ŠIFROVAT JAKÝKOLI DOKUMENT

Můžete vidět online fóra a diskuse jako: jak mohu zašifrovat celou složku? (přeneste obsah do souboru ZIP!), soubor PDF? jak zašifruji soubor DOC atd.?

Je to falešný problém, žádný dokument ničím jiným než posloupností n bajtů, takže důležité je pouze získat šifrovaný soubor, kde

byte (n) + algoritmus = šifrovaný byte (n)

a že můžete získat původní dokument zpět

šifrovaný bajt (n) - algoritmus = bajt (n)

Bez ohledu na typ dokumentu bude k dispozici aplikacím, které jej používají, s jeho obsahem a původním názvem.

Šifrování dokumentu

Zašifrované dokumenty můžete pojmenovat libovolně.

Název zdrojového souboru je uložen v zašifrovaném souboru, takže když je dokument dešifrován, je mu automaticky přiřazen původní název, aniž by byl nucen si pamatovat, ke kterému dokumentu se daný soubor vztahuje.

Šifrování textu

To, co píšete z klávesnice, je přímo šifrováno, což je užitečné pro psaní krátkých poznámek nebo zpráv, které se mají připojit k e-mailu.

Jakmile byla zpráva dešifrována, najdete ji v MESSAGE.TXT

AUTENTIFIKACE

Každý šifrovaný dokument obsahuje neopakovatelný identifikační kód (**NIDE)**, který vylučuje jakoukoli možnost manipulace a bezpečně potvrzuje totožnost odesílatele.

Šifrovací systém je ve skutečnosti takový, že stejný dokument, šifrovaný stejným klíčem nkrát, generuje n vždy odlišných šifrovaných souborů, a tedy n různých **NIDE**. (viz technická poznámka výše)

NIDE se zobrazí na konci šifrování, zkontroluje jej systém před dešifrováním každého dokumentu a je v každém případě ověřitelný kdykoli pomocí konkrétní funkce, a proto může odesílatel a příjemce zajistit autentický původ šifrovaného dokumentu a jeho integritu.

Kromě kódu NIDE se zobrazí následující:

- datum vzniku

- název použitého klíče

- kdo dokument zašifroval

- název původního dokumentu

Pro správné rozložení:

- vytvořit zástupce Qcrypto na ploše

- klikněte pravým tlačítkem na ikonu zástupce

- vlastnosti / dispozice

- v rozměrech okna nastaveno 30 na výšku a 102 na šířku

KLÍČOVÝ SOUBOR

Soubor klíčů obsahuje všechny uživatelské klíče ve tvaru:

JMENOKLIC (jasné, vidí to kdokoli) + **KLIC** (které vidíte pouze vy, protože je šifrováno pomocí **SOUBOR KLÍČŮ KLÁVES** CO JSME POŽADOVALI PRVNÍ A KTERÉ PŘICHÁZÍ KAŽDOU DOBU se při vstupu do systému

Jakmile je tedy znám název použitého klíče, je extrahován z archivu a je to pouze systém, který jej může dešifrovat (pomocí SOUBOR KLÍČŮ KLÁVES) a povolit jeho použití.

Jméno / reference vztahující se ke klíči jsou uloženy v šifrovaných souborech, a proto bude dešifrovaný klíč převzat bez udání indikace.

Tato SOUBOR KLÍČŮ KLÁVESO je jediná, kterou si musíte pamatovat, ale MUSÍTE si ji pamatovat, jinak již nikdy nebudete moci obnovit již šifrované soubory, protože

v systému mohou pracovat pouze ti, kdo znají **SOUBOR KLÍČŮ KLÁVES**

KLÍČE

Mohou být generovány pomocí specifické funkce programu a následného přiřazení požadovaného názvu.

Sdílený klíč můžete vytvořit s korespondentem pomocí procesu výměny klíčů.

Proces probíhá ve 2 fázích:

A ---------- data ---- »B, která generuje klíč K

B ---------- data ---- »A která generuje klíč = K

Odkaz je uživatelské jméno korespondenta, je přiřazeno automaticky a umožňuje oběma správám dešifrovat zprávy, protože v každém zašifrovaném souboru, který bude vyměněn, bude uživatelské jméno, se kterým byl sdílený klíč vložen do souboru klíče.

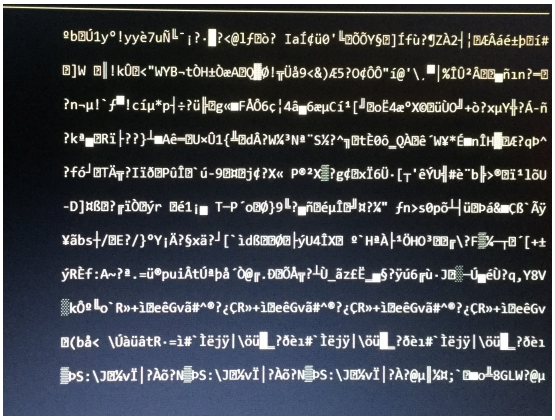
Program ukazuje, která fáze právě probíhá.

Musíte se jen dohodnout, kdo zahájí 1. fázi.

Ke klíčům vytvořeným pro usnadnění identifikace korespondenta lze přiřadit popis.

Klíč lze také importovat do systému pomocí souboru s názvem **KIMPEXP,** který má následující formát: název klíče (24) + uživatelské jméno (24) + klíč (64)

Funkce, která generuje klíče, umožňuje exportovat vygenerovaný klíč do souboru KIMPEXP. Pomocí funkce maskování můžete umístit KIMPEXP dovnitř fotografie, která bude odeslána vašemu partnerovi, a provést tak přiměřeně bezpečnou výměnu klíčů.Účastník provede dekamufláž a naimportuje klíč z KIMPEXP extrahovaného z fotografie. Můžete vytvořit seznam, ve kterém uvidíte všechny klávesy (některé speciální znaky, které nelze zobrazit, jsou nahrazeny znakem ?).



Na straně příklad kláves.

DŮLEŽITÉ: Nikdy nezadávejte nový klíč, který má stejný název jako vaše přezdívka.

Pro správné rozložení:

- vytvořit zástupce Qcrypto na ploše

- klikněte pravým tlačítkem na ikonu zástupce

- vlastnosti / dispozice

- v rozměrech okna nastaveno 30 na výšku a 102 na šířku