10 Prolog (acr31)

A Caesar Cipher (or Shift Cipher) produces ciphertext from plaintext by replacing each letter with another that is found a fixed number of places down the alphabet. Users provide a key from 1 to 25 (inclusive) to determine the number of places to move. Our alphabet contains just the 26 lowercase letters and is circular: moving past z takes you back round to a again. For example under a key of 5 the letter \textit{y} would be replaced by the letter \textit{d}.

When answering this question ensure that each of your predicates has a comment giving a declarative reading of its behaviour and avoid unnecessary use of cut. Do not use any extra-logical predicates (such as \texttt{assertz}) or any library predicates.

\textbf{(a)} One way to represent the ordering of characters is with 26 facts indicating the next character. For example \texttt{next(a,b)} then \texttt{next(b,c)} through to \texttt{next(z,a)}.

Use \texttt{next} to implement a predicate \texttt{nextn(N,C1,C2)} which succeeds if the character \texttt{C2} appears \texttt{N} places after the character \texttt{C1}. You may assume that \texttt{N} is always a ground term. \hfill [3 marks]

\textbf{(b)} Another approach would be to use a list of characters to record the order of letters.

Provide an alternative implementation of \texttt{nextn} which makes use of the list representation \texttt{[a,b,c,...]}. Explain how you deal with the case of moving past the end of the alphabet.

You may assume the existence of two predicates: \texttt{scan(C,R,List)} which succeeds if \texttt{R} is the remainder of \texttt{List} that follows the letter \texttt{C}; and \texttt{charAt(N,C1,List)} which succeeds if \texttt{C1} is the character at position \texttt{N} in \texttt{List}. Position 0 is the first element of the list. \texttt{N} must be a ground term. \hfill [6 marks]

\textbf{(c)} Compare the merits of these two representations giving three relative benefits or drawbacks. \hfill [3 marks]

\textbf{(d)} Implement a predicate \texttt{caesar(K,P,C)} which succeeds if \texttt{C} is the ciphertext of the plaintext \texttt{P} under key \texttt{K}. Both ciphertext and plaintext are represented with a list of letters. You may assume that \texttt{P} and \texttt{K} are ground terms. \hfill [3 marks]

\textbf{(e)} The plaintext for a single ciphertext character has been discovered through a known-plaintext attack. Extend your \texttt{caesar} predicate to recover the key in this scenario and give an example invocation. \hfill [5 marks]