8 Cryptography

8.1 Character Ciphers

---

1. **Introduction:** The goal of this entire chapter (and the rest of the course) is to talk about encryption and cryptography.

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

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

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

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

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

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

   (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.

   (i) *Some Names*:

      i. Alice: encrypts and sends

      ii. Bob: receives and decrypts

      iii. Eve: eavesdropper

3. **Basic Methods:**

   (a) **Character Assignment:** To begin, we will 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 will exclude lower-case, punctuation and spaces, but we could include those and use a different modulus.
   Note: This can be confusing since `A` is the first leter of the alphabet and so we would naturally want to assign it to 1. We use this for purposes of making our modular arithmetic easier.

   (b) **Shift Cipher:** For each plaintext letter P we assign ciphertext

$$C \equiv P + b \bmod 26$$

Ex. Encrypt `LEIBNIZ` with $b = 3$.

$$\begin{aligned}
L: &\quad P = 11, 11 + 3 \equiv 14 = C : O \\
E: &\quad P = 4, 4 + 3 \equiv 7 = C : H \\
I: &\quad P = 8, 8 + 3 \equiv 11 = C : L \\
B: &\quad P = 1, 1 + 3 \equiv 4 = C : E \\
N: &\quad P = 13, 13 + 3 \equiv 16 = C : Q \\
I: &\quad P = 8, 8 + 3 \equiv 11 = C : L \\
Z: &\quad P = 25, 25 + 3 \equiv 2 = C : C
\end{aligned}$$

Which then results in `OHLEQLC`. To decrypt we simply reverse: $C \equiv P + b \bmod 26$, $P \equiv C - b \bmod 26$.

(c) **Affine Cipher:** Choose a and b and encrypt via $C = aP + b \bmod 26$. How will decryption work? $C \equiv aP + b \bmod 26$, $aP \equiv C - b \bmod 26$ there needs to be a unique P. To have this we need $\gcd(a, 26) = 1$ so that a has a multiplicative inverse. Then $P \equiv a^{-1}(C - b) \bmod 26$. How many choices? $\phi(26) = 12$ for a and 26 choices for b.

Ex. If we choose $a = 5$ and $b = 7$ then encryption is $C \equiv 5P + 7 \bmod 26$ and decryption is $5P \equiv C - 7 \bmod 26 \implies P \equiv 21(C - 7) \bmod 26$ (calculated from 21 being the multiplicative inverse of 5).