XGEN R&D

SaveNet

Hojda Adelin

Prof. coord. Andrea Burcuș

Colegiul Național „Dragoș Vodă” Sighetu Marmației

XGEN R&D

Introducere

- Importanța securității în IT
- Protejarea documentelor
- Algoritmi de criptare obișnuiți
- Algoritmul de criptare cu caractere ASCII
- Aplicația SaveNet
- Concluzie

Importanța securității în IT

De ce este necesară securitatea în IT?

- Pentru a nu pierde informații importante.
- Pentru a preveni daunele materiale sau cele îndreptate către oameni.

Cine creează daune?

- Virușii lăsați liberi pe internet.
- Hackerii sub denumirea de “Black hat”.

Cum prevenim daunele și pierderea informațiilor?

- Folosind instrumente profesionale de securitate.
- Prin prudență.

Protejarea documentelor

Deși securitatea cibernetică nu este doar despre partea locală, aici se dau cele mai multe atacuri. Hackerii știu că persoanele obișnuite, fără cunoștințe în securitate cibernetică, sunt o țintă ușoară de aceea majoritatea atacurilor sunt îndreptate către populație. Persoana atacată, neavând cunoștințele necesare, va fi pradă acestor hackerii și va suferi daune însemnate, poate pierde sau i se pot deteriora documente importante, poze, etc.

Soluții:

- Criptarea acestor documentelor importante.
- Păstrarea lor în medii virtuale.

XGEN R&D

Algoritmi de criptare obișnuiți

AES(Advanced Encryption Standard) este cel mai cunoscut algoritm de criptare folosit în toată lumea.

DES(Data Encryption Standard) este printre primii algoritmi de criptare care la momentul de față este considerat învechit dar tot folosit de marea majoritate a aplicațiilor de criptare.

Problemele acestor algoritmi de criptare:

- Fiind foarte folosiți, virușii avansați înțeleg mai bine motorul din spatele acestor algoritmi, decriptând cu ușurință conținutul.
- Vulnerabilitatea în fața forței brute.

XGEN R&D

Algoritmul de criptare cu caractere ASCII

Soluția mea pentru aceste defecte ale algoritmilor clasici este algoritmul bazat pe caractere ASCII.

Trăsături:

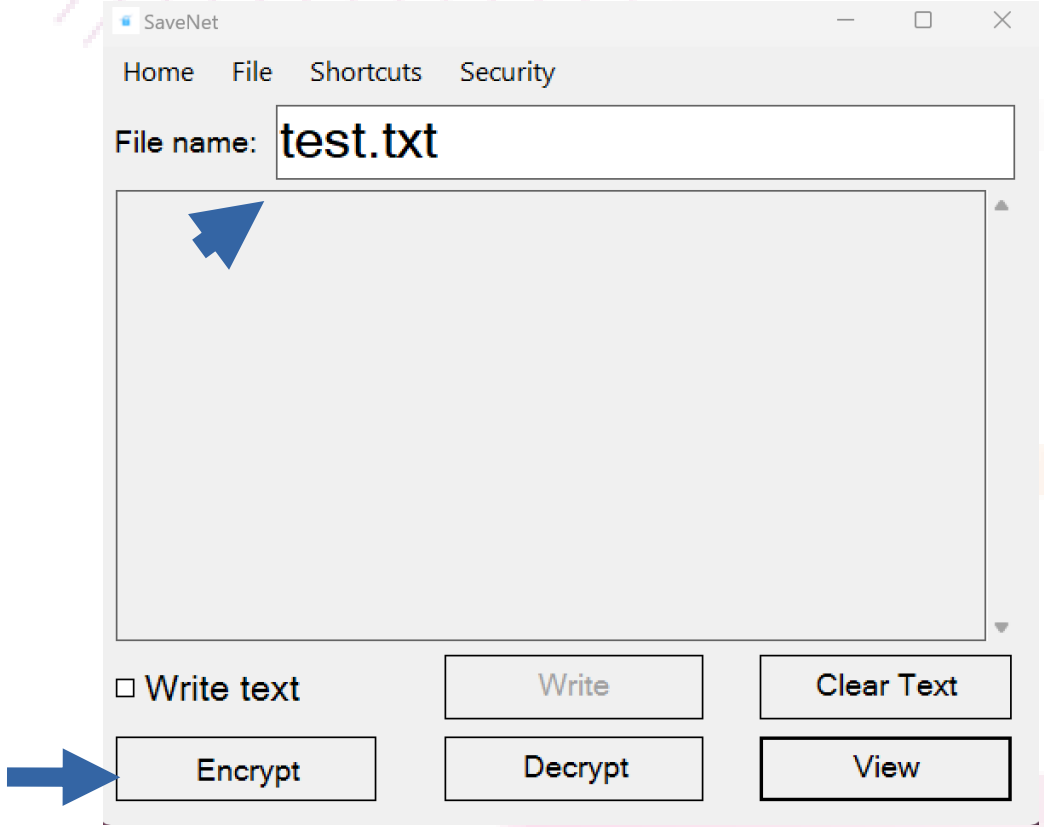
- Algoritmul utilizează extinderea de caractere ASCII neregăsite în tabelul obișnuit.
- Algoritmul este nou și dificil pentru viruși de a decripta conținutul, fiind probabil bazați pe algoritmi clasici
- Caractere unice îl fac rezistent la atacurile frecvente deoarece hackerii tind să utilizeze metode standard de decriptare (forța brută, dicționarul, etc)

Aplicația SaveNet

Pentru a folosi acest algoritm putem utiliza programul SaveNet dezvoltat de mine în C++ bazat pe acest algoritm.

Modul de criptare:

1. Introducem numele fișierului
2. Apăsăm pe butonul “Encrypt”
3. Intrăm din nou în fișier



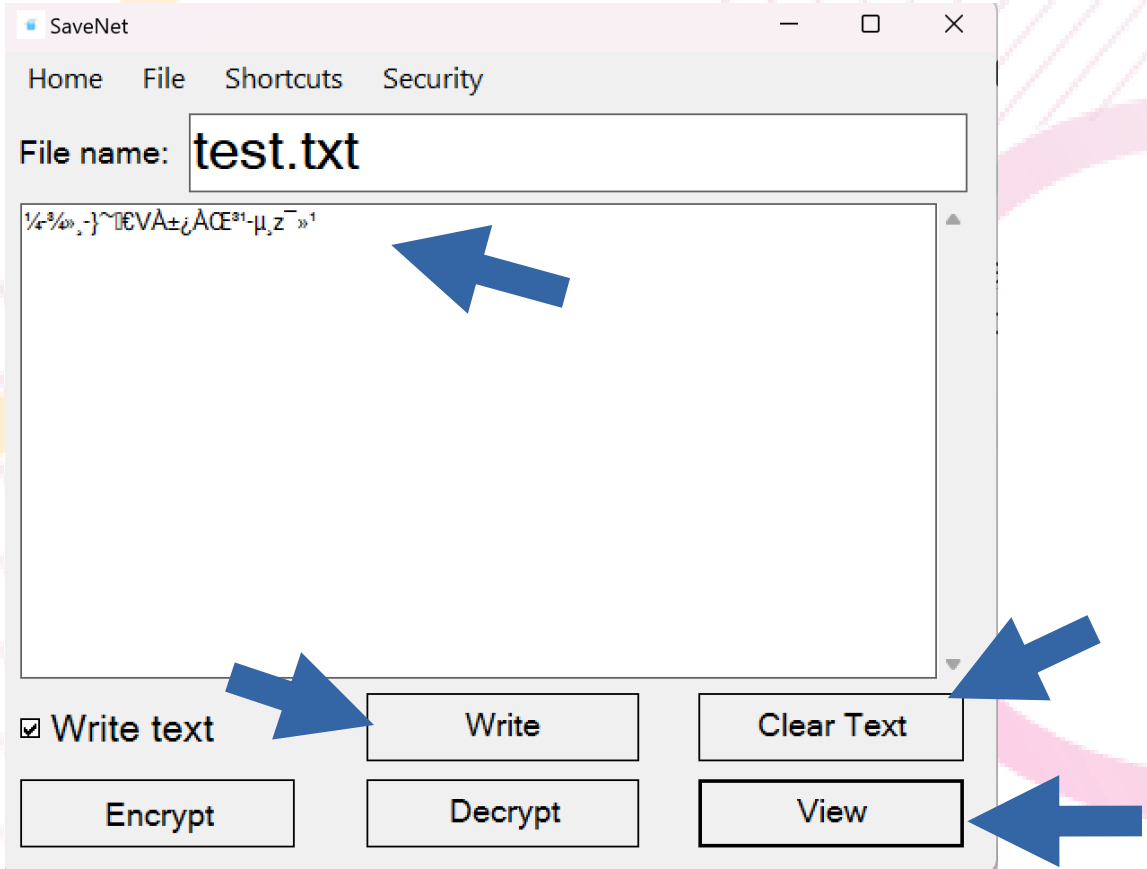
- Din conținutul fișierului fără criptare s-a ajuns la:

```
parola1234
test@gmail.com
```

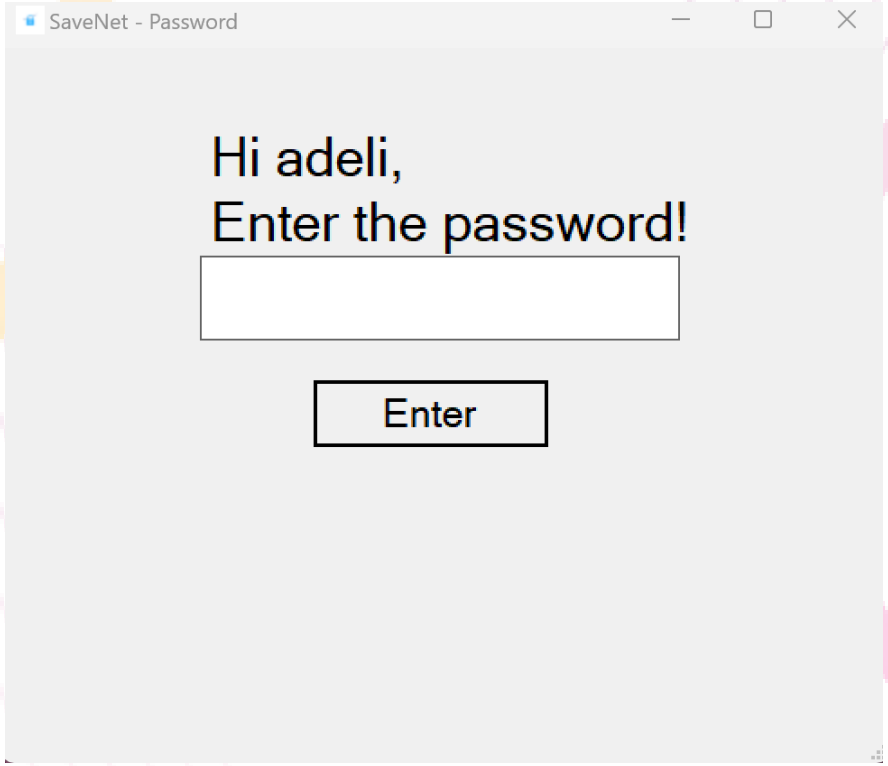
```
¼¾» ¸ }~□€VÀ±¿ÀŒ³¹µ¸z¯»¹
```

Modul de decriptare este la fel de simplu apăsând pe butonul “Decrypt”.

Aplicația dispune de funcți care afișează conținutul direct în aplicație fără a mai intra în fișier utilizând funcțiile “Write”, “View”, “Clear text”



Pentru a nu lăsa persoane neautorizate să decripteze fișierele utilizând această aplicație, aplicația are un mecanism numit “Local password” care creează o parolă locală criptată tot cu acest algoritm și care nu lasă orice persoană să acceseze aplicația. Atunci când intrăm în aplicație ni se va fa cere parola creată.



XGEN R&D

Concluzie

Acest algoritm nu se termină aici și va fi actualizat mult timp de acum încolo pentru a servi nevoilor populației de a securiza documentele importante.

Securitatea în IT este foarte importantă din toate punctele de vedere la fel ca alte securități din alte domeni de aceea trebuie să folosim intrumente puternice pentru a ne securiza informațiile.

Aplicația SaveNet și algoritmul de criptare cu caractere ASCII pot fi o soluție ideală pentru acest lucru și pentru a diversifica lumea algoritmilor de criptare care deja sunt foarte cunoscuți de către hackeri.