Generatori di numeri casuali per la crittografia

Di Cristiano Armellini (cristiano.armellini@alice.it)

Sappiamo che una delle maggiori difficoltà del cifrario perfetto di Vernam è quello di generare un numero casuale (la chiave di crittografia/decrittografia) che sia lunga quanto il messaggio. Un modo per risolvere il problema è quello di generare un numero casuale di dimensione ***n*** pensato come n numeri casuali di numero tra o e 9. Ovvero: ***cas(9)x cas(9) = cas(99***) sta ad indicare per esempio che due numeri casuali tra 0 e 9 generano insieme un numero casuale tra 0 e 99 (qui x è il prodotto insiemistico cartesiano). Possiamo sviluppare una applicazione in VB.NET

```
Module Module1

  Sub Main()
    Dim ran As New Random(Timer)

    Dim n As Integer
    n = 40

    Dim cas(n) As Integer

    Dim i As Long

    For i = 0 To n - 1

      Dim a As Integer
      a = ran.Next(0, 9)
      cas(i) = Int(a)

    Next i

    Console.WriteLine("generazione di un numero  di dimensione n")

    Dim j As Integer

    For j = 0 To n - 1
      Console.Write(cas(j))
    Next j
    Dim temp As String

    temp = Console.ReadLine()

  End Sub

End Module
```

Possiamo usare anche l'Excel mettendo in ogni cella un numero casuale (generato tramite la funzione casuale()).

Generare numeri così grandi potrebbe avere un'altra applicazione: si genera un numero di 100 cifre e si verifica tramite un test di primalità se è primo: dopo alcuni tentativi si trova il numero primo. Poi si prosegue cercando un secondo primo di dimensione diversa (ad esempio da 120 cifre). Dopo alcuni tentativi si trova anche il secondo numero primo. Quindi si moltiplicano i due numeri e si inizia il processo crittografico secondo l'algoritmo RSA.