## SPCS CRYPTOGRAPHY
## HOMEWORK 1

*Please try all the unmarked problems. #, ⋆ problems are both optional, with ⋆ problems being harder. You are strongly encouraged to work in groups, but you have to write up the solution on your own.*

# 1. Send me an email and tell me what you think about the class today, but **encrypt** your comment using one of the ciphers we discussed.

2. We can use the cipher wheel (Figure 1) to encrypt/decrypt messages. Here the outer wheel is the plaintext and the inner wheel is the ciphertext. For example, `a` is encrypted as `T`, `g` is encrypted as `Z`, and `fun` is encrypted as `YNG`.
   (a) Encrypt the following text,

   `the quick brown fox jumps over the lazy dog`

   (b) Decrypt the following sentence,

   `Rxl mabl bl max vhkkxvm tglpxk`

   (c) Decrypt the following sentence,

   `Mh ux hk ghm mh ux matm bl max jnxlmbhg`

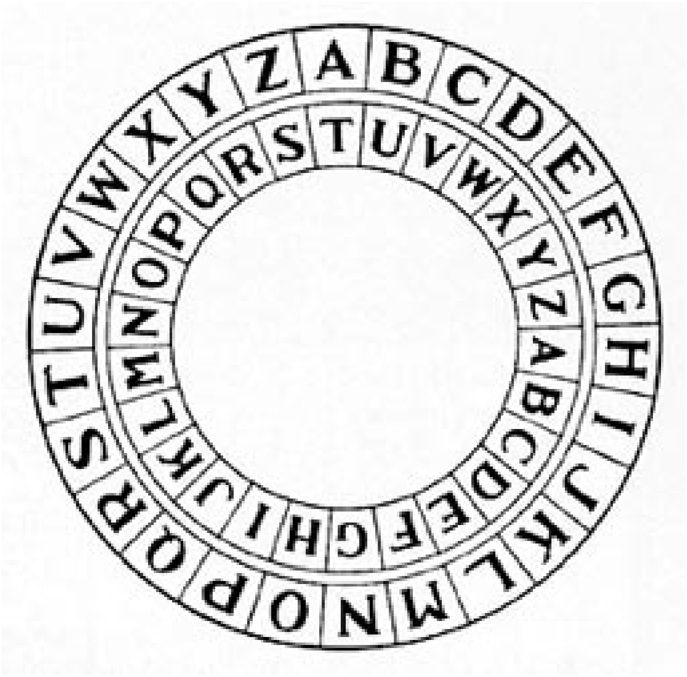
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S

FIGURE 1. Picture taken from a blog, *The Asylum.*

3. Sometimes when you run the Caesar cipher, one English word becomes another. For example, "*COLD*" becomes "*FROG*" if we shift everything to the right by 3. In this case we say that the **shift key** is 3.

   Figure out which word each of the following can be encrypted to. Pick any three parts for your problem set.
   (a) FOLK
   (b) DAZED

(c) ALOHAS
(d) ARENA
(e) FAKE
(f) LATTE
(g) LAYOUT
(h) MEET
(i) OVALS

4. Suppose that you have an alphabet of 26 letters. A simple substitution cipher is the one we discussed in class - we encrypt letter by letter.
   (a) How many possible simple substitution ciphers are there?
   (b) How many simple substitution ciphers are there with $A$ fixed?
   (c) How many simple substitution ciphers are there with $A$ and $B$ fixed?
   (d) How many simple substitution ciphers are there with $A$ or $B$ fixed?
   ⋆ (e) How many simple substitution ciphers are there with no letter fixed?
   Hint: to get started on the problem, you may want to work out the case of 4 letters first.

5. Substitution cipher 2 Each of the following messages has been encrypted using a simple substitution cipher. Decrypt them.
   (a) (This one has the space preserved.)

```
AUHC MVKFC V BYZUGC V IZMC CJ GUMBZYAZD UKUVM.
VC HZZGZB CJ GZ V HCJJB PD CFZ VYJM KUCZ AZUBVMK
CJ CFZ BYVWZ UMB OJY U IFVAZ V TJNAB MJC ZMCZY OJY
CFZ IUD IUH PUYYZB CJ GZ.
```

   ⋆ (b) The flora.

```
KZRNK GJKIP ZBOOB XLCRG BXFAU GJBNG RIXRU XAFGJ
BXRME MNKNG BURIX KJRXR SBUER ISATB UIBNN RTBUM
NBIGK EBIGR OCUBR GLUBN JBGRL SJGLN GJBOR ISLRS
BAFFO AZBUN RFAUS AGGBI NGLXM IAZRX RMNVL GEANG
CJRUE KISRM BOOAZ GLOKW FAUKI NGRIC BEBRI NJAWB
OBNNO ATBZJ KOBRC JKIRR NGBUE BRINK XKBAF QBROA
LNMRG MALUF BBG
```

   Hint: The frequency table is

|  | B | R | G | N | A | I | U | K | O | J | L | X | M | F | S | E | Z | C | T | W | P | V | Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Freq | 32 | 28 | 22 | 20 | 16 | 16 | 14 | 13 | 12 | 11 | 10 | 10 | 8 | 8 | 7 | 7 | 6 | 5 | 3 | 2 | 1 | 1 | 1 |

   The most frequent bigrams are: NG and RI (7 times each), BU (6 times), BR (5 times), and GL, OA, IN, XR, BN, KI, GR, GJ, GB (4 times).

   Here's a frequency table for alphabets and digrams in English: (Reference: here and here.)

| Alphabets Frequency | | | |
|---|---|---|---|
| e | 12.7 % | m | 2.4 % |
| t | 9.1 % | w | 2.4 % |
| a | 8.2 % | f | 2.2 % |
| o | 7.5 % | g | 2.0 % |
| i | 7.0 % | y | 2.0 % |
| n | 6.7 % | p | 1.9 % |
| s | 6.3 % | b | 1.5 % |
| h | 6.1 % | v | 1.0 % |
| r | 6.0 % | k | 0.8 % |
| d | 4.3 % | j | 0.2 % |
| l | 4.0 % | x | 0.2 % |
| c | 2.8 % | q | 0.1 % |
| u | 2.8 % | z | 0.1 % |

| Bigrams Frequency | | | |
|---|---|---|---|
| th | 1.52 % | en | 0.55 % |
| he | 1.28 % | ed | 0.53 % |
| in | 0.94 % | to | 0.52 % |
| er | 0.94 % | it | 0.50 % |
| an | 0.82 % | ou | 0.50 % |
| re | 0.68 % | ea | 0.47 % |
| nd | 0.63 % | hi | 0.46 % |
| at | 0.59 % | is | 0.46 % |
| on | 0.57 % | or | 0.43 % |
| nd | 0.56 % | ti | 0.34 % |
| ha | 0.56 % | as | 0.33 % |
| es | 0.56 % | te | 0.27 % |
| st | 0.55 % | et | 0.19 % |

# 6. Prove the following by modifying Euclid's proof.

(a) There are infinitely many primes congruent to 3 mod 4. (Hint: Suppose that there are only finitely many such primes, and they are $p_1, \cdots, p_k$. Consider $N = 4p_1 \cdots p_k + 3$.)

$\star$ (b) Prove that there are infinitely many primes congruent to 1 mod 4.

7. Check that multiplication modulo $m$ is well-defined. In other words, prove that if $a \equiv a' \mod m$ and $b \equiv b' \mod m$, then

$$ab \equiv a'b' \mod m.$$

8. (a) Find $100 \cdot 101 \cdot 102 \cdot 103 \mod 99$.

(b) Find $100 \cdot 99 \cdot 98 \cdot 97 \mod 101$.

(c) Find the last digit of $2^{2015}$.

(d) Given an integer $n$ in its decimal expansion $\overline{a_k a_{k-1} \cdots a_0}$, show that

$$n \equiv a_k + a_{k-1} + \cdots + a_0 \mod 9$$

For example, this means that

$$1234 \equiv 1 + 2 + 3 + 4 \mod 9 \equiv 10 \mod 9 \equiv 1 \mod 9.$$

In particular, find the remainder of

$$\underbrace{20152015 \cdots 2015}_{\text{repeating 2015 times}}$$

when divided by 9.

(e) Can you design a divisibility test for 11? In other words, given an integer $n$ in its decimal expansion $\overline{a_k a_{k-1} \cdots a_0}$, figure out a way to quickly find $n \mod 11$.

9. Which problem do you like the best/the least? Why?