CTI Jelentés

# A kriptográfia napjainkban


1996
Fortes fortuna adiuvat
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI
KIBERVÉDELMI INTÉZET

# Tartalomjegyzék

# Mi az a kriptográfia?

Manapság, amikor a kiberbűnözők különböző csoportokba szerveződve próbálják meg különféle és egyre fejlettebb eszközökkel megszerezni az érzékeny és személyes információinkat így növelve profitjukat, a titkosítás jelentősége egyre kritikusabbá válik.

A **kriptográfia** egy olyan **tudományág**, amelyben egy adott információt olyan módon rejtjelezünk, hogy az csak annak válik elérhetővé, aki jogosult azt megkapni és feldolgozni. Az informatikában a kriptográfia nagyrészt a matematikai szabályok és algoritmusok felhasználásával az információk biztonságos tárolására, illetve valamilyen kommunikációs technológián keresztül való biztonságos továbbítására utal.

A titkosítási vagy rejtjelezési eljárások egy fontos összetevője a kulcs, amelynek a birtokában a tikosított információ megismerhető. Jelenlegi digitális világunkban ezeket az algoritmusokat titkosítási kulcsok létrehozására, digitális aláírásokhoz, internetes böngészésre és biztonságos kommunikációhoz is használják.





# Titkosítási módszerek

A mai világban a **szimmetrikus és aszimmetrikus titkosítás** mindennapos része az online biztonságnak és adatvédelemnek.

**Szimmetrikus titkosítás**

Gyors és hatékony megoldást kínál az adatok védelmére.

**Aszimmetrikus titkosítás**

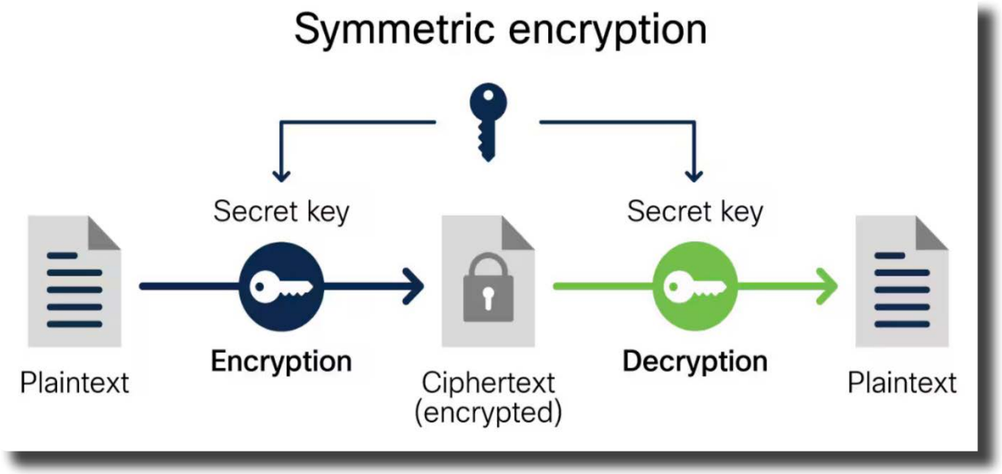
Magasabb szintű biztonságot nyújt, mint a szimmetrikus titkosítás.

Ezek a technológiák alkotják az alapját a banki tranzakcióknak, az online kommunikációnak és az adatok tárolásának, így biztosítva az adatok védelmét és a felhasználók bizalmát a digitális térben.

## Szimmetrikus kulcsú rejtjelezés

A **szimmetrikus kulcsú rejtjelezés** egy olyan **titkosítási módszer**, amely csak **egyetlen kulcsot használ** az adatok titkosítására és visszafejtésére. A felhasználók először egy titkos kulcsot generálnak, majd ezzel a kulccsal titkosítják az adott üzenetet. A visszafejtés során a fogadó fél ugyanezt a kulcsot használja.

A szimmetrikus kulcsú titkosítás technológiája egyszerű és könnyen használható. Ebben a típusú rejtjelezésben **a biztonság a legkritikusabb kérdés**, hiszen **a titkosítási kulcsot nagy biztonságban szükséges őrizni** a felek között.

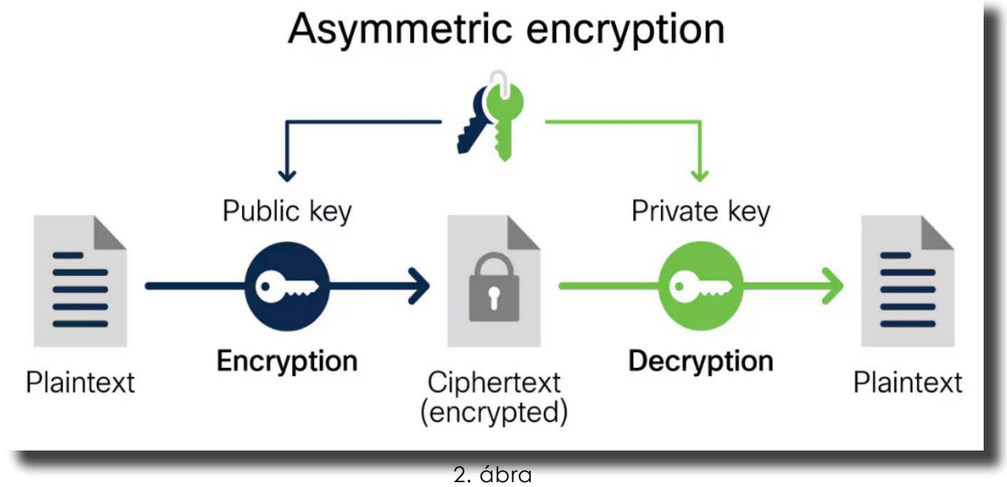



1. ábra
**A szimmetrikus titkosítás illusztrációja**
*Forrás: cisco.com*

## Aszimmetrikus kulcsú rejtjelezés

Az **aszimmetrikus kulcsú rejtjelezés** egy olyan kriptográfiai eljárás, amely során különböző, de matematikailag összefüggő kulcsot használnak fel a titkosításhoz és a visszafejtéshez. Ezeket a kulcsokat általában **"publikus" és "privát" kulcsnak nevezik**.

A legismertebb aszimmetrikus kulcsú titkosítási módszer a későbbiekben részletezett **RSA algoritmus**. Először a két fél generál egy **publikus-privát kulcspárt**. A **publikus kulcs** mindenki számára elérhetővé teszi a titkosított üzeneteket, míg a **privát kulcs** csak a tulajdonos számára hozzáférhető. Ha a feladó titkosít egy üzenetet a publikus kulcs segítségével, akkor a címzett csak a hozzá tartozó privát kulcs segítségével tudja visszafejteni azt.




2. ábra
**Az aszimmetrikus titkosítás illusztrációja**
*Forrás: cisco.com*

## Egyirányú titkosítás (Hash)

Az **egyirányú titkosítás**, vagy más néven **hashelés**, egy olyan eljárás, amely egy tetszőleges hosszúságú bemeneti adatot alakít át egy fix hosszúságú, ún. hash értékké. A hash függvények széles körben használatosak a kriptográfiában, például jelszavak tárolására, digitális aláírások készítésére, valamint adatintegritás ellenőrzésére.

Egy **weboldalnak nem kell tárolnia a felhasználók tényleges jelszavait,** hanem csak a jelszavak hash értékeit. Ezáltal ha valaki hozzáférést szerez a tárolt adatokhoz, még mindig nem tudja az eredeti jelszavakat, csak a hash értékeket.

Amikor egy felhasználó bejelentkezik, **a rendszer egyszerűen hasheli a megadott jelszót, és összehasonlítja a tárolt hash értékkel.**

**TUDTAD?**

A hash függvények meghatározó tulajdonságai:

- **Determinisztikus**: Ugyanaz a bemenet mindig ugyanazt a hash értéket adja eredményül.
- **Egyszerű számítás**: A hashelés nagyon gyorsan elvégezhető.
- **Nem lehetséges a visszafelé számítás**: Mivel a hash függvények egyirányúak, ezért nem lehet visszafejteni.
- **Kis módosulások nagy változást okoznak**: Egyetlen karakternyi változás a bemeneten teljesen más hash értéket eredményez.





# A jelenleg leggyakrabban használt algoritmusok

Ebben a fejezetben bemutatunk néhány, a jelenleg leggyakrabban használt titkosítási algoritmust a teljesség igénye nélkül.

## 1 Triple Data Encryption Standard

A **Triple DES** (Triple Data Encryption Standard) egy **blokktitkosítási algoritmus**, amely háromszoros ismétléssel alkalmazza az alap, DES (Data Encryption Standard) algoritmus eljárásait, lépéseit. A DES blokktitkosítás 64-bites blokkokat kezel, illetve 56-bites kulcsot használ.

A Triple DES három fő eljárással rendelkezik, melyek a következők:

- **EDE** (Encrypt-Decrypt-Encrypt)
  Ebben a módban a szöveget először **titkosítják**, majd a titkosított szöveget **visszafejtik, majd újra titkosítják**. Ez az eljárás a leggyakoribb a Triple DES alkalmazásánál.

- **EEE** (Encrypt-Encrypt-Encrypt)
  **Mindhárom lépésben a szöveget titkosítják**. Ez az eljárás növeli a biztonságot, de nincs visszafelé kompatibilitás a DES-el.

- **DED** (Decrypt-Encrypt-Decrypt)
  Az először **visszafejtett szöveget titkosítják, majd a titkosított szöveget újra visszafejtik**. Ezt a módszert ritkábban alkalmazzák.

A Triple DES működését a következő lépésekben lehetséges bemutatni, részletezni:

- A 64-bites bemeneti blokk szétbontásra kerül két 32-bites blokkra.
- A bemeneti blokkot 16 „rétegben” titkosítják a megadott kulcsok segítségével.
  - Ha az **EDE** eljárásra van szükség, akkor a titkosított eredmény visszafejtésre kerül az első kulcs segítségével.
  - Amennyiben az **EEE** eljárást szeretnénk használni, akkor a titkosított eredmény ismét titkosításra kerül a két kulcs felhasználásával.
- Az utolsó lépésben, ha szükséges, a szöveg újra titkosításra kerül a harmadik kulccsal.

Fontos kiemelni, hogy a **Triple DES sebezhetőségei és alacsony hatékonysága miatt a 2023-as évtől már nem alkalmazandó.**

Helyette a következőkben részletezett, fejlettebb **AES** algoritmust használják.

## 2 Advanced Encryption Standard (AES)

Az **Advanced Encryption Standard** (AES) az egyik **legelterjedtebb és legbiztonságosabb szimmetrikus blokktitkosítási algoritmus**. Az AES-t az Amerikai Nemzeti Biztonsági Ügynökség (NSA) által kiírt versenyen választották ki 2001-ben.

Az AES egy blokktitkosítási algoritmus, amelynek során a **bemeneti adatot blokkokra osztja, így külön-külön titkosítva minden blokkot**. A kulcsa lehet 128, 192 vagy 256 bit hosszú. Minél hosszabb a kulcs, annál erősebb a titkosítás. A bemeneti blokkot többszörösített permutációs hálózatok sorozatán keresztül dolgozza fel. Ez magában foglalja a bit-alapú műveleteket, például az XOR-t, a bitcseréket és a ciklikus eltolást.

Az algoritmus több lépésben dolgozza fel a bemeneti blokkot, amelyek száma a kulcs hosszától függ. Az algoritmust az elektronikus kommunikációban, adatbázisok titkosításában, fájlok titkosításában és sok más területen is használják. **Használata nagy mértékű biztonságot nyújt, illetve hatékonyan kezeli a nagy mennyiségű adatot is.**

Az AES működése a következő lépéseket tartalmazza:

- A kulcsot kiterjesztik olyan alkulcsokká, amelyek a különböző körökben felhasználásra kerülnek.
- A bemeneti blokkot egy kezdő állapotra alkalmazzák.
- Az algoritmus a különböző körökben alkalmazza a kiterjesztett kulcsokat és a permutációs hálózatokat.
- Az utolsó kör után az eredmény blokk kerül generálásra, amely a titkosított üzenet lesz.

## 3 Rivest-Shamir-Adleman (RSA)

Az **RSA** (Rivest-Shamir-Adleman) egy **kriptográfiai algoritmus**, amelyet abból a célból terveztek, hogy egy biztonságos és visszafejthetetlen titkosítási megoldást adjon a felhasználók számára. Az algoritmus nevét a feltalálói, Ron Rivest, Adi Shamir és Leonard Adleman után kapta. Az RSA algoritmus elméleti alapjai a **moduláris számelmélet**, illetve a **prímszámelmélet** területeiből tevődnek össze. A titkosított üzenetet csak a privát kulccsal van lehetőség visszafejteni, ezáltal a prímfaktoroknak köszönhetően az esetleges támadóknak már igen nehéz dolga akadna.

Az RSA egyike a **legelterjedtebb és legbiztonságosabb** kriptográfiai eljárásoknak, amelyek széles körben használatosak digitális aláírások, SSL/TLS kommunikáció, illetve egyéb titkosítási műveletek során. Fontos megjegyezni, hogy az algoritmus megfelelő használata és konfigurálása kulcsfontosságú a biztonság szempontjából.





## 4 Elliptic Curve Cryptography (ECC)

Az **ECC** (Elliptic Curve Cryptography) egy olyan **kriptográfiai eljárás**, amely **elliptikus görbék** alapján működik. Az ECC egyre elterjedtebb olyan alkalmazásokban, ahol a korlátozott erőforrások és a kis méretű kulcsok szerepe kritikus. Az ECC lényegesen kisebb kulcsokat használ, mint a hagyományos RSA, ugyanakkor hasonló mértékű biztonságot nyújt. Az eljárás alapja a nehéz elliptikus görbéken végzett műveletek. Felhasználása széleskörű, találkozhatunk az SSL/TLS protokollok használatánál, digitális aláírásokban, IoT eszközökön, illetve mobilalkalmazásokban is.

## 5 Secure Hash Algorithm (SHA)

Az **SHA** (Secure Hash Algorithm) a **kriptográfiai hash függvények egy típusa**, amelyek olyan matematikai tételeket alkalmaznak, amelyek bemenetüket véletlenszerű méretű adatból állandó méretű, általában rövid kimenetre alakítják.

A leggyakrabban használt SHA algoritmusok a következők:

### SHA-1

Az SHA-1-es verzió 1995-ben jelent meg, a fejlesztők céljai a digitális aláírások és az SSL/TLS tanúsítványok előállítása volt. Az algoritmus ma már elavultnak számít, ezért **2017-ben a szakértők hivatalosan is nem biztonságossá nyilvánították.**

### SHA-256, SHA-384, SHA-512

Ezek a verziók már az SHA-2 család tagjai, amelyek **biztonságosabbnak számítanak, mint az elődjük**. Jelenleg széles körben használják a digitális aláírások, SSL/TLS tanúsítványok, valamint az adatok integritásának ellenőrzése terén is.

### SHA-3

Ez már egy újabb generációja az SHA algoritmusoknak, amelyet a NIST (National Institute of Standards and Technology) állított össze 2015-ben. A SHA-3 már különböző hash függvényeket kínál a szerteágazó alkalmazási igények kielégítésére.

Az SHA típusú algoritmusok működése egy bemeneti üzenet *(pl. szöveg vagy adatfájl)* átalakításával egy rövidebb, állandó méretű hash érték létrehozásán alapszik.

A hash függvényeknek számos fontos tulajdonsága van, ideértve az **egyirányú működést**, a **determinisztikusságot** és a **kis változásoknak a hash értékére gyakorolt jelentős hatását.** Ezek a tulajdonságok teszik az SHA függvényeket alkalmassá olyan feladatokra, mint a digitális aláírások, az adatok integritásának ellenőrzése, illetve az adatok egyedi azonosítása.



Az alábbi példa bemutatja, hogy akár egyetlen egy karakter megváltoztatása mennyiben befolyásolja a végén kapott hash értékét.

Ha a következő karaktereket: **„almafa1”** az SHA256 segítségével titkosítjuk a következőt kapjuk eredményül:
**„cf8e75b95a136f9ad273b3386f92e8f502571518e815da30ed1ce676b3f45782”**

Most változtassunk a bemenő adaton, az 1-es karaktert írjuk át 2-esre, tehát a következőt titkosítjuk ezúttal: **„almafa2”**. Így az alábbi hash generálódik:
**„f34d217e7307d45d8adbc6c23d4e8cc2ad1401ff9bb528a7b76a8c0a24b27aa4”**

A fenti példából láthatjuk, hogy **akár egy karakter megváltoztatása** is már **nagy hatást fejt ki a titkosított karaktersorozatban.**

## 6 Blowfish

A Blowfish egy **blokktitkosító algoritmus**, amelyet Bruce Schneier fejlesztett ki 1993-ban.

Ez az eljárás **hatékony, könnyű implementálni,** illetve **nagy teljesítményt nyújt** számos különböző alkalmazásban. A Blowfish egy szimmetrikus kulcsú titkosítási módszer. Meghatározott méretű blokkokba felosztva dolgozza fel az adatokat. Az alapértelmezett blokkméret 64 bit. Maga az algoritmus két fő részből áll, az előzetes kulcsgenerálásból és a titkosítási/visszafejtési folyamatból.

A Blowfish használata során a titkosítás, illetve a visszafejtés a következő lépésekből áll:

- A titkosításhoz és a visszafejtéshez **generálásra kerül egy kulcs**, amelynek hossza változhat, de általában 32 és 448 bit között van.
- A generált kulcs alapján az algoritmus **előállítja a Blowfish belső kulcstábláit**.
- Az adatok blokkokra való felosztása után, minden blokkot egy **előre meghatározott rendszer szerint titkosítanak**.
- A titkosított blokkok visszafejtése ugyanazt a folyamatot követi, de a titkosítási folyamat során **előállított érték megfelelő sorrendben kerülnek alkalmazásra.**

A Blowfish algoritmust számos területen alkalmazzák, beleértve a számítógépes játékokat, a biztonságos kommunikációt, illetve az adatbázisok titkosítását is.

Bár az algoritmus **hatékony és megbízható**, a 64 bites blokkméret miatt problémák merülhetnek fel a nagy adatblokkok titkosítása során. Ebből kifolyólag néhány modern alkalmazás fejlesztői inkább az AES vagy más alternatív blokktitkosító algoritmust részesítenek előnyben.





# Milyen területeken használnak titkosítást?

A kiberbűnözők technikáinak fejlődésével és egyre szofisztikáltabbá válásával, valamint annak a ténynek köszönhetően, hogy az átlag internetfelhasználó személyes adatai egyre több helyre és egyre nagyobb számban kerülnek fel, kiemelt kulcsszerepet kap a digitális titkosítás.

Ebben a fejezetben röviden bemutatunk olyan területeket, melyekben a titkosítás használata kritikus fontosságú. **Fontos kiemelni, hogy a titkosítás önmagában nem garantálja a sérthetetlenséget és a hitelességet.** A sérthetetlenség azt jelenti, hogy az adatokat nem lehet módosítani vagy manipulálni észrevétlenül. A hitelesség pedig biztosítja, hogy az információ valóban attól a forrástól származik, akitől eredetileg érkezett, illetve, hogy nem történt közben módosítás, hamisítás.

## Virtuális magánhálózatok

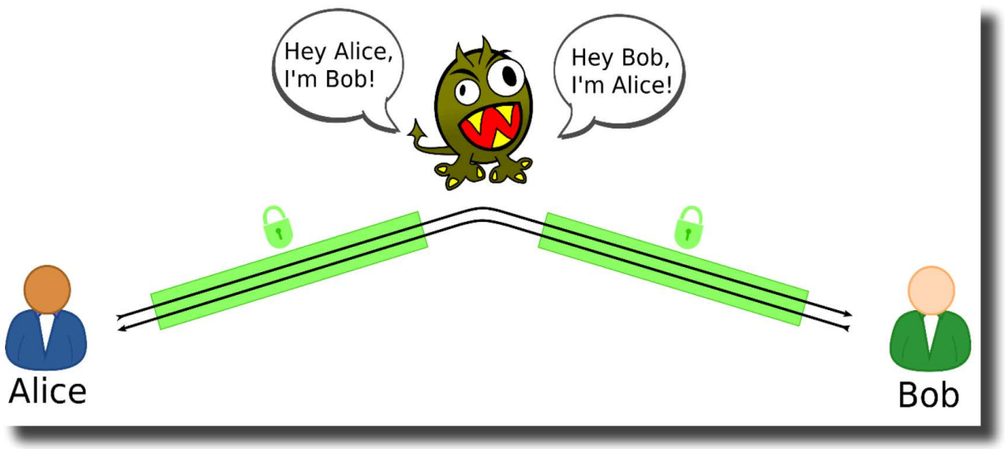

A **virtuális magánhálózatok** (Virtual Private Network - VPN) **célja, hogy a felhasználók hálózati kommunikációja**, illetve **adatai egy biztonságos, privát hálózaton keresztül haladjon**.

Egy titkosítási kulcs gondoskodik arról, hogy a kommunikáció illetéktelen szemek előtt rejtve maradjon. A kulcsot csak a felhasználó eszköze és a VPN szerver ismeri, ezáltal a kommunikációt csak ezeken a végpontokon lehet feloldani.

## SSL/TLS biztonsági protokollok

A **Transport Layer Security** (TLS), illetve a **Secure Sockets Layer** (SSL) olyan, az **internetes kommunikációban használt alapvető biztonsági protokollok**, melyek az adott üzenet integritását biztosítják.

Az említett titkosítási algoritmusok felhasználásával nehezebbé és elkerülhetőbbé tehető egy esetleges **közbeékelődéses (MITM) támadás.**




3. ábra
**Az MITM támadás illusztrációja**
*Forrás: sec.cs.univie.ac.at*





## Jelszavak titkosítása


Egy bejelentkezési folyamat során a kliensünk elküldi a hálózaton keresztül az adott szervezethez a jelszavunkat, ezáltal ellenőrzi, hogy az valóban helyes-e. **Akármilyen erős jelszót is választunk, ha egyszerű szövegként (plain text) kerül tárolásra a szerver oldalon, semmivel sem fog nagyobb védelmet nyújtani egy egyszerű számsornál, ha a támadók kompromittálják a rendszert.** Emellett fontos megjegyezni, hogy léteznek már olyan adatbázisok, ahol kulcs-érték páronként tárolják az adott jelszavakat és hasheket. Ez akkor veszélyes, ha egy támadás során megszerzik  a feltört rendszerből a hash értékeket, és ezalapján megpróbálják kinyerni az eredeti jelszót.

Hiába tűnik biztonságos jelszónak például a

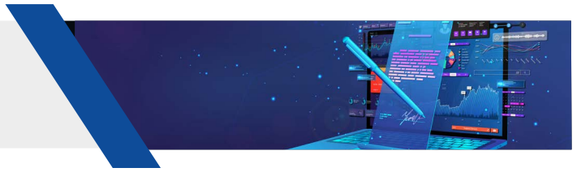
`7cdab41b409db1d38c13dfc9f5b6635dd7b6352a`.

**Egy jelszó adatbázisban gyorsan megtalálják az eredeti párját** („`almafa`"), amely SHA-1 algoritmussal került titkosításra.

**TUDTAD?**

A legbiztonságosabb módszer, ha kliens és szerver oldalon is megtörténnek a megfelelő lépések. Előbbinél egy kellő hosszúságú és erősségű jelszó választása az ideális, míg utóbbinál pedig a megfelelő titkosítás. A témához kapcsolódó, biztonságos jelszókezelésről készült kiadványunkat ide kattintva olvashatja el.

## Elektronikus, digitális aláírások



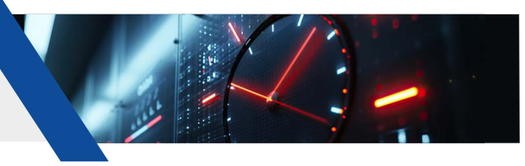
A **digitális aláírás** egy olyan **matematikai algoritmusokkal készített „lenyomat”**, amely lehetővé teszi az adott felhasználó számára, hogy bizonyítsa, ő valamilyen digitális termék jogos tulajdonosa. Ez a módszer lehetőséget ad a kommunikáló felek számára, hogy meggyőződjenek az üzenet integritásáról.

A digitális aláírások a **nyilvános kulcsú kriptográfián**, más néven **aszimmetrikus kriptográfián** (pl. RSA) alapszik. Létrehozásához szükséges egy privát és egy publikus kulcs is. A küldő fél titkosítja az üzenetet a privát kulcs segítségével, a publikus kulccsal pedig aláírja azt. A fogadó fél ezután dekódolja az üzenetet a publikus kulcsával és összehasonlítja a visszafejtett üzenetet az eredetivel, ha ezek megegyeznek, akkor az üzenetet nem módosították illetéktelenek. Olyan előnyökkel rendelkezik a módszer, mint a biztonság, időbélyegzés, szabvány miatti elfogadottság világszerte, idő- és költségmegtakarítás és nyomonkövethetőség.





## Időbélyegzés

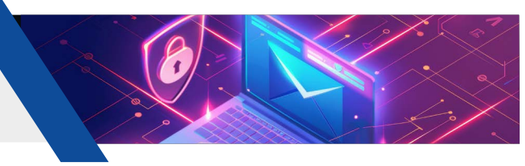


Az **időbélyegzés** során egy dokumentumhoz vagy adathoz egy adott időpontot rendelnek hozzá. Ez a folyamat arra szolgál, hogy bizonyítsák, az adott dokumentumot ténylegesen az időbélyeg szerinti időpontban hozták létre (általában másodperc pontossággal). Gyakran az elektronikus dokumentumok hamisítása ellen használják fel.

## Hitelesítés

A **hitelesítés** egy olyan folyamat melynek során megbizonyosodunk az adott felhasználó személyazonosságáról. Ilyen metódusok közé tartozik a szöveges és grafikus jelszavak, autentikációs tokenek, szimmetrikus és aszimmetrikus kulcsú azonosítás, valamint a biometrikus azonosítás.

## Biztonságos csevegés, E2EE



Egyes csevegőszolgáltatásokban megjelent a **végpontok közötti titkosítás** (End-to-end encryption - E2EE). A kriptográfiai algoritmusok segítségével privát környezetben maradhatnak az üzenetek, illetve a kommunikációban található érzékeny információk.

A **végponttól-végpontig titkosítás** egy olyan **kommunikációs módszer**, amely során **az adatokat csak a feladónak és a fogadónak van lehetősége feloldani és értelmezni**. Ezt a kriptográfiai lehetőséget használja sok online üzenetküldő alkalmazás is.

Megvédi az üzenetben található információkat az illetéktelenektől, létrehoz egy biztonságos kommunikációs csatornát, illetve hitelesíti a két kommunikációt folytató felet. Ez olyan szempontból hasznos és mára már elengedhetetlen, hogy amennyiben egy hacker lehallgatja a hálózatot (sniffing), hiába nyeri ki a nyers hálózati adatforgalmat, nem tud vele mit kezdeni a titkosítás miatt, mivel az az üzenet megérkezése után lesz dekódolva a fogadó oldalon.

## Internetbanki tranzakciók


Az **online térben történt pénzügyi tranzakciók** is a kriptográfia mögé rejtőzve mennek végbe. A titkosítás felel a küldő és fogadó fél személyazonosságának védelméért, illetve a tranzakció biztonságos végrehajtásáért.

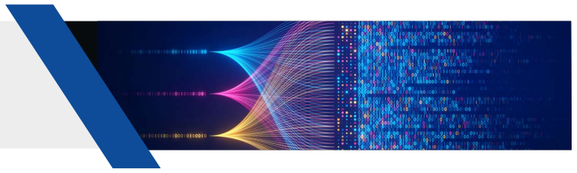
A pénzügyi csalások elkerüléséhez további információt ide kattintva a KiberPajzs oldalán találhat.

KiberPajzs
Védelem a pénzügyekben





## Adattárolás, adatátivel



A kriptográfia szintén fontos területe az **adatállományok védelme** mind tárolás, mind pedig a „mozgatás" közben. Az információk titkosítása az adott eszközön tárolt kulcs segítségével történik. A titkosítás ezen területe nem csak az információk elérhetőségét korlátozza, de segítségével hitelesíteni is lehet az éppen vizsgált adatot, így arról is meggyőződhetünk, hogy az információt nem módosították idegen kezek. Az adatátvitel során is szükséges gondoskodni a megfelelő védelemről, ezért az adatállomány titkosítása ebben az esetben egy olyan kulcs segítségével történik, amelyet csak a feladó és a címzett ismer, illetve képes feloldani.

Megjelentek a nulla tudás alapú felhőszolgáltatások, amelyek abban nyújtanak újdonságot a hagyományos típusúakhoz képest, hogy a szolgáltató nem lát bele a nála tárolt adatokba, ahhoz csak és kizárólagosan az adat tulajdonosának van jogosultsága.

A témában készült podcastünket ide kattintva hallgathatja meg.

KIBERTÁMADÁS! PODCAST

## E-mailek titkosítása

Szintén szükséges megemlíteni, hogy kriptográfiai módszereket használnak az elektronikus levelek küldésében, illetve fogadásában is. Az e-maileket egy algoritmus segítségével titkosítják, így megvédve azokat a rosszakaróktól. Levelek titkosítása esetén érdemes kiemelni a **PGP (Pretty Good Privacy)** titkosítást, melynek célja, hogy a levelek tartalmának integritását és hitelességét biztosítsa.

# Miért biztonságosak az algoritmusok?

A biztonságos titkosítási algoritmusoknak számos fontos tulajdonsága van, amelyek meghatározzák, hogy mennyire alkalmasak az éles helyzetben történő alkalmazásra:

- A titkosítási algoritmusoknak hosszú kulcsokat kell használniuk annak érdekében, hogy ellenálljanak a különböző kriptográfiai támadásoknak, például a brute force támadásnak. **Minél hosszabb a kulcs, annál nehezebb feltörni az algoritmust**, pontosan úgy, ahogy jelszavaink esetében is.

- Egy biztonságos algoritmusnak ellenállónak kell lennie az olyan kriptoanalitikai támadásokkal szemben, mint a **differenciális kriptoanalízis**, vagy a **lineáris kriptoanalízis**.

- Szintén fontos kiemelni a kvantum kriptoanalízisben alkalmazott algoritmusokkal szembeni védelmet, annak érdekében, hogy megőrizzék biztonságukat a jövőbeli kvantum-számítógépekkel szemben.

- A titkosítási algoritmusok nagyon alapos matematikai tervezettséget igényelnek, illetve a fejlesztőknek bizonyítaniuk szükséges a különböző támadások esetében az algoritmus által adott választ is.

  Fontos kiemelni, hogy a titkosítási algoritmusok biztonságossága mellett **kritikus fontosságúak a megfelelő kulcskezelési gyakorlatok**, illetve helyes alkalmazásuk.

# Létezik-e teljesen biztonságos titkosítási algoritmus?

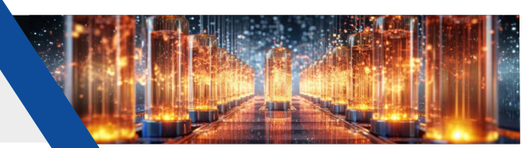
**Egy titkosítási algoritmus sosem lehet teljes mértékben biztonságos vagy feltörhetetlen.** Több szempontból szükséges vizsgálni egy algoritmust, ha a sebezhetőségekről beszélünk. A modern titkosítási eljárások biztonsága matematikai tételeken, sajátosságokon nyugszik.

Ezen problémák jelenlegi megfejtésére **nem ismerünk érdemi idő alatt végrehajtott megoldásokat**, még a fejlődő technológia és a számítási kapacitás nagymértékű növekedése ellenére sem. Ezért teljes biztonsággal **nem jelenthetjük ki, hogy matematikailag lehetetlen megoldást találni rájuk**.

A **kvantumszámítógépek** megjelenésével például olyan algoritmusokat hozhatnak létre, amelyek **hatékonyan oldanak meg olyan matematikai problémákat, amelyek jelenleg nehézséget okoznak a hagyományos számítógépeknek**. Érdemes megemlíteni a titkosítási algoritmusok során előforduló implementációs hibákat is, melyek akár különböző támadások során is felhasználhatóak *(pl.: titkosított adatok vagy kulcsok helytelen kezelése)*.

# Jövőkép

## Kvantumkriptográfia



A **kvantumkriptográfia** egy olyan terület a kriptográfiában, amely a **kvantummechanika alapelveit használja fel** a még biztonságosabb kommunikáció és adatvédelem elérésének érdekében.

A kvantummechanika bizonyos jelenségeit kihasználva lehetőség nyílik olyan protokollok kifejlesztésére, amelyek biztosítják az információk megőrzését és integritását a klasszikus számítógépek által nem megoldható kriptográfiai problémákra is. A kvantumtitkosítás egyik alapvető megoldása a **kvantumkulcs-elosztás** (QKD). A **BB84 az egyik legismertebb QKD protokoll**, amely kvantumállapotokat használ a kulcs generálására és az esetleges hibák észlelésére, illetve elméletileg (jelenlegi ismereteink szerint) feltörhetetlen.





A kvantumkriptográfia másik fontos területe a **kvantumtitkosítás**. A **kvantumtitkosítás olyan kvantummechanikai jelenségeket használ fel** az adatok biztonságos titkosításához és dekódolásához, melyek a kvantumkommunikációs csatornán átvitt információkat titkosított kvantumállapotokkal védik, amelyek csak a megfelelő kulcs ismeretében lesznek értelmezhetőek. A kvantumkriptográfia egy rohamosan fejlődő kutatási terület, és bár ígéretes lehetőségeket kínál a biztonságos kommunikáció terén, **még mindig számos kihívás áll előtte** *(pl.: környezeti zaj kezelése)*. Ez az előrehaladás egyre több figyelmet vonz, és a jövőben új lehetőségeket nyithat meg a kiberbiztonság és az adatvédelem területén.

Érdemes kiemelni, hogy az Apple iMessage szolgáltatása, illetve a Signal is már a fenti technológiát használja a kommunikáció biztosítására. A hang és videó továbbítása kvantumkriptográfia felhasználásával eddig nem volt megoldott, azonban erre a problémára talált megoldást egy magyar vállalat. A cég fejlesztése jövőbemutató eredmény a vállalati környezetben folytatott konferenciahívások integritásának megőrzésében.

## Homomorf titkosítás

A **homomorf titkosítás** egy olyan jövőbemutató kriptográfiai technika, amely lehetővé teszi különböző matematikai műveletek végrehajtását titkosított adatokon anélkül, hogy azokat előbb vissza kellene fejteni.

A homomorf titkosítás még javában fejlesztés alatt áll, és egyes implementációk még nem feltétlenül praktikusak nagy mennyiségű adat kezelésekor, ennek ellenére már számos területen (egészségügy, pénzügy, felhőalapú szolgáltatások) használják előszeretettel a biztonsági szakemberek. A technológia az idő előrehaladtával egyre ígéretesebb megoldást kínál az adatvédelem és a biztonságtechnika területén.

## Mi fog történni a jelenleg használt titkosítási módszerekkel?

A jelenleg használt, illetve ismert titkosítási algoritmusok egyelőre megfelelő védelmet nyújtanak az adataink és információink számára. Amennyiben a jövőbeli számítási kapacitás már megköveteli, az átmenet más kriptográfiai megoldásokra hosszú és összetett folyamat lesz.

A biztonságos átállás előfeltétele a jelenlegi titkosítási rendszerek, illetve protokollok alapos vizsgálata, valamint az új technológiák széles körű elfogadása és alkalmazása. Érdemes kiemelni, hogy a titkosítási algoritmusok folyamatos fejlesztés alatt állnak, annak érdekében, hogy a legújabb támadások ellen is hatékony védelmi vonalat próbáljanak ellátni.





A kvantumszámítógépek jövőbeli elterjedésével **hibrid megközelítést** szükséges majd alkalmaznunk, melynek során a **hagyományos és a poszt-kvantum kriptográfia kombinálásával** érik majd el a kutatók az adatok védelmét. Valószínűsíthető, hogy ezek után már szükség lesz a specifikusan kvantumszámítógépek fenyegetései ellen kifejlesztett algoritmusokra is.

Fontos kiemelni, hogy **az átalakulás során a biztonság és a stabilitás kulcsfontosságú szereppel fog bírni**. A jelenlegi titkosítási módszerek továbbra is hatékony védelmet nyújtanak, és az átmenet során nagy odafigyeléssel szükséges eljárni annak érdekében, hogy az adatok biztonsága ne sérüljön.

NEMZETI
KIBERVÉDELMI INTÉZET


nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast


2024