Jegyzőkönyv

Biztonság és védelem az informatikában c. tárgy

11. feladat

Készítette:

Csomor Bence, TVIK4I

2021.04.30.

**A DES, a DESX, a 3DES, és a Triple DES**

DES:

A DES a Data Encryption Standatd rövidítése, magyarul Adat Titkosítási szabvány. 56 bites kulcs bemenetű szimmetrikus kulcsú, azaz 1 kulccsal rendelkezik, ami privát és csak a titkosítást és visszafejtést végző felek képesek az adott kulccsal titkos üzeneteket egymással közölni egy csatornán. A csatorna egy absztrakciója egy információhordozónak, ami egy vagy több fél között megosztott. Manapság az interneten már nem használják a DES-t mert az 56 bit méretű kulcs kicsi, ezért brute-force módszerekkel hamar törhető. Ezért használják a triple-des algoritmust. Ez viszont nagyon elterjedt a mindennapokban. Az algoritmus érzékeny néhány analitikus támadásra, de azok gyakorlatilag kivitelezhetetlenek. A DES alkotói megelőzték a korukat, hiszen nagyon sokáig nem találtak a kriptográfia terén kutató tudósok semmi sebezhetőséget rajta.

A DES az archetipikus blokk-rejtjel - egy algoritmus, amely rögzített hosszúságú sima szöveges bitből álló sztringet vesz fel, és bonyolult műveletek sorozatán keresztül átalakít egy másik, ugyanolyan hosszú titkosított szöveges bitstringbe. A DES esetében a blokk mérete 64 bit. A DES kulcsot is használ az átalakítás testreszabásához, így a visszafejtést állítólag csak azok hajthatják végre, akik ismerik a titkosításhoz használt kulcsot. *A kulcs állítólag 64 bitből áll; ezek közül azonban csak 56-ot használ az algoritmus. Nyolc bitet kizárólag a paritás ellenőrzésére használnak, majd eldobnak. Ezért az effektív kulcshossz 56 bit.*

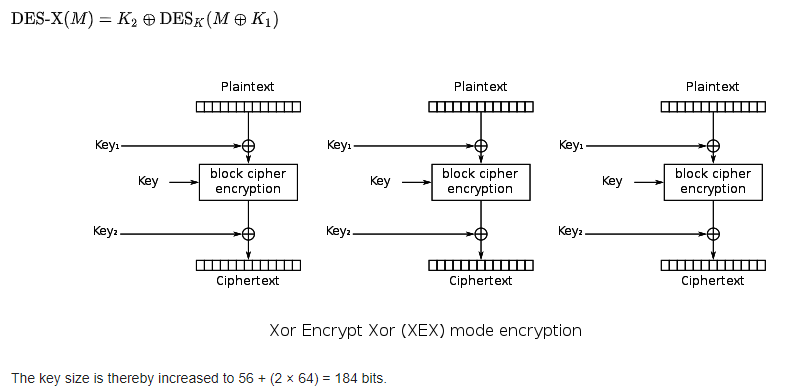
A DES eredete 1972-re nyúlik vissza, amikor az Egyesült Államok kormányának számítógépes biztonságával foglalkozó Nemzeti Iroda a Szabványügyi Hivatal tanulmányában megállapította, hogy kormányzati szintű szabványra van szükség a nem minősített, érzékeny információk titkosításához.

Körülbelül ugyanebben az időben Mohamed Atalla mérnök 1972-ben megalapította az Atalla Corporation-t, és kifejlesztette az első hardver biztonsági modult (HSM), az úgynevezett "Atalla Box" -ot, amelyet 1973-ban hoztak forgalomba. Az offline eszközöket biztonságos PIN-generáló kulccsal védte, és kereskedelmi siker volt. A bankok és a hitelkártya-társaságok attól tartottak, hogy az Atalla uralja a piacot, ami egy nemzetközi titkosítási szabvány kifejlesztését ösztönözte. Az Atalla korai versenytársa volt az IBM-nek a banki piacon, és a DES szabványon dolgozó IBM-alkalmazottak befolyásolják. Az IBM 3624 később a korábbi Atalla rendszerhez hasonló PIN-ellenőrző rendszert fogadott el.

1973. május 15-én, az NSA-val folytatott konzultációt követően, az NBS javaslatot kért egy olyan rejtjelre, amely megfelel a szigorú tervezési kritériumoknak. Egyik beadvány sem volt megfelelő. A második kérelmet 1974. augusztus 27-én tették közzé. Ezúttal az IBM benyújtott egy elfogadhatónak ítélt jelöltet - az 1973–1974 közötti időszakban kifejlesztett rejtjelet egy korábbi algoritmus, Horst Feistel Lucifer rejtjelén alapulva.

DESX vs 3DES:

A DESX a DES titkosítási algoritmus erősebb változata. A DESX-ben a bemeneti sima szöveget bitenként XOR-nal 64 bit további kulcsanyaggal XOR-zik, mielőtt DES-sel titkosítanák, és a kimenetet szintén bitenként XOR-ra tennék további 64 bit kulcsanyaggal.



A 3DES algoritmus ugyanis háromszor használja az Data Encryption Standard (DES) titkosítást az adatok titkosításához.

A DES szimmetrikus kulcsú algoritmus, amely Feistel hálózaton alapul. Szimmetrikus kulcs-rejtjelként ugyanazt a kulcsot használja mind a titkosítási, mind a visszafejtési folyamathoz. A Feistel hálózat mindkét eljárást szinte teljesen azonossá teszi, ami hatékonyabb algoritmust eredményez.

A DES-nek 64 bites blokkja és kulcsmérete is van, de a gyakorlatban a kulcs csak 56 bites biztonságot biztosít. A 3DES-t biztonságosabb alternatívaként fejlesztették ki a DES kis kulcshossza miatt. A 3DES-ben a DES algoritmust háromszor hajtják végre két kulccsal.

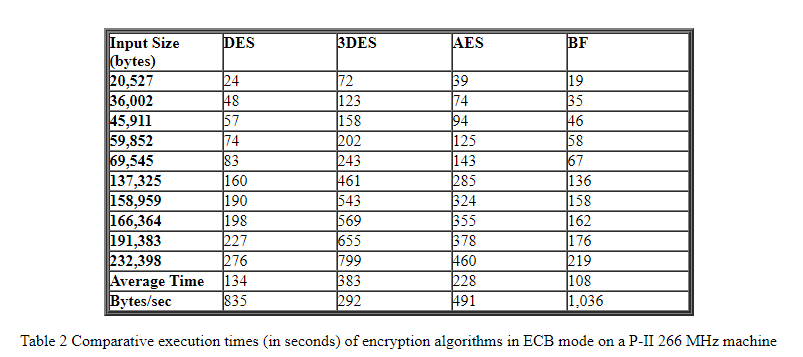
Triple DES vs 3DES:

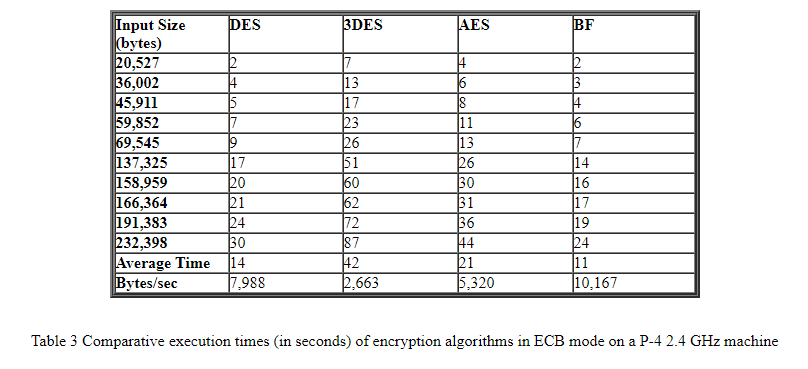
A Triple DES-t a DES-től fejlesztették ki, 64 bites kulcsot használ, amely 56 effektív kulcsbitből és 8 paritásbitből áll. A Triple DES esetén a DES titkosítást háromszor alkalmazzák a sima szövegre. A sima szöveget az A kulccsal titkosítják, a B kulccsal visszafejtik, és ismét a C kulccsal titkosítják.

Itt a különbség az, hogy a 3DES ugyanazt az egy kulcsot használja a kódolásra és a másikat dekódolásra. A Triple DES pedig három különböző kulcsot használ és egyiket sem használja fel többször.

Stream titkosítás:

A DES, felhasználhatók kulcstag előállítására kimeneti visszajelzés (OFB) módban. Ha azonban nem használunk teljes visszajelzést, akkor a kapott adatfolyam átlagosan körülbelül 232 blokk periódusú; sok alkalmazás esetében az időszak túl alacsony. Például, ha a titkosítást 8 megabájt / másodperc sebességgel hajtják végre, akkor a 232 blokk szakasz kb. Fél óra múlva megismétlődik.

Hatékonyságuk táblázatban: 



Titkosítások:

Titkosítandó szöveg: *„amit hárman tudnak, már nem titok”*

Ceacar-féle titkosítás:

Az eltolás legyen 7.

A kódolt üzenet: „dzspnw meüpdzsq wygyqdzsó, peü qíp wnwsó”

Kulcsszó használata (Vigenère-rejtjel):

Itt legyen a kulcsszó „aldi”.

amit hárman tudnak, már nem titok

aldi aldial dialdi, ald ial diald

AÁBCD.EÉFGH.IÍJKL.MNOÓÖ.ŐPQRS.TUÚÜŰ.VWXYZ

AÁBCD.EÉFGH.IÍJKL.MNOÓÖ.ŐPQRS.TUÚÜŰ.VWXYZ

LMNOÓ.ÖŐPQR.STUÚÜ.ŰVWXY.ZAÁBC.DEÉFG.HIÍJK

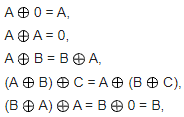
DEÉFG.HIÍJK.LMNOÓ.ÖŐPQR.STUÚÜ.ŰVWXY.ZAÁBC

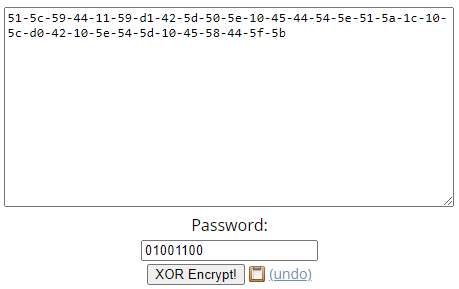
IÍJKL.MNOÓÖ.ŐPQRS.TUÚÜŰ.VWXYZ.AÁBCD.EÉFGH

A kódolt üzenet: „aűla hmútav űádvdr, mmú ueű űőtwo”

XOR kódolás:

Működési elvek:

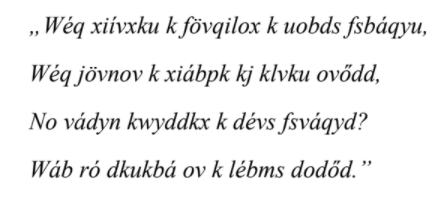




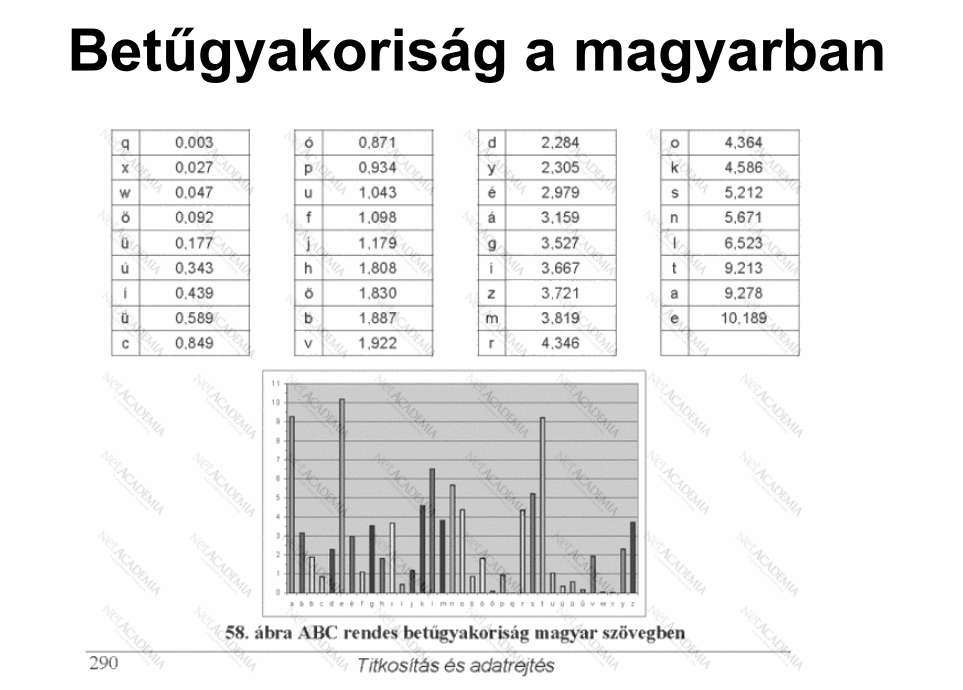
A kódolt üzenet: „51-5c-59-44-11-59-d1-42-5d-50-5e-10-45-44-54-5e-51-5a-1c-10-5c-d0-42-10-5e-54-5d-10-45-58-44-5f-5b”

Betűgyakoriság:

Megfejtendő szöveg:



Magyar betűgyakoriság:



Először megszámolom a nem ékezetes betűk gyakoriságát.

m-1 i-3 q-5

r-1 y-4 b-6

p-1 w-4 o-7

j-2 x-4 v-9

n-3 s-5 d-12

l-3 u-5 k-13

f-3

Mivel sok a különálló „k” ezért valószínűleg az az „a” betű. Akkor a „d” -nek kell lennie az „e” -nek, de mivel két „e” nem sűrű a magyarban ezért a következő leggyakoribb betű, a „t” lesz. És így tovább…

Az első sorban már rá lehet jönni, hogy ez melyik vers, és minden sor után egyre gyorsabb a folyamat, ahogy meglesznek a betűk.

Az eredmény:

k-a s-i l-b

d-t x-n n-d

v-l w-m j-z

o-e y-o p-f

b-r i-y r-h

q-g f-v m-c

u-k

Az eredeti szöveg:

„Még nyílnak a völgyben a kerti virágok,

Még zöldel a nyárfa az ablak előtt,

De látod amottan a téli világot?

Már hó takará el a bérci tetőt.”

források:

<https://hu.wikipedia.org/wiki/DES>

<https://www.browserling.com/tools/xor-encrypt>

<https://en.wikipedia.org/wiki/Data_Encryption_Standard>

<https://www.omnisecu.com/security/public-key-infrastructure/symmetric-encryption-algorithms.php>

<https://en.wikipedia.org/wiki/DES-X>

<https://www.comparitech.com/blog/information-security/3des-encryption/>

<https://en.wikipedia.org/wiki/Stream_cipher>

<https://www.cs.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.html>

<http://www.inf.u-szeged.hu/~zlnemeth/crypto/OLD-SLIDES/crypt2.pdf>