Mesterséges intelligencia

A gondolkodó gép megalkotása régóta foglalkoztatja az emberiséget. Az első ilyen informatikai eszközöket az 1950-es években alkották, és akkor kapta a terület a **mesterséges intelligencia** (MI vagy az angol Artificial Intelligence kifejezésből az AI) elnevezést. Gyors fejlődésnek azonban csak az elmúlt évtizedben indult. A mesterséges intelligencia fejlődése összekapcsolódik az információs társadalom újonnan kialakuló lehetőségeivel, és kétségkívül maga is jelentősen hozzájárul az információs társadalom jövőjének alakulásához.

Mesterséges intelligencia alatt olyan gépet, rendszert értünk, amely képes az emberi viselkedés, gondolkodás utánzására, problémamegoldásra. Fontos tudnunk, hogy a mesterséges intelligencia egy-egy részterületen képes az emberi intelligencia leképezésére, akár jobban is teljesíthet bizonyos jól meghatározott feladatokat.

Egyelőre azonban igen messze áll attól, hogy az emberi gondolkodást teljes komplexitásában helyettesíteni tudja vagy felülmúlja.

A terület mai rohamos fejlődéséhez több tényező járul hozzá. Egyik fontos tényező a számítási kapacitás növekedése, ugyanis a mesterséges intelligencia által használt algoritmusok általában műveletigényesek. Sok olyan chipet gyártanak, amely támogatja a mesterséges intelligenciát. A mobiltelefonjaink egy részében ilyen processzort találhatunk. A mesterséges intelligencia egyik fontos működési elve azon alapszik, hogy a rendszer nagy mennyiségű adat megvizsgálásával tapasztalatokat szerez, ezeket elemezve, feldolgozva, a szabályszerűségeket megfigyelve alakítja ki a helyzetekre adandó megfelelő válaszokat. Ezt a folyamatot nevezzük **gépi tanulásnak.**

Az információs társadalomban óriási mennyiségű adatot állítunk elő. A web 2.0 alkalmazások használatakor a felhasználók saját maguk által készített tartalmakat osztanak meg. Egyre több tevékenységünket rögzítik használati eszközeink (például tartózkodási hely, meglátogatott oldalak, elkészített fényképek, online vásárlások, keresések). A digitalizáció következtében a cégek rengeteg, a tevékenységükhöz kapcsolódó adathoz jutnak

▸ Gépi tanulás

hozzá (gyártási, forgalmi adatok, vásárlók adatai stb.). Egyre több eszközünk kapcsolódik a hálózathoz. Köztük van számos olyan, amelynek hagyományosan nem ez az alapfunkciója, de a hálózati kapcsolattal többletszolgáltatást nyújthat számunkra. Ezek képesek a hálózaton keresztül kommunikálni más eszközökkel, adataikat megosztani és ezt felhasználni az optimális működésük érdekében. Ezek az eszközök alkotják a **dolgok internetét (Internet of Things: IoT)**.

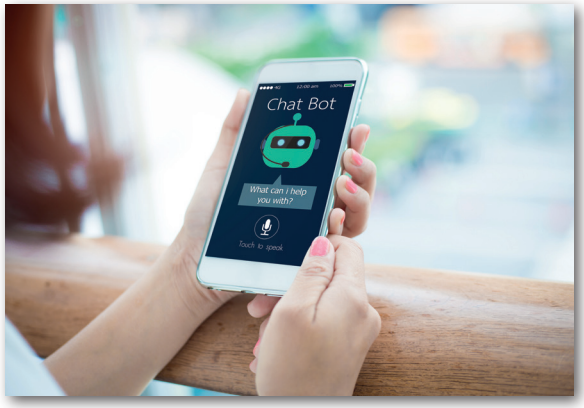
Az IoT a napról napra gyarapodó adatmennyiség elemzésére, feldolgozására új lehetőségeket nyit a gazdaság, a tudomány és a mindennapi élet számos területén. Ez az adatmennyiség nagyságrendileg nagyobb, mint amennyit korábban kezeltünk. Az adatok gyűjtése az IoT-eszközöknek, a hálózati kommunikációnak köszönhetően jelentősen felgyorsult. Feldolgozásuk, elemzésük új eljárásokat igényel. Az ezek mentén kialakuló terület a **Big Data**.

Bár gyakran észre sem vesszük, életünkben már ma is fontos szerepet kapnak a mesterséges intelligencia által működtetett eszközök, megoldások, és egyre nagyobb mértékben járulnak hozzá a fejlődéshez.

A mesterséges intelligencia alkalmazása napjainkban

Lássunk néhány általánosan használt alkalmazást, amelyek mögött mesterséges intelligencia áll.

- Az online kereséskor használt **keresőmotorokat** mesterséges intelligencia működteti.
- Az idegen nyelven megjelenő online tartalmak **automatikus fordításakor** is ezt használjuk.
- Alkalmas a beszéd, a zene és a kép felismerésére. Ez segíti a képalapú keresést, azokat az alkalmazásokat, amelyekkel fel tudjuk ismertetni a hallott zeneművet. Ezt használjuk, amikor hanggal irányítunk egy programot, de a videók automatikus feliratozását is ez végzi.
- Egyre több ügyfélszolgálat, weboldal használ **chatbotot,** azaz beszélgető robotot. Ezek a legygyakoribb kommunikációs helyzetekben képesek az ügyféllel beszélgetést folytatni és az egyszerűbb ügyeket megoldani. Ezzel enyhítenek az ügyfélszolgálat leterheltségén, gyorsabb kiszolgálást tesznek lehetővé. A lefolytatott párbeszédek adataiból tapasztalatokat gyűjtenek, így egyre jobb reakciót képesek adni a kialakuló helyzetekre.



► Chatbot

- A közösségi oldalak személyre szabott tartalma a mesterséges intelligencia segítségével készül. A viselkedésünkre vonatkozó megfigyelések alapján jelenik meg számunkra a várhatóan legkedveltebb tartalom, a személyre szabott reklám. Hasonló módszer alapján képesek személyre szólóan filmeket, zeneszámokat ajánlani a népszerű streamingszolgáltatók.

- **Biometrikus azonosítást,** ujjlenyomat-olvasót, arcfelismerő rendszert számos helyen használunk. Ezek is a mesterséges intelligencia segítségével működnek.
- Találkozhatunk már **önvezető járművekkel.** Ezeket ma még inkább az egyszerűbb forgalmi helyzetekben alkalmazzák. Ilyen például a budapesti 4-es metró, amelyet mesterséges intelligencia vezet.
- Idetartoznak a különböző célfeladatokat ellátó **robotok,** például a robotporszívók, a gyártási folyamatokat elvégző robotok.
- A számítógépes játékok gyakran használnak mesterséges intelligenciát. Ezzel élvezetesebbé teszik a játékot, azt az érzetet keltik, hogy egy valódi partnerrel versenyzünk.

Fejlődési irányok, társadalmi hasznosság

A mesterséges intelligencia fejlődése egyre gyorsuló tendenciájú. Egyre több az olyan terület, amelynek meghatározza a fejlődését. Komoly eredményeket érhetünk el használatával a gazdaság, a tudomány, a mindennapi életünk számos területén. Segíthet a folyamatok optimalizálásában, például a forgalomszervezésben, a jobb energiafelhasználásban, a gyártási folyamatok hatékonyabbá tételében. Pontosabbá és gyorsabbá teheti a diagnosztizálást, legyen szó betegségekről vagy gépek meghibásodásáról. A nagy mennyiségű adat megvizsgálásával képes előre jelezni olyan problémákat, amelyeket nélküle nehezebben ismerhetnénk fel. Használhatjuk ezért egészségmegőrzésre, bűnmegelőzésre, katasztrófavédelemre, termeléskiesés megelőzésére. Várhatóan átvesz tőlünk munkafolyamatokat, de egész munkaköröket is képes lehet ellátni. Alkalmas lehet arra is, hogy új tartalmat állítson elő – mesterséges intelligencia segítségével lehet például zenét komponálni, irodalmi műveket létrehozni. Képes olyan emberi arcokat előállítani, amelyek teljesen valósnak tűnnek, de nem élő emberekhez tartoznak. Tanulási folyamatuk lényegesen gyorsabb, mint az embereké. Az egyik eszköz által begyűjtött ismeretek a többi hasonló feladatot ellátó eszközzel azonnal megoszthatók, vagyis azonnal használhatják a másik eszköz által megszerzett összes ismeretet.

▸ Önvezető autók

Látható, hogy a mesterséges intelligencia számos területen segítheti az emberiség életét, a fejlődést, de nagyon fontos a megfelelő szabályozása. Csak kritikus gondolkodás mellett érdemes felhasználnunk, mert **alkalmazása veszélyeket is rejthet magában.** Társadalmi, erkölcsi és technikai problémát is okozhat, ha nem megfelelően kezeljük. Például a munkaerő kiváltására használt mesterséges intelligencia adhat nekünk rövidebb munkaidőt, kényelmesebb munkavégzést, ha megfelelően alkalmazzuk, de hozzájárulhat dolgozók munkanélkülivé válásához is. Az adatok széles körű felhasználása alkalmas a technika további fejlesztésére, de a hamis vagy manipulált adatok ezt az irányt eltéríthetik. Fontos, hogy az adatok anonimizálásáról megfelelően gondoskodjunk, hogy betartsuk az adatvédelmi szabályokat. Gyakran felmerül a mesterséges intelligenciával működő eszközök esetében a **felelősség kérdése.** Ki lesz a hibás abban az esetben, ha a mesterséges intelligencia nem a megfelelő döntést hozza, és ezzel valamilyen, akár nagyobb bajt okoz?

Azért lényeges ismerni az információs társadalom ezen területét, hogy képesek legyünk megfelelően szabályozni és kézben tartani. Ebben a tekintetben az állampolgároknak, a cégeknek és az államnak is lesz felelősségük.

Kérdések, feladatok

1. Keressük meg a mesterséges intelligenciával működő *Blob Opera* alkalmazást, amelyet operaénekesek segítségével tanítottak meg énekelni! Próbáljuk ki, alkossunk zenét vele!
2. Nézzünk utána, miről nevezetes a Google *DeepMind* algoritmusa!
3. Keressünk példát olyan mesterségesintelligencia-alkalmazásokra, amelyekkel találkoztunk már (ismert chatbotok, járművek, robotok stb.)! Beszéljük meg közösen a talált lehetőségeket! Ha szükséges, nézzünk utána!
4. Nézzünk utána, mi az a *deepfake!* Miért veszélyes?
5. Milyen veszélyes helyzeteket tudunk elképzelni, amelyeket a mesterséges intelligencia alkalmazása okozhat? Hogyan lehet ezeket kivédeni?
6. Milyen konkrét eszközök tartozhatnak az *IoT* kategóriába? Keressünk példákat arra, hogy hogyan egészülhetnek ki az eszköz alapszolgáltatásai! Mi magunk milyen IoT-eszközöket használunk?
7. Mit jelent az okosotthon kifejezés? Milyen szolgáltatásokat nyújt használójának?

Kriptográfiai alapfogalmak

A napi számítógép-használat során gyakran találkozunk az operációs rendszer és a hálózati összetevők (eszközök, protokollok) biztonsági mechanizmusaival. Adataink védelme érdekében alapvető fontosságú ezek megismerése és megértése. Minden operációs rendszer biztosítja számunkra a lokális gépen, illetve lokális hálózaton tárolt adatfájljaink hozzáférés-védelmét, amely a felhasználó azonosításán és hitelesítésén alapul (DAC: discretionary access control). Ez azt jelenti, hogy csak a felhasználónév (azonosítás) és a hozzá tartozó jelszó (hitelesítés) megadásával történt bejelentkezés után férhetünk hozzá az adatfájlokhoz (és egyéb védendő objektumokhoz), és csak olyan módon, ahogyan az az egyes fájlokon/objektumokon engedélyezett számunkra (például csak olvasás, de írás nem).

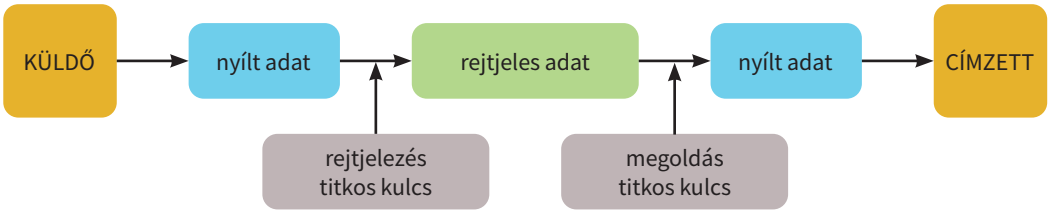
Ez a fajta védelem nem terjed ki az interneten elérhető adatokra és erőforrásokra. Ezért az internetről letöltött/feltöltött adatok hitelességét és hozzáférés-védelmét más módon kell biztosítani. A továbbiakban ezeket a biztonsági mechanizmusokat tekintjük át, amelyek megértéséhez néhány egyszerű kriptográfiai fogalmat kell tisztázni.

Rejtjelezés

Az adatok védelmének érdekében rejtjelezést az ősidők óta használnak. Célja, hogy a nyilvános csatornán (például internet) továbbított bizalmas adatokat védjük az illetéktelen megismerés ellen. Ezért a **nyílt adatot** csak a küldő és a címzett által ismert **kulccsal** rejtjelezzük, majd a **rejtjeles adatot** küldjük át a nyilvános (védtelen) csatornán. A címzett a közös kulcs ismeretében **meg tudja oldani** a rejtjeles adatot, így olvashatóvá válik számára a nyílt adat. A rejtjelezési eljárást **rejtjelalgoritmusnak** nevezzük. Nagyon egyszerű rejtjelalgoritmus lehet például az, hogy a nyílt szöveg minden betűjét más betűre cseréljük, így téve értelmezhetetlenné a rejtjeles szöveget. Ebben az esetben a kulcs a betűcseréket leíró permutáció. Természetesen ez az algoritmus szinte semmit sem ér, mivel egy kicsit is intelligensebb kódfejtő a kulcs ismerete nélkül is képes visszanyerni a rejtjeles szövegből a nyílt szöveget. Ezt a műveletet nevezzük **megfejtésnek** (vagy rejtjelfejtésnek). Összefoglalva a most megismert fogalmakat:

- **Nyílt adat:** a rejtjelezendő adat.
- **Rejtjeles adat:** a nyílt adat rejtjelezett formája, amely nyilvános csatornán továbbítható.
- **Rejtjelalgoritmus:** a rejtjelezés műveletét leíró algoritmus.
- **Kulcs:** a rejtjelalgoritmus működését meghatározó titkos adat (csak a küldő és a címzett ismerheti).
- **Rejtjelezés:** rejtjeles adat előállítása a nyílt adatból a kulcs ismeretében, rejtjelalgoritmus használatával.
- **Megoldás:** nyílt adat előállítása a rejtjeles adatból a kulcs ismeretében, a rejtjelalgoritmus használatával.
- **Megfejtés:** nyílt adat előállítása a rejtjeles adatból, a kulcs ismerete nélkül. A rejtjelalgoritmus vagy ismert, vagy nem (nehezebb eset).

A leírt rejtjelezési sémát **szimmetrikus kulcsú rejtjelezésnek** nevezzük, mivel a rejtjelezéshez és a megoldáshoz is ugyanazt a kulcsot használjuk.



▶ Szimmetrikus kulcsú rejtjelezés

Léteznek **aszimmetrikus kulcsú rejtjelezési algoritmusok** is, ahol a rejtjelező- és a megoldókulcs különböző. A példaként leírt betűcserés algoritmusnál (szaknyelven: egyszerű helyettesítés) jóval fejlettebb algoritmusokat használunk. Közkeletű tévedés, hogy megfelelő erőforrás-ráfordítással minden rejtjelezés feltörhető (megfejthető). Ez egyrészt elvileg sem igaz (mivel léteznek elvileg sem megfejthető rejtjelezések), másrészt a modern algoritmusok gyakorlatilag csak a kulcs teljes kipróbálásával fejthetők meg. A teljes kipróbálás azt jelenti, hogy az összes lehetséges kulcsot végig kell próbálni a rejtjelalgoritmussal, míg meg nem kapjuk a nyílt adatot. Ha például a kulcs 128 bites, akkor 2^{128} számú esetet kell tekintetbe venni a megfejtés során (128 bit körülbelül 20-21 beírható karakternek felel meg). A modern algoritmusok esetén (például AES, IDEA, HC128) a mai tudásunk szerint ez gyakorlatilag kivitelezhetetlen. Ez nem jelenti azt, hogy ne lenne támadható a rejtjelezés, ha gyenge kulcsot adtunk meg.

Gyenge (begépelt) kulcsok ellen jól ismert módszer a **szótáralapú támadás.** Ekkor egy szótárból veszik a kipróbálandó jelszavakat vagy azok némileg módosított formáit, annak reményében, hogy a rejtjelező pont azt a szót választotta kulcsként.

Az interneten használt biztonságos protokollok (például https) is alkalmaznak szimmetrikus kulcsú rejtjelezést, azonban nyilván nem begépelt, hanem véletlenszerűen generált kulccsal. Itt a fő kérdés az, hogy hogyan alakítanak ki közös szimmetrikus kulcsot a kommunikáló felek. Erre a problémára az aszimmetrikus kulcsú rejtjelezés nyújt megoldást.

Hitelesítés

A hitelesítés célja, hogy az adat és/vagy a forrás hitelességét bizonyítsa. Az adat hitelessége azt jelenti, hogy a kommunikáció során az adat nem sérült, vagyis valóban a feladó által eredetileg elküldött adatot kaptuk meg sértetlen állapotban. Az átviteli hibákból adódó (tehát nem rosszindulatú támadás miatti) adatsérülés különböző kontrollösszegek (például CRC – Cyclic Redundancy Check) alkalmazásával észlelhető és javítható. Rosszindulatú támadás ellen ez nem véd, mivel a támadó a manipulált adatra számolhat helyes kontrollösszeget. Az ilyen támadás ellen a **digitális aláírás** védi az adatot, amely az aláíró személy azonosságát (a forrás hitelességét) is bizonyítja. Tehát a hagyományos, papíralapú dokumentum aláírásával szemben a digitális aláírás nemcsak az aláíró személyét bizonyítja, hanem az aláírt dokumentum tartalmát és akár idejét is (vagyis azt, hogy valóban az aláíró személy, valóban azt a tartalmú dokumentumot és valóban abban az időpontban írta alá).

A **digitálisan aláírt** (vagy másként: elektronikusan hitelesített) **dokumentum** aláírását természetesen csak számítógépen lehet ellenőrizni. Vagyis a papírra kinyomtatott, elektronikusan hitelesített dokumentum **nem hiteles,** hiába látható rajta az „elektronikusan

hitelesített” pecsét. Tipikus példa erre a Földhivataltól kikért, elektronikusan hitelesített, kinyomtatott tulajdoni lap, amelyet **nem szabad hitelesnek elfogadni,** hiszen az „elektronikusan hitelesített” pecsétet bárki rászerkesztheti bármilyen papíralapú dokumentumra. A digitálisan aláírt PDF-fájlt megfelelő PDF-olvasó programmal (Acrobat Reader, Foxit Reader stb.) betöltve lehet (és kell) ellenőrizni. Ez hibát jelez, ha a dokumentum tartalma megváltozott az eredeti (aláírt) tartalomhoz/időponthoz képest, vagy ha nem a deklarált személy/hivatal írta alá.

Digitális aláírást egyaránt lehet alkalmazni nyílt (például tulajdoni lap) és rejtjeles dokumentumon, illetve adatfolyamon. Ritkább eset, hogy a dokumentumot/adatfolyamot csak rejtjelezik, de nem hitelesítik, bár maga a rejtjelezés is biztosít bizonyos szintű (sokszor elegendő) adat- és forráshitelességet. Ugyanis ha a címzett a közös kulccsal meg tudja oldani a rejtjeles adatot, és értelmes szöveget kap vissza, továbbá biztos benne, hogy a közös kulcsot csak a kommunikáló felek ismerik, akkor ez önmagában is bizonyítja az adat és a forrás hitelességét. Az interneten használt biztonságos protokollok azonban mindig alkalmaznak hitelesítést is. Manapság megfigyelhető, hogy alig akad olyan nyilvánosan elérhető weboldal, amely nem a biztonságos https-protokollt, hanem a nyílt http-protokollt használja. Ennek oka elsősorban az adat és forrás hitelességének bizonyítása, és nem a tartalom rejtjelezése (hiszen az nyilvános).

Kérdések, feladatok

1. Nézzünk utána, mit jelent a Caesar-kód vagy Caesar-rejtjel! Miért fejthető meg könnyen az így kódolt üzenet?
2. Mi a különbség a rejtjelezett adat megoldása és megfejtése között?
3. Milyen nyelvi jellemzők alapján ismerhető fel az egyszerű helyettesítés? Hogyan lehetne megfejteni?
4. Nézzünk utána, mi az az Enigma! Hogyan kapcsolódik a történelemi eseményekhez és a számítógépekhez?
5. Készítsünk programot, amely egy szöveg titkosítását valósítja meg egyszerű helyettesítés segítségével!

Aszimmetrikus kulcsú titkosítás

Hashfüggvény

A digitális aláírás működésének megértéséhez még meg kell ismerkednünk a hash- (hasító) függvény fogalmával.

> A hashfüggvény olyan matematikai művelet, amely tetszőleges hosszúságú adatfolyamhoz fix hosszúságú bitsorozatot rendel.

Az adatfolyam **hashértéke** tulajdonképpen az adatfolyamra jellemző kivonat. Ez azt jelenti, hogy ha az adatfolyam egyetlen bitje megváltozik, akkor a hashértéke teljesen más lesz (a hashérték bitjeinek körülbelül a fele megváltozik). Vagyis gyakorlatilag lehetetlen egy adott hashértékhez másik adatfolyamot találni, amelynek ugyanez lesz a hashértéke. Természetesen végtelen sok olyan adatfolyam létezik, amelynek ugyanaz a hashértéke, hiszen a fix hosszúságú hashértékek száma véges (például ha a hash 160 bites, akkor 2^{160} darab különböző hashérték van), míg az adatfolyamok száma végtelen.

Két azonos hashértékű adatfolyam esetén **hashütközésről** beszélünk. A hash elleni támadás során az adott hashértékhez kell találni olyan adatfolyamot, amelynek éppen ez az érték a hashértéke. Ez kriptográfiai hash- (SHA1-, MD5-) függvények esetén gyakorlatilag kivitelezhetetlen (bár az MD5 128 bites hasht már nem tekintik kriptográfiailag biztonságosnak). Az átviteli hibák ellen védő kontrollösszegek (például CRC) szintén hashfüggvénynek tekinthetők, de semmiképpen nem kriptográfiailag biztonságosnak.

Hashfüggvény képezhető rejtjelező algoritmusból is, például úgy, hogy a hashelendő adatfolyamból kulcsot képeznek, amellyel fix nyílt adatot (például a hash hosszúságának megfelelő csupa 0 bitet) lerejtjelezik, és ezt tekintik hashértéknek. Tehát itt a nyílt adat (a hash hosszúságának megfelelő csupa 0 bit) és annak rejtjeles képe ismert (ez a hashérték), ebből azonban a kulcsot (a hashelt adatfolyamot) nem lehet visszaállítani.

A **digitális aláírás folyamata** a következőképpen történik: az aláírandó dokumentumnak kiszámolják a kriptográfiai hashértékét (például 160 bites SHA1), amelyet az aláíró kulcsával lerejtjeleznek, és mellékelnek a dokumentumhoz. Az aláírást a másik fél ellenőrizni tudja, ha ismeri az aláírókulcsot, ugyanis ugyanezt a műveletet megismételve ugyanezt az eredményt kell kapnia (pre-shared key alapú digitális aláírás). A nagy probléma ezzel a módszerrel az, hogy bárki produkálhat megfelelő aláírást, aki ellenőrizni tudja, hiszen ismeri az aláírókulcsot. Bizonyos protokollok ennek ellenére használják a pre-shared key alapú digitális aláírást (például az IPsec gatewayek). A fenti probléma az aszimmetrikus kulcsú rejtjelezéssel kezelhető, amikor a rejtjelező- és megoldókulcs különböző.

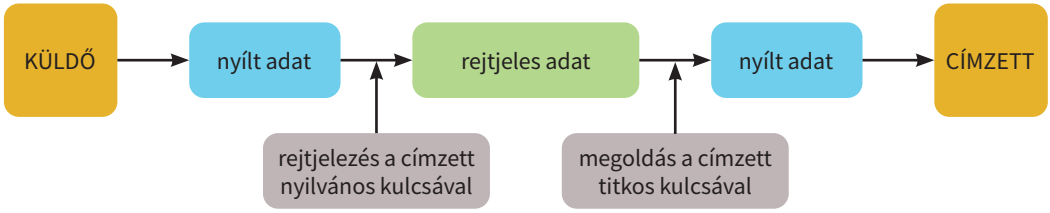
Aszimmetrikus kulcsú rejtjelezés

Az interneten zajló kommunikáció során közvetlenül nem alkalmazható a szimmetrikus kulcsú rejtjelezés és hitelesítés (aláírás), hiszen a kommunikáló felek a nyílt csatornán nem küldhetik át a szimmetrikus kulcsaikat. Ezért más megoldást kell találni. Az alapötlet az, hogy mindegyik fél saját kulcspárral rendelkezik, amelyikből az egyik **titkos** (private) **kulcs,** a másik pedig a **nyilvános** (public) **kulcs.** A titkos kulccsal rejtjelezett adat a neki megfelelő

nyilvános kulccsal oldható meg (hitelesítés, aláírás). Azonban a nyilvános kulcs is használható rejtjelezésre, amely a neki megfelelő titkos kulccsal oldható meg (nyilvános kulcsú rejtjelezés). Ez úgy képzelhető el, mint egy lakat, amelyhez két különböző kulcs tartozik. Az egyik kulccsal bezárt lakatot csak a másik kulccsal lehet kinyitni, azonban bármelyik kulccsal zárható a lakat. A két kulcs összetartozik: a titkos kulcsnak csak az adott nyilvános kulcs lehet a párja, és viszont. Az interneten kommunikáló felek aszimmetrikus kulcsok segítségével, a következőképpen kommunikálnak: mindegyik fél generál saját maga számára egy aszimmetrikus kulcspárt. A kulcspár egyik kulcsát kinevezi titkos kulcsnak, amelyet ezután titokban tart, és nem ad ki senkinek. A kulcspár másik kulcsát pedig kinevezi nyilvános kulcsnak, és közzéteszi. Bárkinek elküldi, aki kommunikációt kíván kezdeményezni vele. Az aszimmetrikus kulcspár rejtjelezésre és aláírásra egyaránt használható.

Rejtjelezés aszimmetrikus kulccsal

Tegyük fel, hogy András rejtjeles üzenetet kíván küldeni Beának. Nincs még közös szimmetrikus kulcsuk, ezért András elkéri Bea nyilvános kulcsát. Mivel ez nyilvános kulcs, küldhető nyílt csatornán. András Bea nyilvános kulcsával rejtjelezi az üzenetet, amelyet Bea a saját titkos kulcsával meg tud oldani. A gyakorlatban az aszimmetrikus kulcsú rejtjelezést szimmetrikus kulcs kicserélésére használják (például PGP), vagyis András üzenete a javasolt szimmetrikus kulcs lesz, mivel a szimmetrikus kulcsú rejtjelezés sokkal gyorsabb.



▶ Rejtjelezés aszimmetrikus kulccsal

Aláírás aszimmetrikus kulccsal

Tegyük fel, hogy András olyan üzenetet kíván küldeni Beának, amelyben bizonyítja, hogy valóban ő az üzenet írója, és valóban az az üzenet tartalma, amit aláírt. Az üzenet nem feltétlenül rejtjelezett. Először is, András elküldi saját nyilvános kulcsát Beának, aki majd ezzel tudja ellenőrizni András aláírását. András megírja az üzenetet, hashértéket számol rá (például SHA1-et), majd a hashértéket rejtjelezi a saját titkos kulcsával. Ez a rejtjelezett hashérték lesz az üzenet aláírása, amelyet az üzenethez mellékelve szintén átküld Beának. Bea megoldja az aláírást András nyilvános kulcsával, és az eredményt összeveti az általa szintén kiszámolt hashértékkel. Ha a két érték egyezik, akkor az üzenet tartalma sértetlen, és valóban András az aláíró.

Mint a fenti példákból megfigyelhető, rejtjelezésnél a partner nyilvános kulcsával rejtjelezzük az üzenetet, amit ő a titkos kulcsával tud megoldani. Aláírásnál a hashértéket saját titkos kulcsunkkal rejtjelezzük, amit a partner a mi nyilvános kulcsunkkal tud ellenőrizni. Tehát a rejtjelezésnél a nyilvános kulcsot rejtjelezésre, a titkos kulcsot megoldásra használjuk, míg aláírásnál a titkos kulcsot rejtjelezésre, a nyilvános kulcsot pedig megoldásra használjuk.

► Aláírás aszimmetrikus kulccsal

A legismertebb és legszélesebb körben használatos aszimmetrikus kulcsú rejtjelrendszer az RSA (Rivest–Shamir–Adleman). RSA-kulcspár generálásánál két nagyon nagy prímszámot (1024–4096 bitest) választanak, amelyek szorzatából képezik a nyilvános kulcsot (nem pont a szorzat lesz a nyilvános kulcs!). Hogy a nyilvános kulcsból a hozzá tartozó titkos kulcsot ki lehessen számolni, ezt a szorzatot kellene tényezőkre bontani. Ez azonban ekkora prímek esetén gyakorlatilag megoldhatatlan feladat. Ez adja az **RSA-módszer** erejét. Ezenkívül léteznek más aszimmetrikus kulcsú rendszerek is.

A most vázolt aszimmetrikus kulcsú rejtjelezéssel és aláírással van egy nagyon nagy probléma: a nyilvános kulcsok közzététele/terjesztése nem hitelesített. Ez azt jelenti, hogy András ugyan elkéri Bea nyilvános kulcsát (és Bea Andrásét), de nem lehet biztos benne, hogy valóban Bea nyilvános kulcsát kapta meg. Egy közbeékelődő támadó (man-in-the-middle attack) eljátszhatja Bea szerepét András felé, és András szerepét Bea felé. Ekkor mindketten a támadó nyilvános kulcsát kapják meg, azt gondolván, hogy az a partnerük nyilvános kulcsa. A támadó olvashatja a rejtjeles üzeneteket, átírhatja a tartalmukat, és hamisíthatja az aláírásokat. Mindebből András és Bea semmit nem vesznek észre. Ennek a problémának a megoldására jöttek létre a **tanúsítványok (certificate)** és a **tanúsítványkibocsátó szervezetek** (certificate authority: CA).

Tanúsítványok

A tanúsítványok – nagyon leegyszerűsítve – tanúsítványkibocsátó szervezet által digitálisan aláírt nyilvános kulcsok. Emellett számos egyéb információt is tartalmaznak (a tulajdonos neve, https esetén doménnév, lejárati dátum stb.). Tanúsítványok alkalmazásával kivédhetők a közbeékelődő támadások, mert a CA garantálja, hogy az általa aláírt tanúsítvány valóban a tanúsítványban megnevezett entitáshoz (magánszemély, szervezet, szerver) tartozik (https-tanúsítványban a doménnév is szerepel). A tanúsítvány ellenőrzése az aláíró CA nyilvános kulcsa (tanúsítványa) segítségével történik, ami az ellenőrzést végző gépen már eleve el lett tárolva (például a Windows telepítésekor). Tehát az egész infrastruktúra működése azon alapul, hogy a kommunikáló felek megbíznak egy harmadik félben (ez a CA), aki biztosítja őket a másik fél személyazonosságáról. Ezt a modellt **„Trusted-Third-Party”-modellnek** nevezik (röviden: TTP). A kommunikáló felek nem tudják ellenőrizni, hogy a harmadik fél az ő érdekükben jár el (például nem ad ki hamis tanúsítványt), ezért kénytelenek megbízni benne, hasonlóan ahhoz, mint ahogy az állami hivatalok tisztességes működésében is megbízunk. Ez a fajta bizalmi viszony a harmadik fél (CA) felé akkor jön létre, amikor például a Windows operációs rendszert telepítjük a gépünkre, melynek során a megbízhatónak nyilvánított CA-k tanúsítványa bekerül az operációs rendszer tanúsítványtárába. Vagyis, ha megbíztunk az operációs rendszer telepítőcsomagjának eredetiségében, akkor

a feltelepített CA-tanúsítványokban (és ezzel együtt magukban a CA-kban) is meg kell bíznunk. A feltelepített CA-tanúsítványok között az összes, úgynevezett root CA- (gyökér CA-) tanúsítvány megtalálható lesz (lásd később).

A tanúsítványkibocsátó szervezetek (CA) adott esetben kiadhatnak alárendelt tanúsítványkibocsátó szervezetek (röviden: al-CA) részére olyan tanúsítványt, amellyel azok szintén kiadhatnak tanúsítványokat. Így egy **tanúsítványlánc** jön létre. A tanúsítványlánc tetején a root CA áll. A root CA-tanúsítványát értelemszerűen csak saját maga képes aláírni, ezért az ilyen tanúsítványt **önaláírtnak** nevezzük. Csak root CA esetén tekinthető érvényesnek az önaláírt tanúsítvány. A tanúsítványlánc alján a **végfelhasználói tanúsítvány** áll. Végfelhasználói tanúsítvánnyal már nem lehet újabb tanúsítványt aláírni (kibocsátani). A tanúsítványláncban szereplő CA-k nem rendelkeznek az általuk kibocsátott tanúsítványok nyilvános kulcsának titkos párjával.

A különböző szintű tanúsítványok a szintjüknek megfelelő adminisztratív eszközökkel igényelhetők. Például nagyvállalati szintű CA-tanúsítványt a megfelelő országos szintű CA-tól kell igényelni. Az igénylés során adminisztratív módon (céges papírok, közjegyző, személyes megjelenés, személyazonosítás stb.) kell bizonyítani az igénylő entitás személyazonosságát és jogosultságát, aminek jelentős anyagi vonzata is lesz. A végfelhasználói (tanúsítványkibocsátásra alkalmatlan) tanúsítvány igénylése lényegesen egyszerűbb és olcsóbb. Nincs feltétlenül szükség adminisztratív személyazonosításra, és akár ingyen is igényelhető (például Let's Encrypt). Természetesen ebben az esetben is szükség van valamiféle bizonyítékra, hogy például (https esetén) az adott domén a mi felügyeletünk alá tartozik.

A tanúsítványlánc ellenőrzése a végfelhasználói tanúsítványtól indul. A láncban felfelé haladva a kibocsátó CA nyilvános kulcsával ellenőrizzük a tanúsítványkibocsátó általi aláírást, míg el nem jutunk a root CA-hoz. A root CA önaláírt tanúsítványa természetesen érvényes, mivel szerepel az operációs rendszer tanúsítványtárában. Ha az ellenőrzési lánc valahol megszakad, akkor a végfelhasználói tanúsítvány érvénytelen.

András és Bea kommunikációjában a tanúsítványok használata a következőképpen néz ki: mindketten RSA-kulcspárt generálnak maguk számára, majd a nyilvános kulcsukat és egyéb adatokat átadják egy megbízható CA-nak. A CA, miután meggyőződött az igénylő személyazonosságáról, a kapott adatokból előállítja a tanúsítványnak megfelelő adatstruktúrát, amelyet a saját titkos kulcsával aláír. Az így létrejött adatstruktúrát nevezzük tanúsítványnak. Ezután András és Bea között a már ismertetett módon zajlik a kommunikáció. Mindkettőjüknek a másik nyilvános kulcsára van szüksége (akár rejtjelezésről/kulcscseréről, akár aláírás ellenőrzéséről van szó), de most már a nyilvános kulcsok eredetiségében megbízhatnak, hiszen azokat egy általuk megbízhatónak tartott CA aláírta. Vagyis a kommunikáció nem a nyilvános kulcsok, hanem a tanúsítványok cseréjével kezdődik.

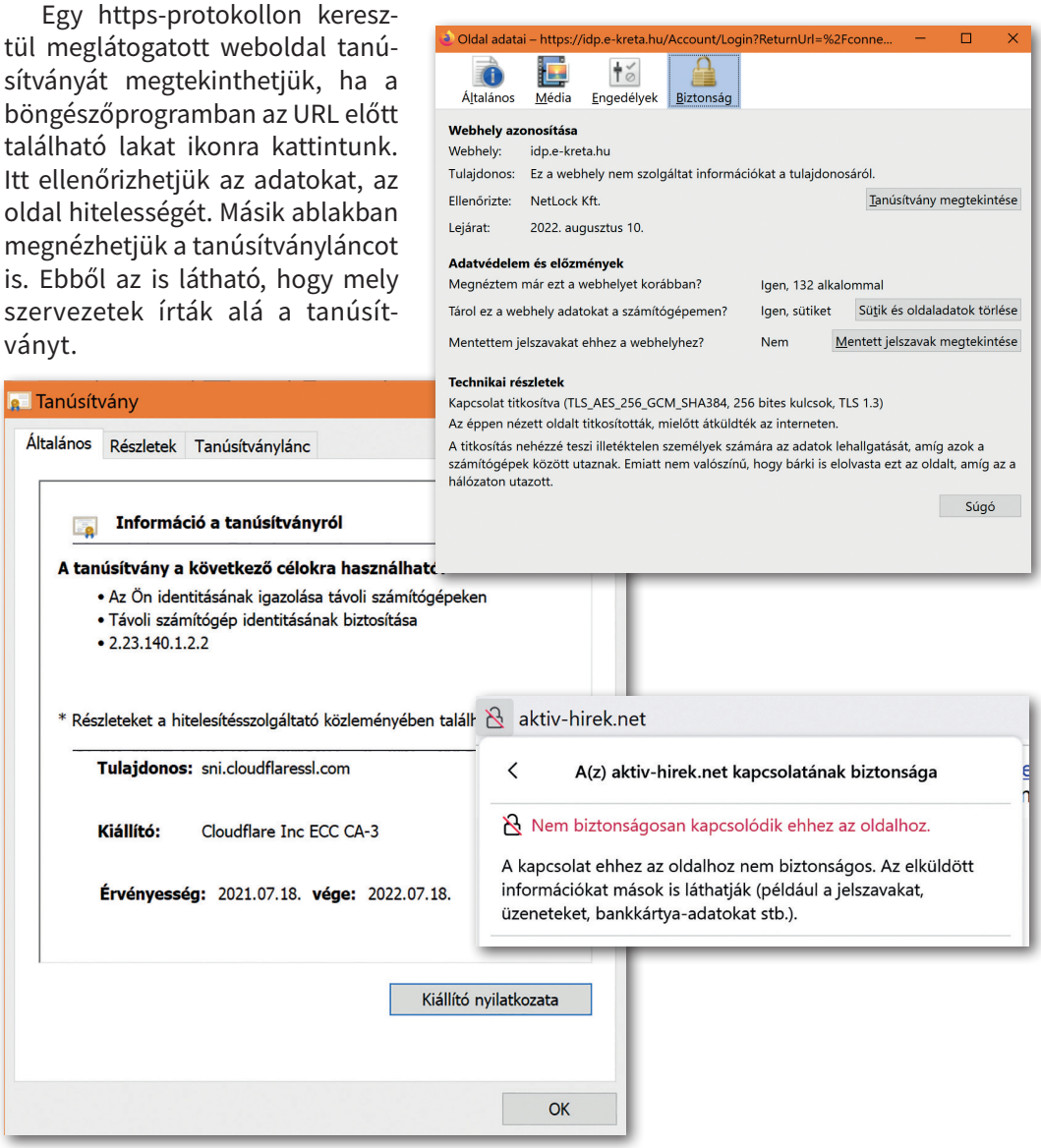
Kérdések, feladatok

1. Milyen előnye van a digitális aláírásnak? Miben különbözik a hagyományos aláírástól? Mit garantál még az aláíró személyén kívül?
2. Nézzünk utána, hogy magánszemélyként, magyar állampolgárként hogyan használhatunk elektronikus aláírást!

Adatvédelem böngészés közben

A https-protokoll mind tartalom-rejtjelezést, mind pedig forrás-/adathitelesítést biztosít, amihez az RSA-tanúsítvány-CA infrastruktúrát használja. A hitelesítést általában „csak féloldalasan” alkalmazzák, ami azt jelenti, hogy csak a szerver hitelesíti magát a kliens felé, de fordítva általában nem. A hitelesítés során a kliens ellenőrzi a szerver tanúsítványát.

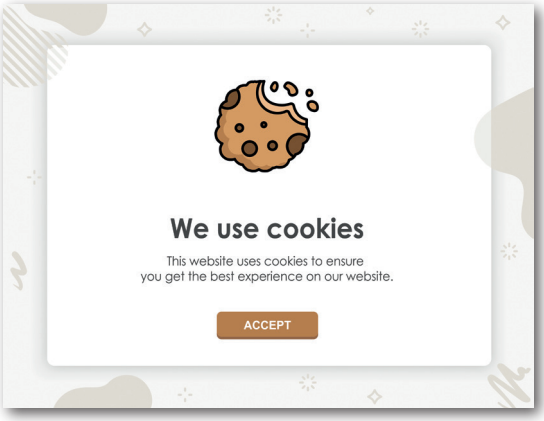
Egy https-protokollon keresztül meglátogatott weboldal tanúsítványát megtekinthetjük, ha a böngészőprogramban az URL előtt található lakat ikonra kattintunk. Itt ellenőrizhetjük az adatokat, az oldal hitelességét. Másik ablakban megnézhetjük a tanúsítványláncot is. Ebből az is látható, hogy mely szervezetek írták alá a tanúsítványt.



Érdemes tehát figyelnünk arra, hogy az általunk meglátogatott weboldal tanúsítványa rendben legyen. Ennek segítségével győződhetünk meg arról, hogy valóban a megfelelő oldallal kommunikálunk.

Ha belépünk egy weboldalra, gyakran tapasztaljuk, hogy el kell fogadnunk a **sütik** (cookies) használatát. Az előző években már megismerkedtünk a süti fogalmával. Tudjuk, hogy ezek kis méretű, adatokat tartalmazó fájlok, amelyeket a weboldal a böngészőprogram segítségével tárol a számítógépünkön. A webszerver és a böngészőprogramok közötti kommunikációt segítik.

A böngészés során többfajta sütit használhatunk.



► Sütik használatára figyelmeztető üzenet

- A **munkamenetsütik** (session cookies) a weboldal működéséhez szükségesek. Nélkülük nem folytatható megfelelő kommunikáció a weboldallal. Érvényességük a weboldalról való kilépéssel lejár, ezért a böngészőprogram bezárásakor automatikusan törlődnek. Ezek a sütik tehát ideiglenesek. Feladatuk sokféle lehet, például a felhasználó azonosítását, a webportál egyes lapjai közötti közlekedést vagy a multimédia-lejátszás beállításait segíthetik.
- Az **állandó sütik** segítségével a weboldallal való kommunikációt tehetjük gördülékenyebbé. Ezeknek köszönhetően oldható meg, hogy ne kelljen beírni a bejelentkezési adatainkat, rögzíteni a kedvelt beállításainkat minden alkalommal, amikor az oldalra bejelentkezünk. Ezek a sütik az oldal elhagyása után is tárolódnak a számítógépünkön, így tudják megőrizni a szükséges adatokat az oldal következő felkereséséig. Egy másik fajtájuk az oldalon való tevékenységeink statisztikai megfigyelését teszi lehetővé. Ez részben az oldal üzemeltetőinek nyújt segítséget a szolgáltatásuk fejlesztéséhez. Lehetséges, hogy céljuk az oldalon megjelenő reklámok egyénre szabása.
- A **harmadik féltől származó** sütiket nem az az oldal hozza létre, amelyiket böngésszük. Ilyen lehet például, amikor a weblapon megjelenő gomb segítségével valamelyik közösségi oldal szolgáltatásait használhatjuk, például lájkolhatjuk, megoszthatjuk a tartalmat. Ilyen az is, amikor egy másik oldal helyezi el a saját hirdetéseit a böngészett oldalon. Használatuk a böngészett oldal számára anyagi hasznot hoz. Ezek a sütik alkalmasak lehetnek a látogató személyének azonosítására.

Az Európai Unió **GDPR**-szabályozásának megfelelően a weboldalaknak tájékoztatást kell nyújtaniuk a sütik használatáról. Amennyiben nem csak a technikailag szükséges sütiket használják, beleegyezésünket kell kérniük ehhez. Ezt a beleegyezést bármikor megváltoztathatjuk. Erre azért van szükség, mert tágabb értelemben véve a böngészési szokásaink, beállításaink, a sütik által tárolt és átadott adataink is tekinthetők személyes adatnak, bizonyos esetekben beazonosítható a személyünk általuk.

► Sütik törlése Mozilla Firefoxban

A böngészőprogramok mindegyikében lehetőségünk van a sütikkel kapcsolatos beállítások kezelésére, a feleslegesek törlésére. Ezt az összes sütire együtt vagy weboldalanként is megtehetjük. Időnként érdemes ezeket az adatokat áttekinteni.

A böngészőprogramok lehetőséget nyújtanak arra is, hogy a nyomkövető weboldalak tevékenységét a beállításokon keresztül korlátozzuk.

Kérdések, feladatok

1. Tekintsük meg egy biztonságos kapcsolaton keresztül felkeresett weboldal tanúsítványát! Nézzük meg a tanúsítványláncot is!
2. Miért lehet gyanús, ha ingyenes szervezet szolgáltatja egy fontos adatainkat bekérő weboldal tanúsítványát?
3. Keressük meg, tekintsük át a böngészőprogramunk adatvédelmi beállításait!
4. Nézzük meg egy kiválasztott weboldalon a cég adatvédelmi nyilatkozatait, beállítási lehetőségeit! Keressük meg, hol lehet megváltoztatni a sütik kezelésére vonatkozó nyilatkozatunkat!
5. Milyen következményekkel járhat, ha a böngészőprogramban valamelyik weboldalhoz tartozó sütiket töröljük?