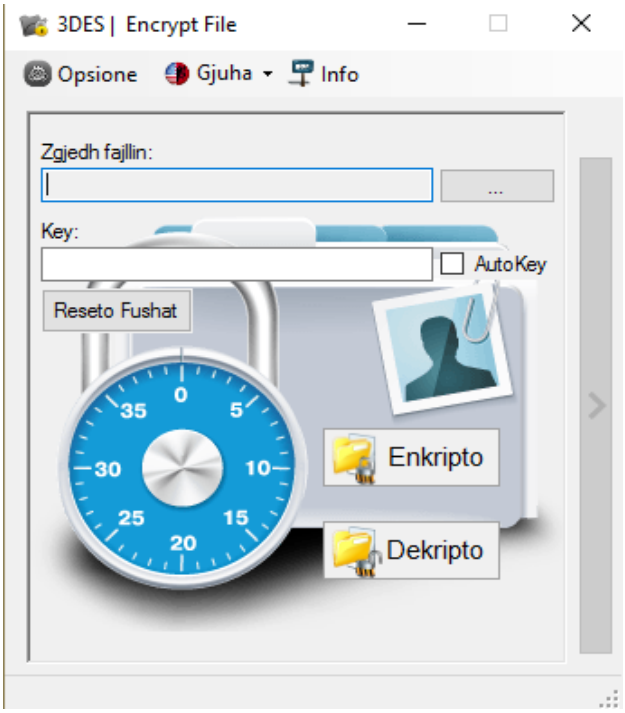
Universiteti i Prishtinës ‘Hasan Prishtina’
Fakulteti i Inxhinjerisë Elektrike dhe Kompjuterike
Prishtinë



Enkriptimi/Dekriptimi i file-it me 3DES

Profesori: prof.Dr. Blerim Rexha

Mentori: Prof. Ilir Murturi

Studenti: Arton Hoti

11.12.2016

Përmbajtja

Qëllimi i projektit

Krijimi i programit që mundëson enkriptimin me 3DES të një fajlli, të cilin ne mund t'a zgjedhim. Programi të mundësoj shkruarjen e celsit enkriptues dhe gjithashtu ketë si alternativë gjenerimin automatik të celsit enkriptues.
Ky program duhet të bëj leximin brenda file-it, të enkriptoj dhe të ruaj celsin enkriptues në mënyrë që faili i enkriptuar pas një kohë (Stop runnning → Start) të mund të dekriptohet me atë celës!

Koncepte të përgjithshme për (3)DES-in

Triple Data Encryption Algorithm 3DES i cili pastaj bënë Data Encryption Standard (DES) tri herë në secilin bllok me të dhëna.
Algoritmi DES përdorë celsin me gjatësi 56 bitesh, tanimë nuk është shumë i sigurtë sepse me kompjuter të fuqishëm ai mund të thyhet me bruteforce dhe për t'i ikur këtij rreziku 3DES-i përdor celsin 3*56=168 bit (mund të përdorë cels edhe me 115 bit).
Celsat mund të jenë:

1. Celsat të pavarur Key1 ≠ Key2 ≠ Key3 (që e bënë të pamundur BruteForce-in).
2. Key1 dhe Key2 janë të pavarur, ndërsa Key3 = Key1. (celës 112bitsh)
3. Të tre celsat janë të njejtë Key1 = Key2 = Key3 (është njejtë sikur DES-i, 56bit).

Algoritmi

Teksti i enkriptuar (ciphertext) është rezultat i përbërë nga:

1. Enkriptimi të tekstit (plaintext) me celsin Key1
2. Dekriptimi i tekstit me celsin Key2 i asaj që fitohet pas pikës të lartë përmendur 1.
3. Enkriptimi i tekstit që fitohet nga pika e lartë përmendur 2.

$$ciphertext = E_{Key3}(D_{Key2}(E_{Key1}(plaintext)))$$

Dekriptimi është i anasjelltë:

$$plaintext = D_{Key1}(E_{Key2}(D_{Key3}(ciphertext)))$$

Modi enkriptues i cili është përdorur në këtë projekt është CBC, ky mod është më i sigurtë pasiqë në bllokun e parë përdor IV (vektorin inicializues) dhe hyrja e bllokut tjetër përdorë daljen e bllokut paraprak.

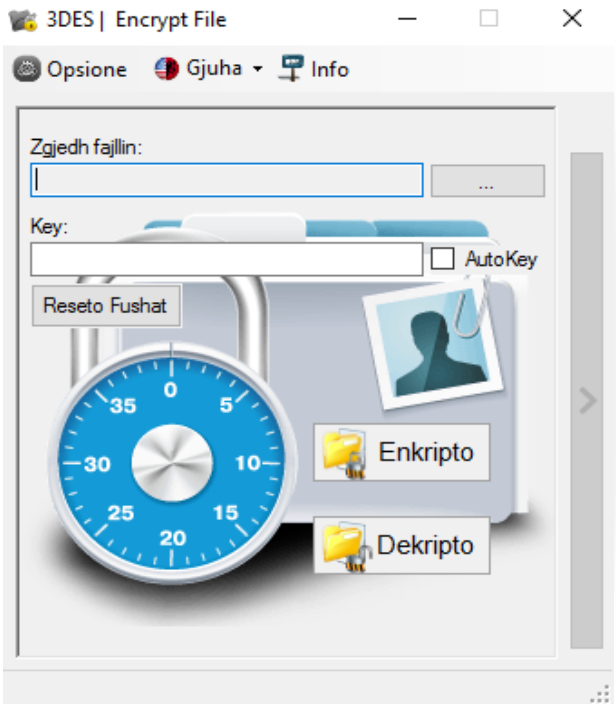
Përdorimi i 3DES-it

3DES-i gjenë përdorim në industrit e pagesave elektronike, në Microsoft OneNote, Microsoft Outlook 2007, Microsoft System Center Configuration Manager 2012 përdorë Triple DES për mbrojtjen password-it të user-ave dhe të dhënat e sistemit.

Testimi i programit dhe kodi esancial i tij

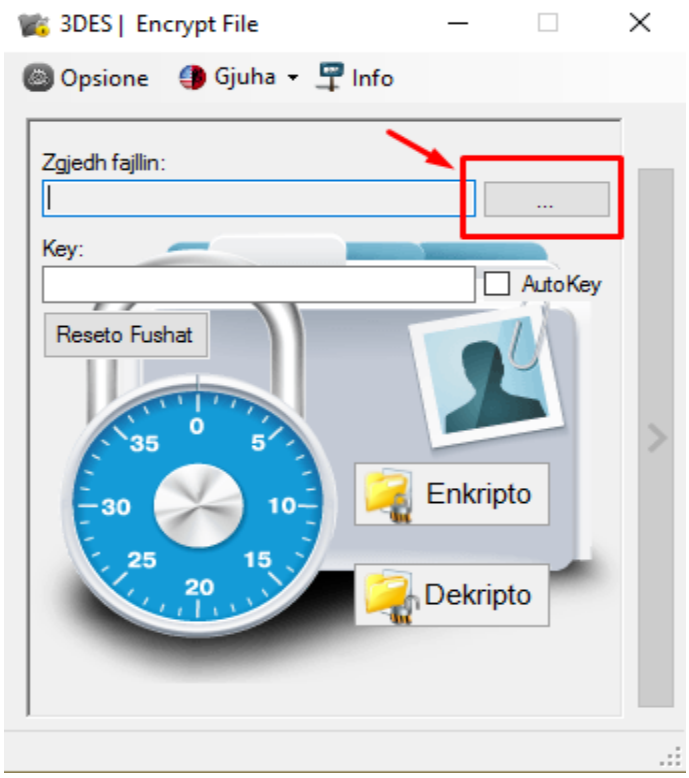
1. Startimi i '3DES | Encrypt File'

Pas startimi të programit hapet një dritare me madhësi fikese 359x423 pixel. Forma është e thjeshtë dhe e vetëkuptueshme, ka të implementuar dy gjuhë (Shqip dhe Anglisht) e parazgjedhur është gjuha Shqipe.



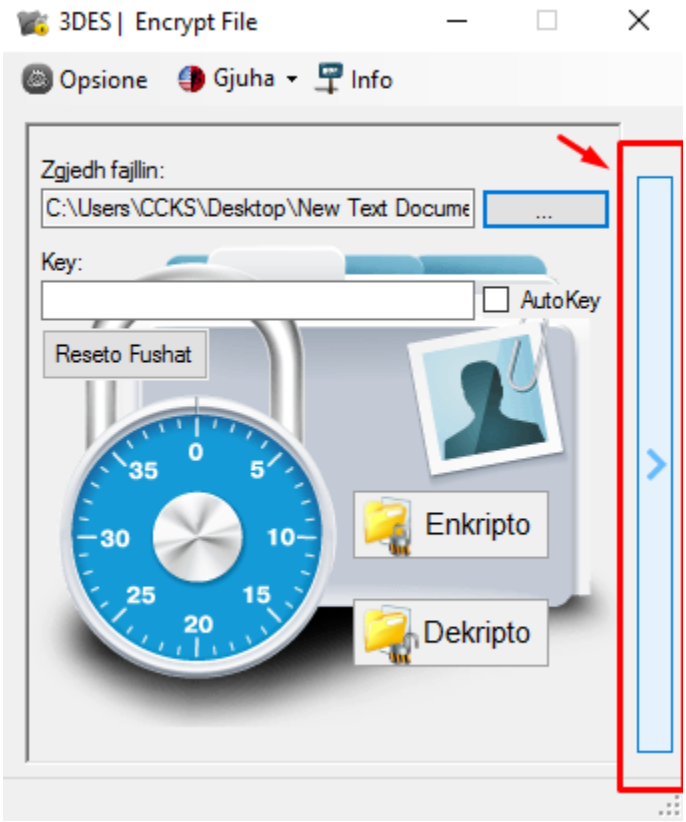
2. Perzgjedhja e file-it

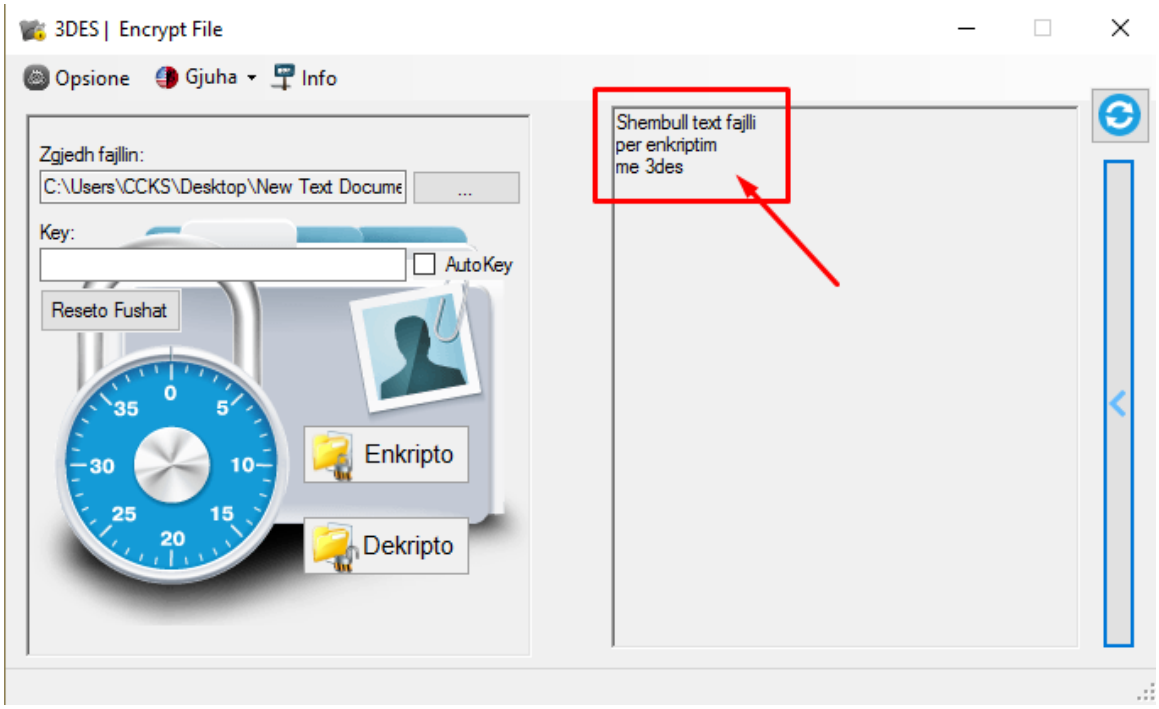
Ne duhet ta zgjedhim file-in të cilin deshirojmë t'a enkriptojmë. Këtë e bëjmë duke klikuar në butonin ' … '.
Anash këtij butoni "…" është butoni " > " i cili do t'a rritë formen horizontalisht dhe brenda tij do t'a shfaqë përmbajtjen e file-it të cilin e zgjedhim.
Përderisa nuk është zgjedhur ende file-i, ky buton " > " mbetet i palejueshëm (not enabled).



3. Leximi i file-it të përzgjedhur

Tani që është zgjedhur file-i, lejohet klikimi i butonit ">" i cili na mundëson ta shohim përmbajtjen e atij file-i. Klikojmë dhe na shfaqet pamja e më poshtme.



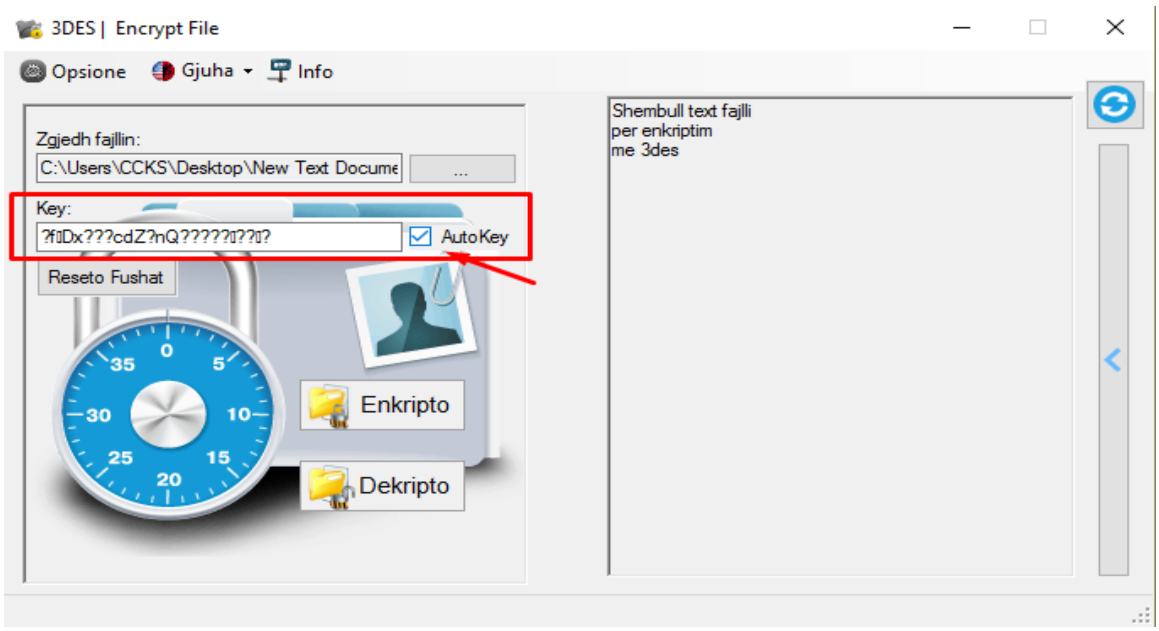


4. Vendosja e celsit

Vendosja e celsit mund të bëhet në dy mënyra:

1. Duke shkruajtur celsin në fushën përkatëse
2. Duke vendosur '√' në AutoKey

Vlenë të ceket se gjeneruesi i celsit automatik përdor RandomNumberGenerator që e krijon një celes me madhësi 192bita që e bënë shumë të sigurtë, mund të themi se ky është Random, gjithmonë krijohet një i ri. (E kemi testuar)

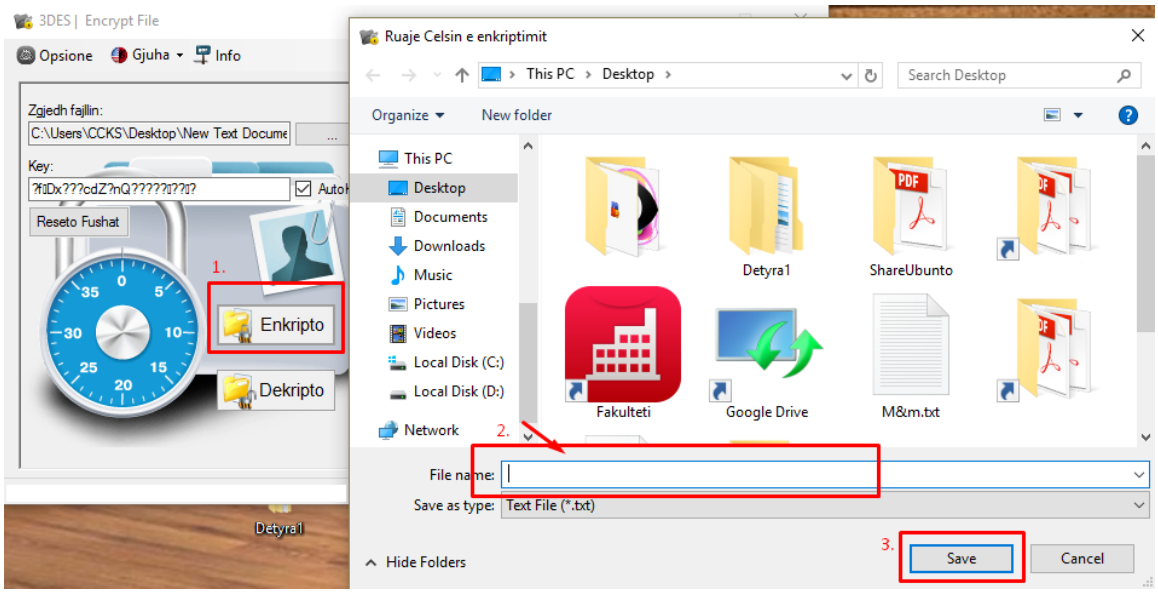


Kodi për gjenerim automatik te ketij celesi është:

```
private void AutoKey_CheckedChanged(object sender, EventArgs e)//Gje
{
    if (chAutoKey.Checked)
    {
        RandomNumberGenerator rng = RandomNumberGenerator.Create();
        byte[] key = new byte[24];
        rng.GetBytes(key);
        txtkey.Text = Encoding.ASCII.GetString(key);
    }
    else txtkey.Clear();
}
```

5. Enkripto file-in

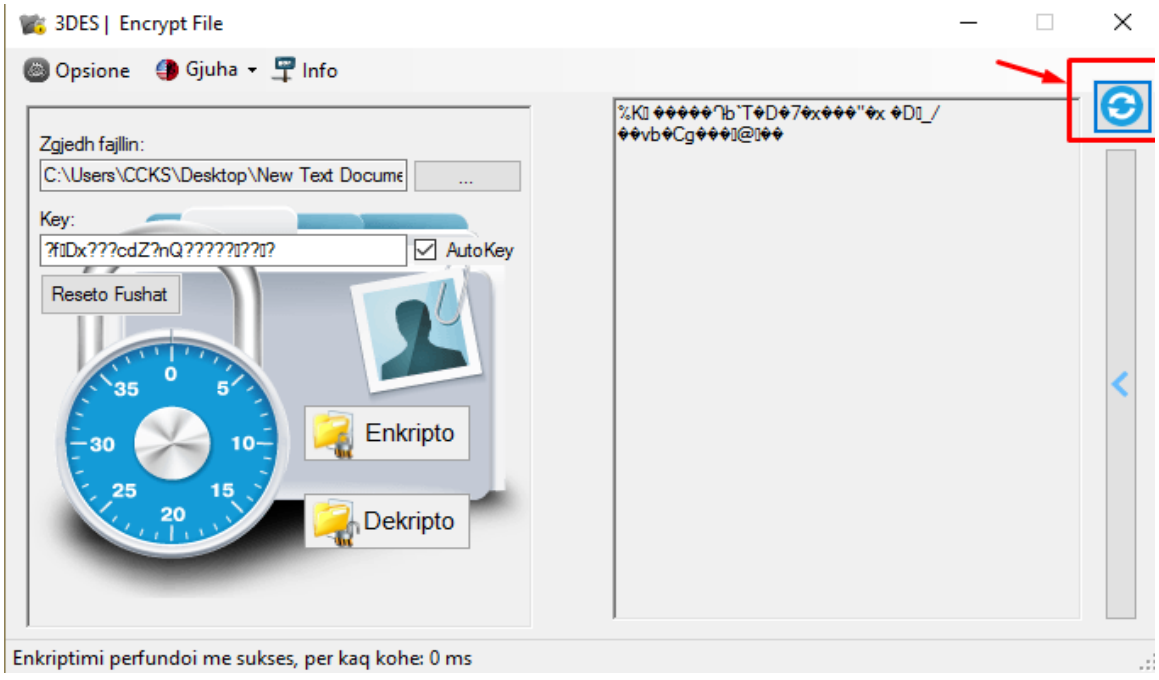
Me klikimin e butonit ‘Enkripto’ neve do të na hapet një dritare e re ‘Ruaje Celsin e Enkriptimit’ në të cilen ne e zgjedhim path-in, shkruajm emrin me të cilin dëshirojmë ta ruajmë celsin.



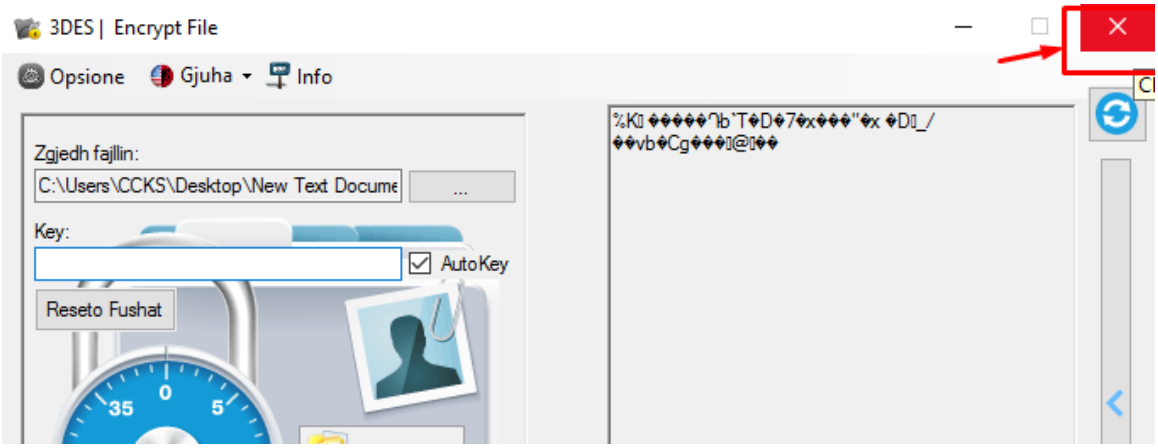
Kodi i butonit ‘Enkripto’ është si më poshtë:

```
    tDES.Key = utf8.GetBytes(txtkey.Text);  //me utf8 merr edhe disa karaktere tveqanta
    tDES.Mode = CipherMode.CBC;
    tDES.IV = utf8.GetBytes("06041995");
    tDES.Padding = PaddingMode.Zeros;

    StreamReader sr = new StreamReader(txtFajlli.Text);
    string permbajtja = sr.ReadToEnd();
    sr.Close();
    FileStream fs1 = new FileStream(txtFajlli.Text, FileMode.Create, FileAccess.Write);
    CryptoStream cs = new CryptoStream(fs1, tDES.CreateEncryptor(), CryptoStreamMode.Write);
    StreamWriter sw = new StreamWriter(cs);
    sw.Write(permbajtja);
    sw.Flush();
    sw.Close();

    int fundi = DateTime.Now.Millisecond;

    //Ruajtja e qelsit ne fajll
    string permbajtjaQelsit = txtkey.Text;
    SaveFileDialog saveFD = new SaveFileDialog();
    saveFD.InitialDirectory = Convert.ToString(Environment.SpecialFolder.Desktop);
    saveFD.Title = titulliNeRuajtjeTeCelsit;
    saveFD.Filter = "Text File|*.txt|Word Document|*.docx";
    saveFD.FilterIndex = 1;
    if (saveFD.ShowDialog() == DialogResult.OK && saveFD.FileName.Length > 0)
    {
        FileStream fs2 = new FileStream(saveFD.FileName, FileMode.Create, FileAccess.Write);
        StreamWriter sw2 = new StreamWriter(fs2);
        sw2.Write(permbajtjaQelsit);
        sw2.Flush();
        sw2.Close();
    }
```

E kemi enkriptuar file-in dhe e kemi ruajtur celsin, pastaj klikojmë këtu për t'a parë përmbajtjen brenda file-it se a ka ndryshuar!
-shohim se është enkriptuar (kjo përmbajtje është e drejtpërdrejt nga faili origjinal).
Gjithashtu programi kalkulon kohen e enkriptimit nëse gjithcka shkon mirë!

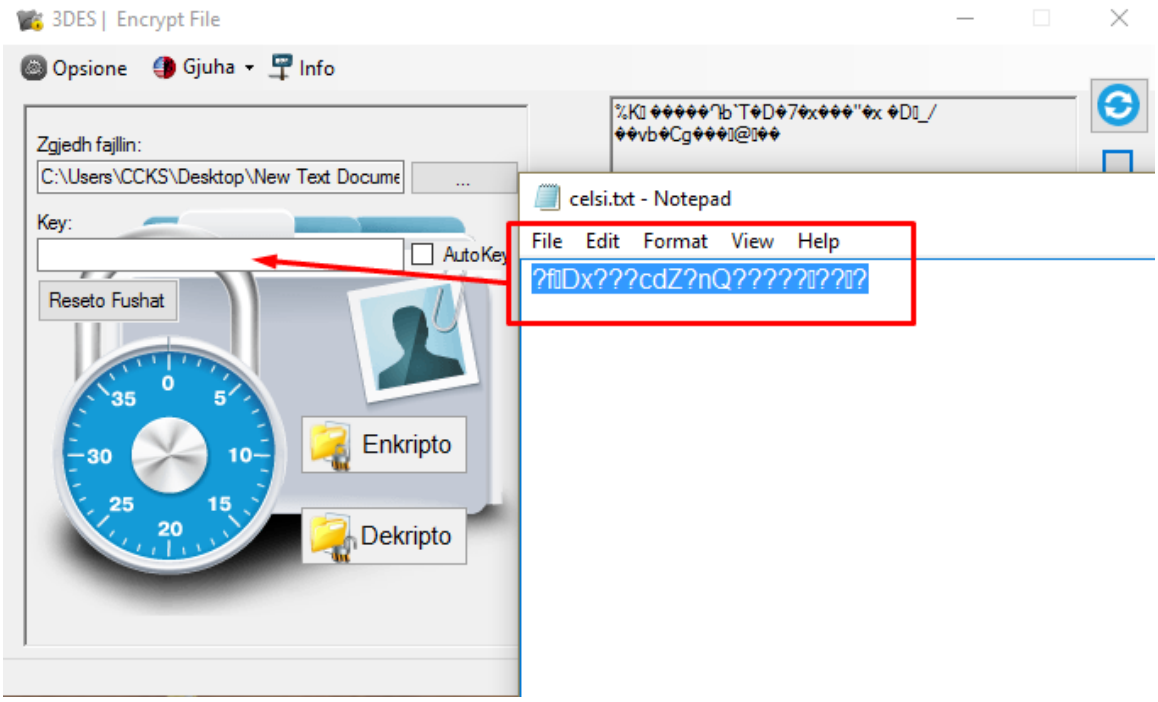


E mbyllim ekzekutimin e programit për ta testuar dekriptimin.

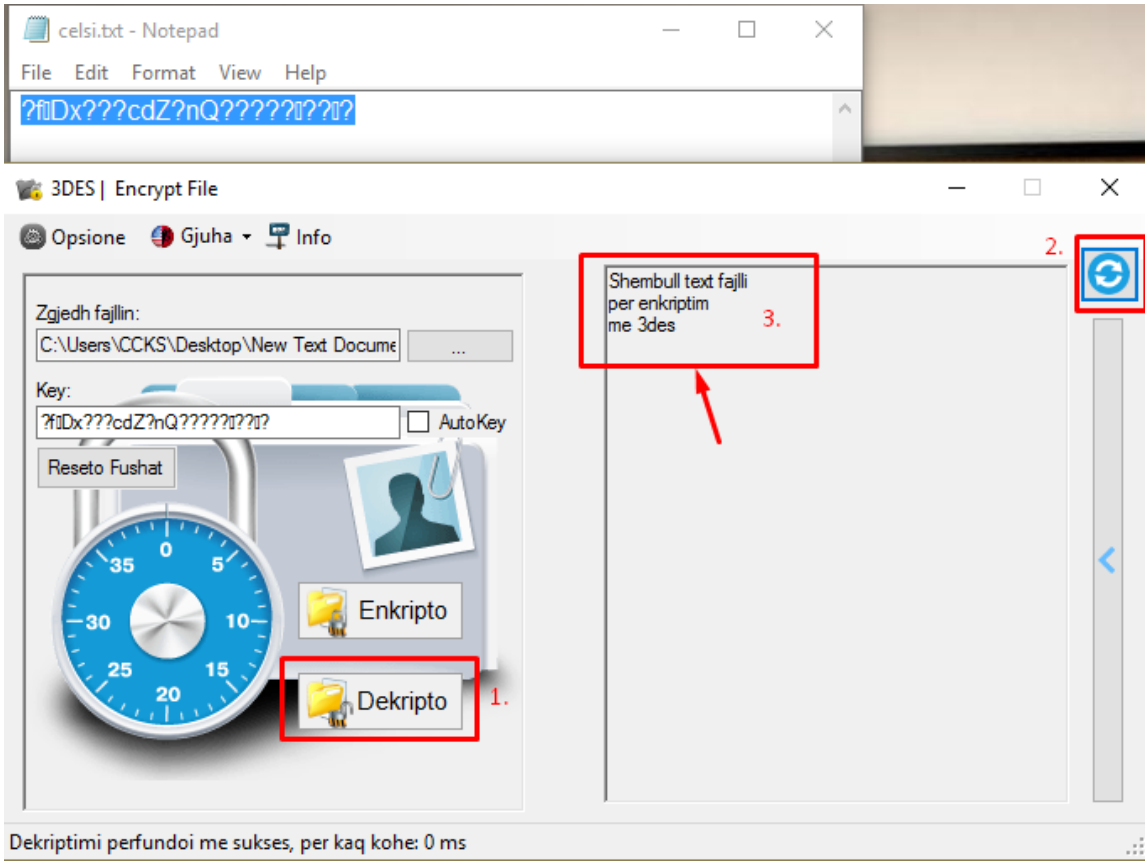


6. Dekripto file-in

E startuam edhe njëherë programin, e zgjodhëm file-in e enkriptuar, e hapëm edhe tekst dokumentin me celësin enkriptues që e kemi ruajtur më herët, tani e vendosim celsin.



Dhe klikojmë ‘Dekripto’, pastaj e klikojmë edhe butonin ‘Refresh’ për t’a parë përmbajtjen e re në atë file!

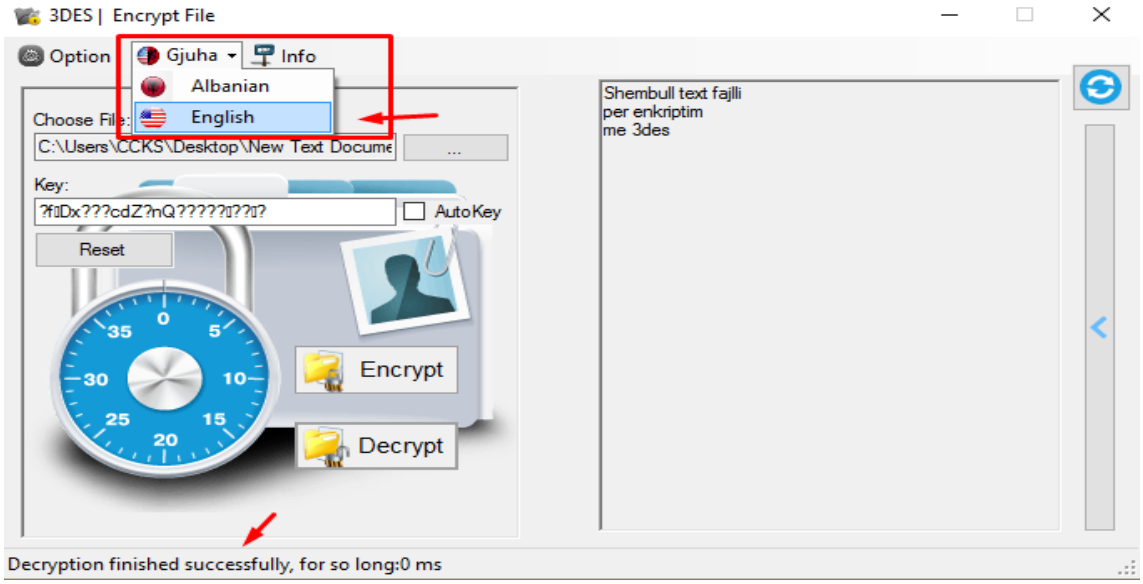


-është enkriptuar me sukses me celës të njejtë dhe përmbajtja tani është e lexueshme.
Dekriptimi zgjati shumë shpejtë, meqë në file ka pak fjali.
Kodi i butonit 'Dekripto' është paraqitur më poshtë:

```
{
    fillimi = DateTime.Now.Millisecond;
    tDES.Key = utf8.GetBytes(txtkey.Text);
    tDES.Mode = CipherMode.CBC;   //modi enkriptues Cipher Block Chaining each block of plain
    tDES.IV = utf8.GetBytes("06041995");
    tDES.Padding = PaddingMode.Zeros;

    FileStream fs = new FileStream(txtFajlli.Text, FileMode.Open, FileAccess.Read);
    CryptoStream csDec = new CryptoStream(fs, tDES.CreateDecryptor(), CryptoStreamMode.Read);
    StreamReader sr = new StreamReader(csDec);
    string permbajtja = sr.ReadToEnd();
    sr.Close();
    fs.Dispose(); fs.Close();

    int fundi = DateTime.Now.Millisecond;
    tstStatusi.Text = statusiD + (fundi - fillimi) + " ms";

    StreamWriter sw = new StreamWriter(txtFajlli.Text);
    sw.Write(permbajtja);
    sw.Flush();
    sw.Close();
}
```

7. Dy gjuhësi

Programi mund të përdoret edhe nga përdorues të cilët përdorin gjuhën Angleze.



8. Informata rreth projektit

Një formë e thjeshtë në të cilën është treguar shkurtimisht projekti poashtu ajo përbëhet edhe nga info rreth të tre anëtarëve të projektit.
Largimi i kësaj dritare ‘info’ bëhet duke klikuar kudo në hapësirë tjetër (jo në të).