CRITTOGRAFIA DEI DATI

by

A Strange Site

http://astrangesite.altervista.org

Powered by dott. Alessandro Strano

La crittografia consiste nell'uso di un codice che sia di difficile comprensione da parte di chi non lo conosca.

Un semplice ma efficace sistema di crittografia consiste nel "mascherare" i dati utilizzando una "chiave alfanumerica" e l'operatore logico OR-esclusivo (di seguito XOR). Per ottenere i dati originari è sufficiente eseguire l'operatore XOR su quelli codificati utilizzando la medesima chiave.

Tavola 1

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

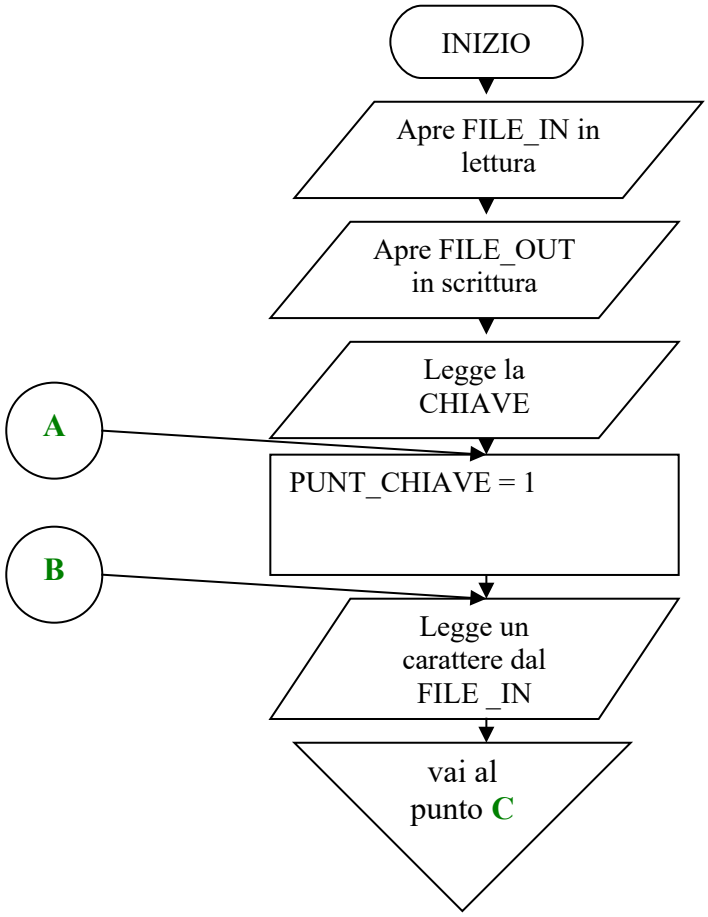
Siano ad esempio X_1 i bit originari e X_2 quelli della chiave. L'applicazione dell'operatore sui dati originari produce la sequenza 0 1 1 0 (vedi Tavola 1) se su di questa applichiamo nuovamente l'operatore XOR, utilizzando ovviamente la stessa chiave, otteniamo la sequenza 0 0 1 1 (vedi Tavola 2) cioè i dati di partenza.

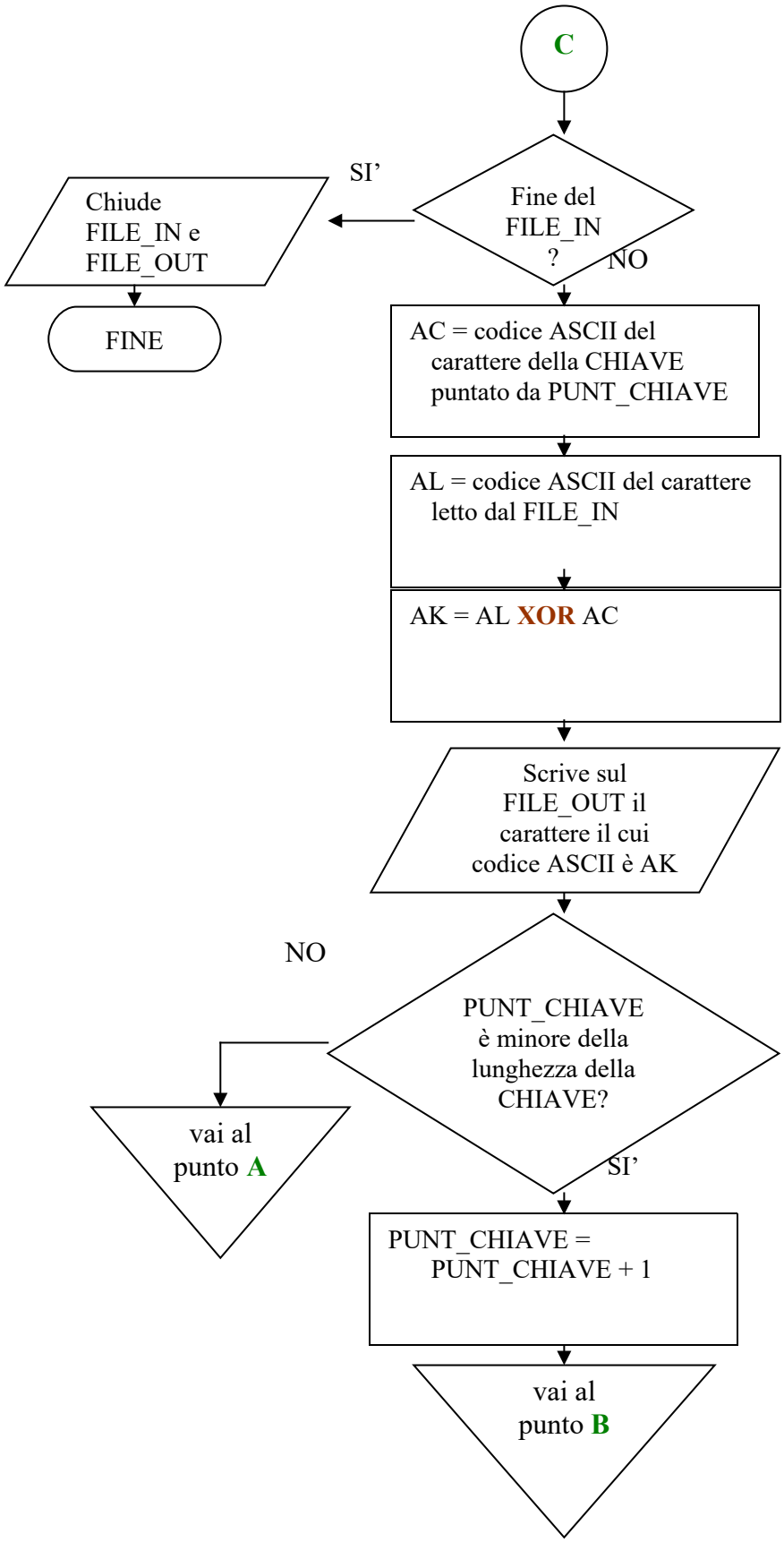
Tavola 2

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

Per risalire ai dati originari occorre pertanto conoscere la "chiave" che è stata impiegata per codificarli. Un primo accorgimento consiste quindi nell'uso di "chiavi" piuttosto lunghe (almeno 10 caratteri) al fine di ottenere una buona confusione dei dati.

Esempio di crittografia




C
Fine del FILE_IN ?
SI'
NO
Chiude FILE_IN e FILE_OUT
FINE
AC = codice ASCII del carattere della CHIAVE puntato da PUNT_CHIAVE
AL = codice ASCII del carattere letto dal FILE_IN
AK = AL XOR AC
Scrive sul FILE_OUT il carattere il cui codice ASCII è AK
PUNT_CHIAVE è minore della lunghezza della CHIAVE?
NO
SI'
vai al punto A
PUNT_CHIAVE = PUNT_CHIAVE + 1
vai al punto B

Lo stesso algoritmo è valido anche per risalire ai dati di partenza; sarà sufficiente aprire in lettura l'archivio codificato mentre in output otterremo l'archivio originario.

Nel caso in cui l'archivio originario contenga una lunga sequenza di caratteri dal codice ASCII "0" (od anche una lunga sequenza di spazi) da un semplice esame del file crittografato sarebbe agevole risalire alla chiave. Per evitare questo inconveniente è necessario ripetere la crittografia con una chiave della stessa lunghezza della precedente ma differente, nel senso che i caratteri alfanumerici (lettere/numeri) che occupano la medesima posizione devono essere diversi, sui dati già codificati. Riferendoci all'algoritmo riportato sopra, potremmo richiedere all'utente di inserire due chiavi e pertanto, indicando con AS il codice ASCII del carattere della SECONDA CHIAVE puntato da PUNT_CHIAVE, cambieremo l'istruzione XOR in: AK = (AL XOR AC) XOR AS.

Si badi che non ha affatto importanza l'ordine con cui si considerano i codici ASCII (lo XOR gode delle proprietà commutativa ed associativa).

Un altro particolare accorgimento è quello di modificare l'estensione dell'archivio codificato (si potrebbe ad esempio utilizzare l'estensione .DLL) al fine di sviare l'attenzione dei più curiosi.

Il codice che segue è una semplice codifica in Visual Basic dell'algoritmo riportato sopra. Occorrerà aggiungere i seguenti controlli nel form:

Text1 – in cui indicare «l'archivio da leggere»;
Text2 – in cui indicare «l'archivio da codificare»;
Text3 – in cui indicare «la chiave»;

Command1 - nel cui evento “Click” dovrà essere riportato il codice che segue.

```
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 “Utilizza una chiave di almeno 10 caratteri!”
      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 "Elaborazione conclusa!"
   Exit Sub
GestErrore:
                                                    Close

Close
```

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