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 y would be replaced by the letter 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 assertz) or any library predicates.

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

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

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

Provide an alternative implementation of nextn which makes use of the list representation [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: scan(C,R,List) which succeeds if R is the remainder of List that follows the letter C; and charAt(N,C1,List) which succeeds if C1 is the character at position N in List. Position 0 is the first element of the list. N must be a ground term. [6 marks]

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

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

(e) The plaintext for some of the ciphertext characters has been discovered through a known-plaintext attack. Extend your caesar predicate to recover the key in this scenario and give an example invocation. [5 marks]