

Encrypt a String

An example showing how to encrypt and decrypt a string using a password.

```

//encrypt.boo

import System.Security.Cryptography
import System.Text
import System.IO
import System

def encrypt(s as string) as string:
  return encrypt(s, "d!&%#@?,:")
def decrypt(s as string) as string:
  return decrypt(s, "d!&%#@?,:")

def encrypt(s as string, key as string) as string:
  salt = array(byte,[0x12,0x34,0x56,0x78,0x90,0xAB,0xCD,0xEF,0xDD,0x31])
  try:
    pdb = PasswordDeriveBytes(key,salt)
    alg = Rijndael.Create()
    alg.Key = pdb.GetBytes(32)
    alg.IV = pdb.GetBytes(16)
    ms = MemoryStream()
    cs = CryptoStream(ms,alg.CreateEncryptor(),CryptoStreamMode.Write)
    sbytes = Encoding.UTF8.GetBytes(s)
    cs.Write(sbytes,0,len(sbytes))
    cs.FlushFinalBlock()
    return Convert.ToBase64String(ms.ToArray())
  except e:
    return "ERROR: " + e.Message

def decrypt(s as string, key as string) as string:
  salt = array(byte,[0x12,0x34,0x56,0x78,0x90,0xAB,0xCD,0xEF,0xDD,0x31])
  try:
    pdb = PasswordDeriveBytes(key,salt)
    alg = Rijndael.Create()
    alg.Key = pdb.GetBytes(32)
    alg.IV = pdb.GetBytes(16)
    ms = MemoryStream()
    cs = CryptoStream(ms,alg.CreateDecryptor(),CryptoStreamMode.Write)
    inputbytes = Convert.FromBase64String(s)
    cs.Write(inputbytes,0,len(inputbytes))
    cs.FlushFinalBlock()
    return Encoding.UTF8.GetString(ms.ToArray())
  except e:
    return "ERROR: " + e.Message

samplestring = "Hello, test message."
print samplestring
enc = encrypt(samplestring, "mypasswd")
print "encrypted:", enc
dec = decrypt(enc, "mypasswd")
print "decrypted:", dec
print "bad password:", decrypt(enc, "badpassword")

```

See also:

- [AES for Crypto Interop between Java and .NET](#)