ECE 4802, Project 1

Calvin Figuereo-Supraner

November 1 2016

All scripts are run as `./q1.rb`, `./q2.rb`, etc.

Problem 1

1a

The script `q1.rb` uses brute force to test all 26 keys. The output eventually gives the key and plaintext.

```
19
THEENEMYKNOWSTHESYSTEM
```

Problem 2

2a

The script `q2.rb` prints a sorted hash of letter counts in the ciphertext. The letters J, K, and X do not appear.

```
{"E"=>29, "N"=>28, "F"=>25, "P"=>24, "G"=>23, "I"=>23, "B"=>17, "V"=>14,
"W"=>13, "M"=>12, "L"=>11, "Q"=>10, "A"=>10, "Y"=>9, "C"=>8, "T"=>7,
"H"=>3, "R"=>2, "S"=>2, "U"=>2, "O"=>2, "Z"=>1, "D"=>1}
```

2b

The script `q2.rb` then replaces the characters by letter frequency. This outputs:

```
THNAUSE THNAUSE SNTTSE DTRL ...
```

This is still unsolved, but could be `TWINKLE TWINKLE LITTLE STAR`. The script `q2.rb` then replaces letters under that assumption. The output reads:

```
TWINKLE TWINKLE LITTLE STAR
HOW I WONDER WHAT YOU ARE
UP ABOVE THE WORLD SO HIGH
LIKE A DIAMOND IN THE SKY

WHEN THE BLAZING SUN IS GONE
WHEN HE NOTHING SHINES UPON
THEN YOU SHOW YOUR LITTLE LIGHT
TWINKLE TWINKLE ALL THE NIGHT

THEN THE TRAVELER IN THE DARK
THANKS YOU FOR YOUR TINY SPARK
HE COULD NOT SEE WHICH WAY TO GO
IF YOU DID NOT TWINKLE SO
```

2c

The text is from a poem by Jane Taylor, and the missing words are below.

```
In the dark blue sky you keep,
And often through my curtains peep,
For you never shut your eye
Till the sun is in the sky.

As your bright and tiny spark
Lights the traveller in the dark,
Though I know not what you are,
Twinkle, twinkle, little star.
```

Problem 3

3b

- $\text{Gen}(kw, pt)$ outputs the keyword and plaintext, concatenated and truncated.
- $\text{Enc}(kw, pt) = (pt_i + k_i) \pmod{26}$ for each i.
- $\text{Dec}(kw, ct) = (ct_i - k_i) \pmod{26}$ for each i.

3c

The script `q3.py` implements the autokey cipher.

3d

The ciphertext decrypts to:

```
NOGOODDEEDGOESUNPUNISHED
```

Problem 4

4a

If the ciphertext is known, a large part of the key is known. Brute-force the cipher using keys that are shifted versions of the ciphertext.

4b

The script `q4.py` will eventually output a possible plaintext, via the attack above.

```
NEASJSENDTHEMONEYTHISAFTERNOON
```