**HƯỚNG DẪN SỬ DỤNG THƯ VIỆN MÃ HÓA CỦA .NET**

**(System.Security.Cryptography)**

**1. Các thuật toán mã hóa:**

Lớp cha: SymmetricAlgorithm

(Các thao tác: sinh khóa, IV, mã hóa, giãi mã thực hiện theo phương thức chung của lớp cha này, các lớp con chỉ thay đổi thuật toán – khái niệm quá tải hàm override của lập trình hướng đối tượng)

Các lớp con kế thừa: DES, TripleDES, Aes

private SymmetricAlgorithm GetAlgorithm()

{

switch (cboAlgorithm.Text)

{

case "DES": return DES.Create();

case "TripleDES": return TripleDES.Create();

case "AES": return Aes.Create();

default: return DES.Create();

}

}

**2. Sinh khóa và IV:**

var cipher = GetAlgorithm();

cipher.GenerateKey();

cipher.GenerateIV();

txtKey.Text = BitConverter.ToString(cipher.Key).Replace("-", "").ToLower();

txtIV.Text = BitConverter.ToString(cipher.IV).Replace("-", "").ToLower();

**3. Mã hóa và giải mã:**

var fsIn = new FileStream(txtFile1.Text, FileMode.Open);

var fsOut = new FileStream(txtFile2.Text, FileMode.Create);

var cipher = GetAlgorithm();

cipher.Key = HexaStringToBytes(txtKey.Text);

cipher.IV = HexaStringToBytes(txtIV.Text);

ICryptoTransform t;

if (type = "MaHoa") t = cipher.CreateEncryptor();

else t = cipher.CreateDecryptor();

var stream = new CryptoStream(fsOut, t, CryptoStreamMode.Write);

var len = (int)fsIn.Length;

var data = new byte[len];

fsIn.Read(data, 0, len);

stream.Write(data, 0, len);

stream.Close();

fsOut.Close();

fsIn.Close();