LAB 6

Base-26

EXPERIMENT 6.1. Let $n = 287,472,347,234$.

(a) Find $s_0, \ldots, s_{12}$ such that we can write n as

$$s_0 \times 10^0 + s_1 \times 10^1 + s_2 \times 10^2 + s_3 \times 10^3 + \cdots + s_{12} \times 10^{12}.$$

This is the *base ten* expansion of n.

(b) Compute REM $(n, 10)$. What do you get?

(c) Compute $n_1 = (n-$ REM $(n, 10))/10$. Was it an accident that you got an integer?

(d) Suppose we keep going. Find $n_j = (n_{j-1}-$ REM $(n_{j-1}, 10))/10$ for $j = 2, \ldots, 12$ without doing any computations.

Experiment 6.2. Keep $n = 287,472,347,234$ from Experiment 6.1.

(a) Let s_0 =REM $(n, 26)$ and set $n_1 = (n - s_0)/26$. Compute s_1 =REM $(n_1, 26)$.

(b) For $j = 2, \ldots, 12$, set $n_j = (n_{j-1} - s_{j-1})/26$ and s_j =REM $(n_j, 26)$. Make a table of all the s's and n's.

(c) Compute

$$s_0 \times 26^0 + s_1 \times 26^1 + s_2 \times 26^2 + \cdots + s_{10} \times 26^{10} + s_{11} \times 26^{11}.$$

What did you get? This is called the *base* 26 *expansion* of n.

(d) Compute the base 26 expansion of $m = 235,823,443$.

You can now use the `IntegerDigits` command to find base-10 or base-26 digits of a number.

EXPERIMENT 6.3. Now we want to turn words into numbers using base 26 expansions. Consider the word `CRYPTOLOGY`. Using our usual numbering for the alphabet, we can think of this as

$$\begin{array}{ccccccccccc} \texttt{C} & \texttt{R} & \texttt{Y} & \texttt{P} & \texttt{T} & \texttt{O} & \texttt{L} & \texttt{O} & \texttt{G} & \texttt{Y} & = \\ 2 & 17 & 24 & 15 & 19 & 14 & 11 & 14 & 6 & 24 & = \end{array}$$

$$2 \times 26^0 + 17 \times 26^1 + 24 \times 26^2 + \cdots + 14 \times 26^7 + 6 \times 26^8 + 24 \times 26^9$$

An important note is that some people will will write this the other way around, i.e., as $2 \times 26^9 + 17 \times 26^8 + \cdots + 6 \times 26^1 + 24 \times 26^0$. This is a matter of convention.

(a) Find the number associated with `CRYPTOLOGY`.

(b) Pick a 20-digit public key for Kid Krypto, and write it on a whiteboard. Remember your private key, and make sure to keep it private.

(c) Pick a text message consisting of at most 14 letters, and turn it into a number using base-26.

(d) Encode your message using another team's public key.

(e) If someone sent you a message, decode it. If not, send more messages until you receive one — and then decode it.