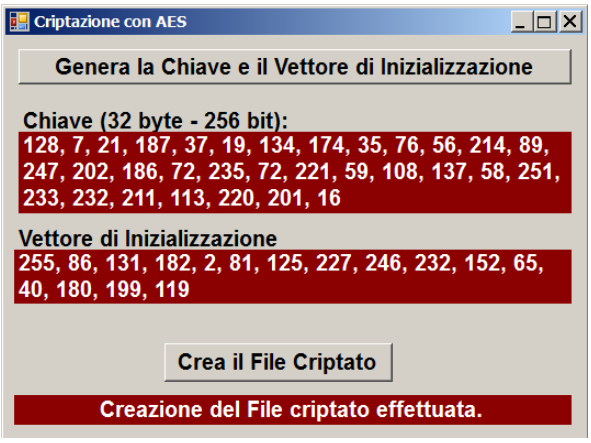
Esempio Pilota:

AES

Definizione della Form



Codice della Form

```
using System;
using System.Windows.Forms;
using System.IO;
using System.Security.Cryptography;

namespace AES
{
  public partial class Form1 : Form
  {
    public Form1()
    {
      InitializeComponent();
    }

    byte[ ]  Chiave;
    byte[ ]  VettoreInizializzazione;
```

```
private void PlsGeneraChiavi_Click(object sender, EventArgs e)
    {
      // Crea l'oggetto per usare l'algoritmo AES (classe Aes)
      // N.B.: non si usa "new" ma un metodo statico "Create" …
      Aes mioAES = Aes.Create( );

      // Genera e visualizza la CHIAVE (32 byte - 256 bit) …
      mioAES.GenerateKey( );
      Chiave = mioAES.Key;
      Visualizza (Chiave, lblChiave);

      // Genera e visualizza il
        VETTORE DI INIZIALIZZAZIONE (16 byte - 128 bit) …
      mioAES.GenerateIV();
      VettoreInizializzazione = mioAES.IV;
      Visualizza (VettoreInizializzazione, lblVetIniz);
    }
```

```
    private void Visualizza ( byte[ ] V,   Label lbl)
    {
      lbl.Text = V[0].ToString();
      for (int K = 1; K <= V.Length - 1; K++)
        lbl.Text = lbl.Text + ", " + V[K];
    }
```

```
  private void PlsCripta_Click(object sender, EventArgs e)
  {
    CriptaDati (   "PromessiSposi.txt", "FileCriptato.txt",
                   Chiave, VettoreInizializzazione );
    lblCripta.Text = "Creazione del File criptato effettuata.";
  }
```

```
  private void CriptaDati
          (string NomeFileOriginale, string NomeFileCriptato,
           byte[ ] Chiave, byte[ ] VettoreInizializzazione)
  {
    // Apri il file originale in lettura ...
    FileStream fileOriginale = File.Open
          ( NomeFileOriginale, FileMode.Open, FileAccess.Read );

    // Crea il file destinazione che ospiterà i dati criptati ...
    FileStream fileCriptato = File.Open
          ( NomeFileCriptato, FileMode.Create, FileAccess.Write );

    // Crea l'oggetto per usare l'algoritmo AES (classe Aes)
    Aes mioAES = Aes.Create();

    /* Definisci il CryptoStream: scrivendo in esso i dati
       saranno criptati e riversati sul file di destinazione.
       Il 2° parametro (CreateEncryptor) è un METODO: sarà usato
       automaticamente dal CriptoStream per criptare i dati.
       N.B.: Per decriptare, il metodo è: CreateDecryptor
     */
    CryptoStream FlussoCheCripta = new CryptoStream
      ( fileCriptato,
        mioAES.CreateEncryptor ( Chiave, VettoreInizializzazione ),
        CryptoStreamMode.Write );

    byte[ ] Buffer = new byte[100];   // leggeremo 100 bytes per volta
    long TotaleBytesLetti = 0;

    // Leggi e Cripta fino alla fine del file originale ...

    while (TotaleBytesLetti < fileOriginale.Length)
    {
      // Leggi un blocco (100 bytes) dal file originale ...
      int BytesLetti = fileOriginale.Read (Buffer, 0, 100);

      /* Scrivi il blocco nel CriptoStream ... esso viene
         criptato e scritto nel file di destinazione ... */
      FlussoCheCripta.Write(Buffer, 0, BytesLetti);

      // Aggiorna il totale dei bytes letti finora ...
      TotaleBytesLetti = TotaleBytesLetti + BytesLetti;
    }

    // Chiudi tutti i flussi ...
    FlussoCheCripta.Close();
    fileOriginale.Close();
    fileCriptato.Close();
  }
 }
}
```