Caesar Cipher

Let $n \mod m$ denote the remainder when $n$ is divided by $m$, i.e., mod means % in C or Java.

Use the numbers 0 to 25 to code the English alphabet: $0 = A$, $1 = B$, $2 = C$, ..., $25 = Z$.

With this code, we can encipher a message by computing with the numbers corresponding to the letters of the message.

Encipher the numbers with a formula.

Then we use the code to change numbers back to letters.
For example, we can “rotate the alphabet” by \(k\) letters.

In terms of the numbers, we encipher \(x\) by adding \(k\) to it modulo 26: \(E(x) = (x + k) \mod 26\).

Julia Caesar used this cipher with \(k = 3\). Under this cipher, the message

\[
\text{RENAISSANCE}
\]

is enciphered as

\[
\text{UHQDLVVDQFH}
\]

One deciphers this cipher either by rotating the alphabet backwards by \(k\) letters: \(D(x) = (x - k) \mod 26\) or by rotating the alphabet forward by \(26 - k\) letters: \(D(x) = (x + (26 - k)) \mod 26\).
The case \( k = 13 \) gives the rotate cipher used in some newsgroups. It has the nice property that the deciphering formula is the same as the enciphering formula: \( D(x) = (x + 13) \mod 26 = E(x) \).

Another possibility is to multiply the numbers which represent the letters by a constant: \( E(x) = kx \mod 26 \).

Under this cipher with \( k = 9 \), the message RENAISSANCE

is enciphered as

XKNAUGGANSK

In order for deciphering to be possible, \( k \) and 26 must be relatively prime. When this is so, let \( jk \mod 26 = 1 \)

Then the deciphering function is \( D(x) = jx \mod 26 \).
Encryption Algorithms

A. Transposition ciphers rearrange characters or bits.

**Example:** Write rows, read columns of a matrix.

There is a fixed period, $d$, say. If we assume all $d!$ permutations to be equally likely, then the shortest length of ciphertext needed to break it is

$$N = \frac{d \log_2(d/e)}{3.2} \approx 0.3d \log_2(d/e).$$

**Example:** With a $3 \times 9$ matrix we have $d = 27$ and $N = 27.9$.

Use digrams to crack transposition ciphers. The process is called *anagramming*. 
B. Substitution Ciphers

Alphabets: Plain \( \{m_i\} \), Cipher \( \{c_i\} \).

Replace (blocks of) characters by other characters. Four types:

1. Simple: Replace \( m_i \) by \( c_i \). Permute alphabet.

2. Homophonic: Replace \( m_i \) by a random one of many possible \( c_j \).

3. Polyalphabetic: Use multiple maps from the plaintext alphabet to the ciphertext alphabet.

4. Polygram: Make arbitrary substitution for groups of characters.

Use frequency counts to distinguish Transposition ciphers from Substitution ciphers.
1. Simple: Replace $m_i$ by $c_i$. Write $f(m_i) = c_i$.

**Example.** Caesar cipher—rotate the alphabet: $f(m) = (m + k) \mod n$, where $n$ is the alphabet size. The shortest length of ciphertext needed to break it is $(\log_2 26)/3.2 \approx 1.5$ letters.

If all $n!$ permutations of the alphabet are equally likely (the best case) in a simple substitution cipher, and the language is English (with $n = 26$), then the shortest length of ciphertext needed to break it would be $\log(26!)/3.2 \approx 27.6$. This is the case for the Cryptoquote in the **Exponent**.

These ciphers may be broken with frequency analysis and trial and error.

An **affine cipher**, $f(m) = (am + b) \mod n$, guess some two-letter pairs and solve two congruences in two unknowns $a$ and $b$.
2. Homophonic: Replace $m_i$ by a random one of many possible $c_j$.

To confound the frequency analysis which succeeds so well for simple substitution ciphers, one might use a ciphertext alphabet larger than the plaintext alphabet and assign each plaintext letter $a$ to a subset (homophone) $f(a)$ of the ciphertext alphabet. To permit deciphering, require $f(a) \cap f(b) = \emptyset$ when $a \neq b$. Encipher each $m_i$ in the plaintext as a randomly chosen $c_j \in f(m_i)$.

Usually, the ciphertext alphabet is much larger than the plaintext alphabet and the size of $f(a)$ is proportional to the frequency of occurrence of $a$ in English. Then the letters of the ciphertext alphabet have a uniform distribution in the ciphertext. Use digrams to break.

One can define $f$ via a standard text using the number of an instance of the letter as its cipher.
3. Polyalphabetic: Use multiple maps $f_i$ from the plaintext alphabet to the ciphertext alphabet.

Encipher $M = m_1 m_2 \ldots$ as $C = f_1(m_1)f_2(m_2)\ldots$.

Let $n$ be the length of the alphabet. The sequence $\{f_i\}$ may be periodic, perhaps defined by a keyword $K = k_1 \ldots k_d$.

**Example:** Vigenère cipher: $f_i(a) = (a + k_i) \mod n$.

**M:** RENA ISSA NCE

**K:** BAND BAND BAN

**C:** SEAD JSFD OCR
**Example:** Beaufort cipher: \( f_i(a) = (k_i - a) \mod n \).

If the period of the key is \( d \), then the shortest length of ciphertext needed to break it is \( \log_2(n^d) / 3.2 = (d/3.2) \log_2 n \). For English (with \( n = 26 \)), this is \( d \log_2(26) / 3.2 \approx 1.47d \).
The way to break a periodic polyalphabetic substitution cipher is to first find the period $d$. Then break it by solving $d$ interleaved simple substitution ciphers by letter frequency, guessing words or using digraphs.

There are two basic methods to find the period of a periodic polyalphabetic substitution cipher.

Kasiski Method: Look for repetitions in cipher text. They might occur at multiples of the period $d$. Look at the gcd of some of the differences.
The Index of Coincidence Method: Measure frequency variations of letters to guess the period \( d \). Let \( \{a_0, a_1, \ldots, a_{n-1}\} \) be the (plain or ciphertext) alphabet. Let \( F_i \) be the frequency of occurrence of \( a_i \) in a ciphertext of length \( N \). Define the Index of Coincidence as

\[
IC = \left( \sum_{i=0}^{n-1} \frac{F_i(F_i - 1)}{2} \right) \frac{N(N - 1)}{2}.
\]

Then \( IC \) represents the probability that two letters chosen at random in the ciphertext are the same.
One can estimate $IC$ theoretically in terms of the period $d$. For English and a polyalphabetic cipher with period $d$, the expected value of $IC$ is

$$\frac{1}{dN-1}N - d(0.066) + \frac{d-1}{dN-1}N(0.038).$$

Guess $d$ by comparing the $IC$ with this table: $(d, IC)$: (1, 0.066), (2, 0.052), (3, 0.047), (4, 0.045), (5, 0.044), (10, 0.041), (infinity, 0.038).

The $IC$ tells you the approximate size of the period $d$. The Kasiski method complements the $IC$ method by telling you a number (the gcd) that probably divides $d$.

**Example.** If $IC = 0.043$, then $d$ is probably 6 or 7. If a Kasiski analysis finds several examples of repeated ciphertext occurring at multiples of 3 in the position of the letters, then $d$ is probably a multiple of 3. These two pieces of information suggest that $d = 6$. 

12