Math 406 Section 8.1: Character Ciphers

1. **Introduction:** The goal of this entire chapter (the rest of the course!) is talk a little about encryption.

2. **Terminology:** We have the following:

   (a) *Cryptology*: The study of encryption.

   (b) *Cryptography*: The study of methods of encryption.

   (c) *Cipher*: A particular method of encryption.

   (d) *Cryptanalysis*: Breaking of systems of encryption.

   (e) *Plaintext*: The human-readable text we wish to encrypt.

   (f) *Encryption*: The process of applying a cipher to plaintext.

   (g) *Ciphertext*: The human-non-readable result.

   (h) *Decryption*: The process of getting the plaintext back.

3. **Basic Methods**

   (a) **Character Assignment:** To begin with we'll assign a number to each letter of the alphabet:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

   Note: For now we'll exclude lower-case, punctuation and spaces, but of course we could add those two and use a different modulus.

   Note: This can be confusing since `A` is the first letter of the alphabet and so we might want to assign it 1. However since we're working with modulus this makes more sense.

   (b) **The Caeser Cipher:** The Caeser Cipher was purportedly used by Julius Caeser and invoved taking each character P in plaintext and assigning the ciphertext C to be the least nonnegative residue of $C+3 \bmod 26$. We'll write $P = C+3 \bmod 26$. So the word `LEIBNIZ` would be assigned the values $11, 4, 8, 1, 13, 8, 25$ and then we would add 3 to each and reduce mod 26 to get $14, 7, 11, 4, 16, 11, 2$ which the yields `OHLEQLC`. We then decrypt it by subtracting 3 and finding the least nonnegative residue.

   (c) **Shift Ciphers:** Caeser's Cipher is an example of a shift cipher. Generically a shift cipher has the form $P = C + b \bmod 26$ for some choice of b.

   (d) **Affine Ciphers:** We can actually go one step further and assign $P = aC + b \bmod 26$ provided we make safe choices. The value of b can be anything (although there are only 26 distinct choices) but for a we must be careful. If we set $a = 2$ for example then $P = 0$ and $P = 13$ both yield $C = 0$.

   What we need is for the mapping $C \equiv aP + b \bmod 26$ to be invertible and hence 1-1. To do this we need to be able to solve for P. Well we have $C - b \equiv aP \bmod 26$ but now we need to multiply by the multiplicative inverse of a and for this we need $\gcd(a, 26) = 1$.

   Thus we can make $\phi(26) = 12$ choices for a and 26 choices for b yielding $(12)(26) = 312$ choices.

   Example: The mapping $C \equiv 5P + 7 \bmod 26$ is an affine cipher with decryption:

$$\begin{aligned} C &\equiv 5P + 7 \bmod 26 \\ 5P &\equiv C - 7 \bmod 26 \\ (-5)5P &\equiv (-5)(C-7) \bmod 26 \\ -25P &\equiv -5C + 35 \bmod 26 \\ P &\equiv 21C + 9 \bmod 26 \end{aligned}$$

4. **Breaking Shift Ciphers** To break a shift cipher requires only figuring out one letter because, if we know some P_0 and C_0 with $C_0 \equiv P_0 + b \bmod 26$ we can simply solve for b. For example if we find out that the ciphertext $F = 5$ corresponds to the plaintext $X = 23$ then we know that $5 \equiv 23 + b \bmod 26$ and we can find $b \equiv 8 \bmod 26$. We often do this using frequency analysis on the letters. Since the letter E occurs most frequently in the English language we can find the most common ciphertext letter and assume it corresponds to E. We then find b, decrypt the entire message and see if it makes sense. If so, we're done. If not, then the letter T is second most frequently so we might assume our most common letter corresponds to T and try that.

   Example:

5. **Breaking Affine Ciphers** This approach will not work for an affine cipher. This is because if we know some P_0 and C_0 with $C_0 \equiv aP_0 + b \bmod 26$ we cannot solve for both a and b. Instead we need to know two characters. This is because if we also know some P_1 and C_1 with $C_1 \equiv aP_1 + b \bmod 26$ we can solve the system. This is because we have:

$$\begin{aligned} C_0 &\equiv aP_0 + b \bmod 26 \\ C_1 &\equiv aP_1 + b \bmod 26 \\ \hline C_0 - C_1 &\equiv a(P_0 - P_1) \bmod 26 \end{aligned}$$

   This system has $\gcd(P_0 - P_1, 26)$ solutions for a provided $\gcd(P_0 - P_1, 26) \mid (C_0 - C_1)$. However if we know for a fact that an affine cipher was used for encryption then we know a solution exists, which guarantees that $\gcd(P_0 - P_1, 26) \mid (C_0 - C_1)$. There will be $\gcd(P_0 - P_1, 26)$ possible solutions for a though, but each a has a specific b since $C_0 \equiv aP_0 + b \bmod 26$ so we can simply try all possible a, b pairs until we get one that makes sense.

   If we are doing frequency analysis though then we will probably be looking for the C_0 corresponding to $P_0 = 4$ for `E` and for the C_1 corresponding to $P_1 = 19$ for `T` in which case $\gcd(P_0 - P_1, 26) = \gcd(4 - 19, 26) = 1$ and there is just one possibility.

   Example: Suppose we intercept the message `WKKTBDKZKKBPKCB`. The most common ciphertext letter is `K` and since K corresponds to $C_0 = 10$ we assume that this corresponds to $P_0 = 4$ for `E` The second most common ciphertext letter is `B` and since B corresponds to $C_1 = 1$ we assume that this corresponds to $P_0 = 19$ for `T`. Thus we solve:

$$\begin{aligned} 10 &\equiv a(4) + b \bmod 26 \\ 1 &\equiv a(19) + b \bmod 26 \\ \hline 9 &\equiv -15a \bmod 26 \\ 9 &\equiv 11a \bmod 26 \\ a &\equiv 15 \bmod 26 \end{aligned}$$

   Then since $10 \equiv 4a + b \equiv 4(15) + b \bmod 26$ we have $b \equiv 10 - 60 \equiv -50 \equiv 2 \bmod 26$. We can then decrypt:

Character	W	K	K	T	B	D	K	Z	K	K	B	P	K	C	B
C	22	10	10	19	1	3	10	25	10	10	1	15	10	2	1
7(C−2) ≡	10	4	4	15	19	7	4	5	4	4	19	13	4	0	19
Character	K	E	E	P	T	H	E	F	E	E	T	N	E	A	T