Form 6 ICT SBA – Case Study 5
Data Encryption

Form 6 _____ Name _____ No. _____ Date_____

1. Tom writes a program to encrypt a text. This program handles capital letters only, as shown below:

```
program Code;
const shift = 13;
var InStr : string;
    i, tmp: integer;
begin
    write('Please input the text: ');
    readln(InStr);
    write('The coded message is : ');
    for i := 1 to length(InStr) do
        if (InStr[i] >= 'A') and (InStr[i] <= 'Z') then
            begin
                tmp := ord(InStr[i]) + shift;
                if tmp > 90 then tmp := tmp - 26;
                write(chr(tmp))
            end
        else
            write(InStr[i]);
    writeln
end.
```

(a) Write down the output of the program if the input is:

(i) BAR _____

(ii) ONE _____

(b) Describe briefly how to decode the encrypted text by using the above program.

_____

_____

(c) What kind of encryption method (symmetric key or asymmetric key) is used in the above algorithm? Explain briefly

_____

_____

Mary has Tom's encrypted text. She is told that Tom's encrypted text can be cracked by using the following steps:

Step 1: Count the number of occurrences of each letter in the encrypted text.

Step 2: In general, statistics show that 'E' is the most commonly used letter in a passage. Thus, Mary replaces the most frequent letter in the encrypted text by 'E' and then the next letter in the alphabet with 'F' and so on. For example, if the most frequent letter in the encrypted text is 'Y', then 'Y' will be replaced by 'E', then 'Z' by 'F', 'A' by 'G', 'B' by 'H', ... , etc.

(d) Mary writes a program to count the number of occurrences of each letter in a text file specified by the user and also to find the most frequent letter. Write the contents of the boxes to complete the program below.

```
program Count;
var filename, InStr : string;
    Infile : [ A ] ;
    Freq : array['A'..'Z'] of integer;
    c, max : char;
    i : integer;
begin
    for c := 'A' to 'Z' do
         Freq[c] : = 0;

    write('Please input the name of the file to be processed :');
    readln(filename);
    assign(Infile, [ B ] );
    [ C ] ;
    while [ D ] do
        begin
            readln(infile, InStr);
            for i : = 1 to [ E ] do
                if (InStr[i]>='A') and (InStr[i]<='Z') then
                    [ F ] ;
        end;
    close(Infile);
    max := 'A';
    for c := 'B' to 'Z' do
        if [ G ] then max := c;
    writeln('The most frequent letter is ', max)
end.
```

A _____

B _____

C _____

D _____

E _____

F _____

G _____

(e) State **two** weaknesses of using this cracking method on a passage that contains capital letters only.

_____

_____

_____