CRYPTOGRAPHY OF DATA

by

A Strange Site

http://astrangesite.altervista.org

Powered by dr. Alessandro Strano

Cryptography consists in using a code that is hard to understand for people who do not know it.

An easy but efficacious method of cryptography consists in "masking" data by means of an "alphanumeric key" and the logic operator exclusive-OR (XOR). It is sufficient applying the operator XOR, with the same key, on coded data to obtain original values.

Table 1

X_1	X_2	X_1 XOR X_2
0	0	0
0	1	1
1	0	1
1	1	0

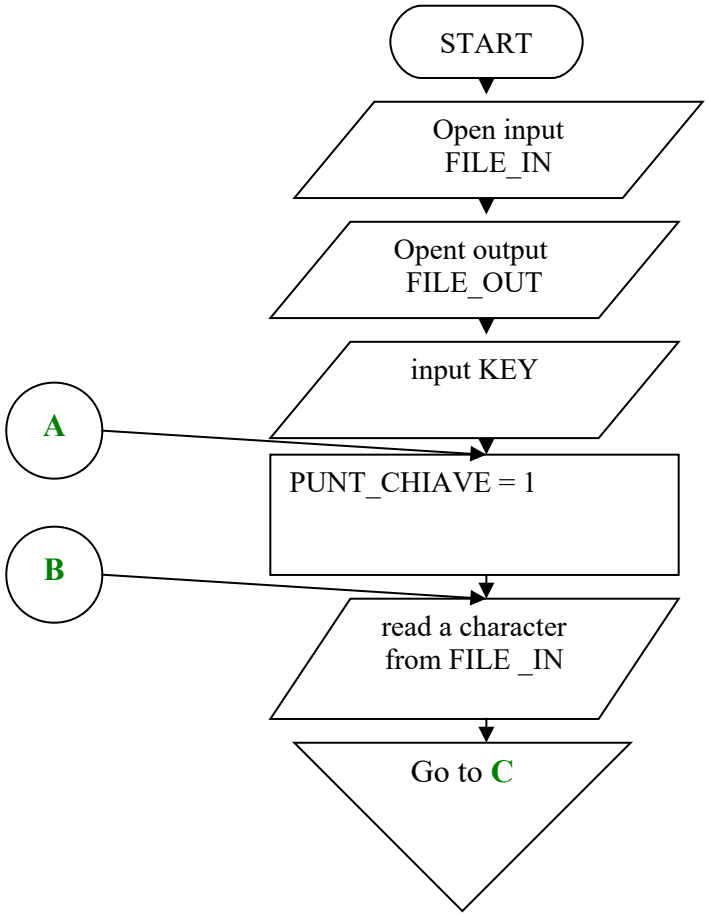
For example, X_1 are data bit and X_2 those of key. Applying the operator on original data we obtain the sequence 0 1 1 0 (see Table 1) and if we apply on this sequence the operator XOR again, using the same key of course, we get the sequence 0 0 1 1 (see Table 2) that is original data.

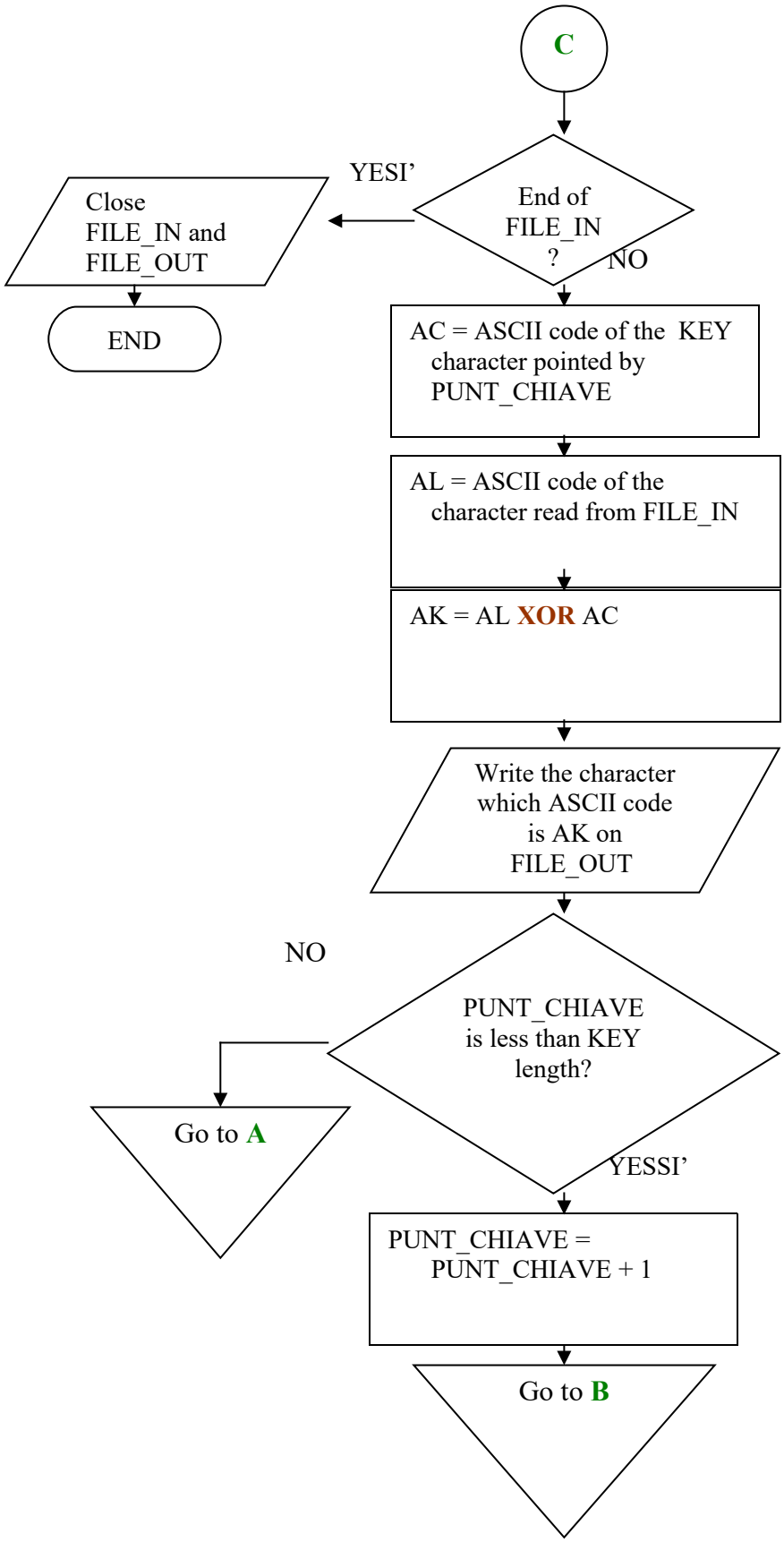
Table 2

X_1	X_2	X_1 XOR X_2
0	0	0
1	1	0
1	0	1
0	1	1

Therefore, it is necessary to know the “key” used to code data in order to get original data. That means we have to use “keys” of ten or more characters to obtain a good “confusion” of our data.

Example of cryptography




C
End of FILE_IN ?
YESI'
NO
Close FILE_IN and FILE_OUT
END
AC = ASCII code of the KEY character pointed by PUNT_CHIAVE
AL = ASCII code of the character read from FILE_IN
AK = AL XOR AC
Write the character which ASCII code is AK on FILE_OUT
PUNT_CHIAVE is less than KEY length?
NO
Go to A
YESSI'
PUNT_CHIAVE = PUNT_CHIAVE + 1
Go to B

The same algorithm sounds good to obtain original data; it is sufficient to open in input the file with coded data while in output we get the file with original data.

If original file contains a long sequence of NUL characters (or a long sequence of spaces) it could be easy to obtain the key simply reading coded file. In order to avoid that, it is better to repeat cryptography on coded data using an other key with the same length but different, characters in same position must be different. Therefore, in above flow-chart, we could ask the user to enter two keys: if we indicate with AS the ASCII code of the second key character pointed by PUNT_CHIAVE, we have to change the instruction XOR in: AK = (AL XOR AC) XOR AS.

Note that it is not important the order you consider ASCII codes (XOR has commutative and associative proprieties).

An other trick is changing the extension of coded file (for example we could use the extension .DLL) in order to divert the attention of the most curious people.

The following code is an easy Visual Basic translation of above flow-chart. You have to add the following controls on the form:

Text1 – write here “input file” name;
Text2 – write here “output file” name;
Text3 – write here the “key”;
Command1 - in the event “Click” you have to copy the following code.

```
Private Sub Command1_Click()
   On Error GoTo GestErrore
   Dim LunKey As Integer, CurPos As Long
   Dim Chiave As String, C1 As String * 1
```

```
    Chiave = Trim(Text3.Text): LunKey = Len(Chiave)
    If LunKey < 10 Then
       MsgBox “Use a key of ten or more characters!”
        Text3.SetFocus
        Exit Sub
    End If
    Open Text1.Text For Binary As #1
    Open Text2.Text For Output As #2
        CurPos = 1
        While Loc(1) < LOF(1)
          Get #1, , C1
          Print #2, Chr(Asc(Left(C1, 1)) Xor _
             Asc(Mid(Chiave, CurPos, 1));
           If CurPos < LunKey Then
              CurPos = CurPos + 1
           Else
              CurPos = 1
           End If
        Wend
    Close
    MsgBox "End!"
    Exit Sub
GestErrore:
                                                                  Close

Close
    MsgBox Err.Description & "!"
End Sub
```