, there are zero divisors: $6 \cdot 4 \equiv 0 \pmod 8$ and it has no inverse.