Homework 2

1. Write a Bozosort implementation in Python or Java. Perform some empirical runtime studies on your method. That is, for list sizes of 2, 3, 4, 5, 6, ... (to as high as you want to go), give the average runtime of your method over several trial runs. Present your results in a nicely formatted table.

   My code is included as bozo.py. The results of the tests are included as results.txt. I ran the bozosort 20 times for each array, then I averaged the times for each. The following is these averages (individual times are omitted for lack of space).

n	Average time (ms)
3	0.0
4	0.100004673004
5	0.249993801117
6	2.2500038147
7	14.7000074387
8	70.7499980927
9	761.450004578
10	2437.15000153

   So, as you can see, this algorithm sucks.

2. Implement the Autokey Vigenere cipher, from scratch, in Java, JavaScript, or Python. Treat characters as codepoints.

   See vigenere.pl

3. The following ciphertext was intercepted. You know the message is in English and that the sender used a monoalphabetic substitution cipher. What is the plaintext?

   ```
   RYW QVKOVWPP KT KLV FVBP, LQKU DYZIY FEE WEPW IYZWTEG HWQWUHP, ZP FP
   DWEE AUKDU RK RYW QLXEZI FP RK BGPWET, FUH ZR ZP, Z RVLPR, VWFPKUFXEG
   PFRZPTFIRKVG FUH WUIKLVFOZUO RK FEE. DZRY YZOY YKQW TKV RYW TLRLVW,
   UK QVWHZIRZKU ZU VWOFVH RK ZR ZP JWURLVWH.
   ```

   ```
   THE PROGRESS OF OUR ARMS, UPON WHICH ALL ELSE CHIEFLY DEPENDS, IS AS
   WELL KNOWN TO THE PUBLIC AS TO MYSELF, AND IT IS, I TRUST, REASONABLY
   SATISFACTORY AND ENCOURAGING TO ALL. WITH HIGH HOPE FOR THE FUTURE,
   NO PREDICTION IN REGARD TO IT IS VENTURED.
   ```

   I began by noting that, three quarters of the way through line 2, there is a single 'Z'. The only two words in the English language that are one letter long are 'A' and 'I'. Many of the two-letter words also contained 'Z's. I began assuming 'Z' was 'A'. I then noticed that the most frequent three-letter word was 'RYW', so I replaced 'RYW' with 'THE', respectively. This was enough to develop a lot of the two letter words, but I found that, 'I' worked much better for 'Z' than 'A', and 'A' would work really nicely in certain areas (mostly as other two and three letter words) as 'A'. Another inside was that the second word ends in 'PP'. Words ending in two of the same letter is fairly rare, unless that letter is ‘S’ or ‘E’. ‘E’ was already accounted for so I set ‘P’ to ‘S’. At this point, the first word of the third line began to look very similar to ‘SATISFACTORY’, and once I filled that in the rest of the puzzle started to fall into place. Certain words with distinctive spellings like ‘MYSELF’ and ‘PUBLIC’ helped get fringe letters like ‘P’ and ‘M’, and I realized that the other most common three letter word, ‘FUH’, was almost certainly ‘AND’. At this point the puzzle pretty much just solved itself. It ended up being Lincoln; I was kind of hoping for Zodiac Killer.

4. Decrypt the following ciphertext, given that you know it was encrypted with the bifid algorithm in which the Polybius square was laid out in the usual fashion using the keyphrase “Darn, not another cryptanalysis question”.

```
TWBTLLAEPODTUBTWBTLTDLDDVSNNHEETLSKDDSIFGIIMWLYDKDDSPHBPQKOFHMDLSKRS
```

Our Polybius square is as follows:

	1	2	3	4	5
1	D	A	R	N	O
2	T	H	E	C	Y
3	P	L	S	I	Q
4	U	B	F	G	K
5	M	V	W	X	Z

So it follows that

```
 T   W   B   T   L   L   A   E   P   O   D   T   U   B   T   W   B
 21  53  42  21  32  32  12  23  31  51  11  21  41 42   21  53  42
 T   L   T   D   L   D   D   V   S   N   N   H   E   E   T   L   S
 21  32  21  11  32  11  11  52  33  14  14  22  23  45  21  32  33
 K   D   D   S   I   F   G   I   I   M   W   L   Y   D   K   D   D
 45  11  11  33  34  43  44  34  34  51  53  32  25  11  45  11  11
 S   P   H   B   P   Q   K   O   F   H   M   D   L   S   K   R   S
 33  31  22  42  31  35  45  15  43  22  51  11  32  33  45  13  33
```

```
21534221323212233151112141422153422132211132111152331414222345213233
45111133344344343451533225114511113331224231354515432251113233451333
COMPUTERSCIENCEISNZDOREABOUTCOMPUTERSTHANASTRONOMYISABOUTTELFWCOPESS
```