Kriptográfia és Információbiztonság
1. előadás

MÁRTON Gyöngyvér

Sapientia Egyetem, Matematika-Informatika Tanszék
Marosvásárhely, Románia
mgyongyi@ms.sapientia.ro

2025

Bevezető

- a kriptográfia talán az írás megjelenésével egyidős → Klasszikus kriptográfia
- legtöbbször diplomáciai-katonai életben alkalmazták,
- csak titkosítást végeztek,
- könnyen feltörhetőek statisztikai elemzések alkalmazásával,
- két fél között a bizalmas információcserét valósították meg,
- a számítógépes környezetben a klasszikus rejtjelezők statisztikai elemzésekkel feltörhetők → kriptoanalízis
- az adatok rejtjelezése (encryption):
  - rejtjelező, titkosító (cypher): egy algoritmus, egy eljárás, amely alapján átalakították az adatokat,
  - az adatok általában valamilyen nyelv betűi, szavai voltak, pl. latin nyelv, angol nyelv
  - a klasszikus rejtjelezők legtöbbször titkosak voltak,
  - egy szigorúan titkos információ a kulcs segítségével végezték,
  - a rejtjelezett tartalmat a kulcs segítségével amikor szükséges volt visszaállították.

Bevezető

- a mai számítógépes rendszerek esetében:
  - a bemeneti adathalmaz elemei legtöbbször bitek, vagy bájtok, vagy olyan matematikai objektumok, amely átalakíthatóak bitekké, bájtszekvenciákká,
  - a kriptográfia további fontos feladatokat is ellát: az adatok integritásának, hitelességének a biztosítása, a kommunikáló felek hitelesítése, személyek, eszközök azonosítása, stb.
- biztonságos kriptorendszer tervezése, implementálása, működtetése:
  - nem egy egyszerű feladat, nem egyszemélyes munka,
  - komoly szakmai felkészültséget igényel: matematikai és programozói ismeretek,
  - etikai, filozófiai, politikai problémák: személyi jogok, szólásszabadság, hatalom kiszolgálása, fekete piac, stb.
- a modern kriptográfia ugyanakkor lenyűgöző!!

Kriptográfia és információbiztonság

- Modern kriptográfia (cryptography)
  - az információ elrejtése, rejtjelezése
  - bizalmas információ-csere
  - az adatok sértetlenségének a biztosítása
  - kommunikáló felek azonosítása
  - stb.
- Hozzáférési jogosultságok (access control)
  - hitelesítés (authentication): adott eszköz, felhasználó beléphet-e egy rendszerbe, hozzáférhet-e egy rendszer adataihoz
  - engedélyezés (authorization): milyen jogosultságokkal rendelkezik egy adott eszköz, felhasználó egy adott rendszeren belül
- Biztonsági protokollok (protocols): szabályok összessége, amelyeket adott helyzetben be kell tartani, ahhoz hogy a rendszer biztonsága ne sérüljön
- Szoftverek (software) az információ tárolására, továbbítására, feldolgozására, stb. szoftvereket használunk; pl egy vírus olyan szoftver, ami kárt tehet egy adott informatikai rendszerben

Alkalmazási terület

- A kommunikáció biztonsága:
  - a webforgalom biztonságát kriptográfiai eljárások biztosítják, a protokoll neve: HTTPS (RSA, Diffie-Hellman, AES, 3DES, RC4)
  - a wifi eszközök biztonságos adatmegosztását a WPA2 protokoll biztosítja
  - a mobil telefonok, a GSM alapú telefonok biztonságát folyamtitkosítási eljárás biztosítja: A5 titkosító család (linear feedback shift register)
  - bluetooth protokoll biztonságát folyamtitkosítási eljárás biztosítja: EO
- A merevlemez biztonsága: a Windows EFS (Encypting File System) titkosítása, régebbi verziókban DESX, az újabbakban AES, SHA, ECC
- A Blu-ray, DVD, CD tartalmak biztonsága: AACS (Advanced Access Control System) másolásvédelmi tehnológia, a lemezen és a készüléken titkosító kulcsok vannak beállítva, amelyeket a lejárati idő után meg kell újítani
- ...

Törzsanyag

- Klasszikus kriptográfiai rendszerek (Caesar és változatai, Affine, Hill)
- Titkos-kulcsú titkosító rendszerek (secret-key encryption, symmetric encryption)
  - matematikai modell, biztonság, tervezés
  - folyam-titkosító rendszerek (stream ciphers): OTP, RC4, LFSR, A5/1, Salsa20, ChaCha20,
  - blokk-titkosító módok (block cipher mode): ECB, CBC, CFB, OFB, CTR, GCM, Poly1305,
  - blokk-titkosító rendszerek (block ciphers): DES, 3DES (DES-EDE), TEA, AES.
- Üzenet-hitelesítő kódok (message authentication codes):
  - követelmények, biztonság,
  - szerkesztési módok: CMAC, HMAC
- Hash-függvények (hash functions):
  - követelmények, biztonság,
  - szerkesztési módok: Merkle-Damgård, sponge

Törzsanyag

- Nyilvános-kulcsú kriptorendszerek (public-key cryptography, asymmetric cryptography)
  - Titkosító rendszerek (public-key encryption):
    - matematikai modell, biztonság
    - a faktorizációs problémán alapuló titkosító rendszerek: RSA, RSA-OAEP,
    - a kvadratikus maradék problémán alapuló titkosító rendszerek: Rabin, SAEP,
  - Kulcscserék (key exchanges):
    - matematikai modell, biztonság
    - diszkrét logaritmus problémán alapuló rendszerek: Diffie-Hellman (DH) kulcscsere, elliptikus görbéken alapuló kulcscsere (ECDH),
  - Digitális aláírások (digital signatures):
    - matematikai modell, biztonság
    - RSA-PSS, ECDSA, EdDSA
- Protkollok: SSL/TLS, Signal

Szoftverek

- Python
  - PyCryptodome
  - NumPy
  - SymPy
  - Windows alatt a PATH környezetváltozó beállítása után, ha fenn van a gépünkön a pip telepítő, akkor pl. a NumPy telepítése a következőképpen történik: `python -m pip install numpy`
  - pyca/cryptography, egy másik kripto csomag, nem ezzel dolgozunk,
- OpenSSL
- NaCl (Networking and Cryptography library)
- Crypto++,

Könyvészet I

- Freud R., Gyarmati E., Számelmélet, Nemzeti Tankönyvkiadó, Budapest, 2000.
- Cormen T.H., Leiserson C.E., Rivest R.L., Algoritmusok, Műszaki Könyvkiadó, Budapest, 2001.
- Rónyai L. Ivanyos G., Szabó R., Algoritmusok, Typotex, Budapest, 2004
- D. Boneh, V. Shoup, *A Graduate Course in Applied Cryptography*.
  `https://toc.cryptobook.us/`
- Buttyán L., Vajda I.: Kriptográfia és alkalmazásai, Typotex, Budapest, 2004.
- Márton Gy, Kriptográfiai alapismeretek, Scientia Kiadó, Kolozsvár, 2008.
  `https://www.ms.sapientia.ro/~mgyongyi/Crypto/Kriptokonyv.pdf`
- Márton Gy, *Szemelvények a diszkrét matematika fejezeteiből*. Scientia Kiadó, Kolozsvár, 2024.
  `https://www.ms.sapientia.ro/~mgyongyi/DiszkretMat/Jegyzet/DiszkretMatematika.pdf`
- Buchmann J., Introduction to cryptography, Springer, 2002.

Könyvészet II

- Boneh D.: Introduction to Cryptography. Online Cryptography.
  https://www.coursera.org/
- Hoffstein J. , Pipher J., Silverman J.H., An Introduction to Mathematical Cryptograhy, Springer, 2008.
- J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, Boca Raton, Florida, 1997.
  https://cacr.uwaterloo.ca/hac/
- Stallings W., Cryptography and network security. Principles and practice, Pearson, 2011.
- Stamp M., Infromation security. Principles and practice, John Wiley&Sons, 2006.
- Stinson D.R., Cryptography theory and practice, Chapman&HallCRC, 2006.
- D. Wong, *Real-World Cryptography*. Manning, 2021.

Történelmi háttér

- i.e. IV század: spártaiak titkosítása, szkütalé használata (transzpozíció/felcserélés)
- i.e. I. század: Caesar-titkosító (szubsztitúció/helyettesítés)
- Megjegyzés: a mai titkosító rendszerek alapműveletei: transzpozíció és szubsztitúció
- 1926, Vernam titkosító
- 1949, Shannon: tökéletes biztonság (perfect secrecy)
- 1970, DES (Data Encryption Standard): Horst Feistel
- 1976, Diffie-Hellman: publikus-kulcsú kriptográfia alapjai
- 1977, RSA kriptorendszer: Rivest, Shamir, Adleman
- 1985, ElGamal kriptorendszer: Taher ElGamal
- 1994, RSA-OAEP titkosító rendszer, új biztonságértelmezések: Bellare, Rogaway
- 1998, Cramer-Shoup titkosító rendszer (az ElGamal egy kiterjesztett változata)
- 2001, AES (Advanced Encryption Standard): Daemen, Rijmen
- 2004, az ECC széleskörben való elterjedése, az első ajánlás még 1985-ben történt
- 2018, TLS 1.3: az RSA kulcscsere már nem szerepel

Modern kriptográfia

- Alapelvei:
  - pontosan értelmezi a biztonság fogalmát,
  - a számítógépek elterjedésével jelenik meg, tudományos alapokon nyugszik,
  - ha a biztonság valamely feltételtől függ, azt pontosan értelmezi,
  - megadja a rendszerek helyességének, biztonságának a bizonyítását,
  - Kerchoff elv: a titkosító, a hitelesítő algoritmus nyilvános, csak a rendszerben alkalmazott kulcsok titkosak,
  - standardizált rendszerek, nyílt forráskódú kriptográfiai könyvtárcsomagok alkalmazása,
- további feladatai: kulcscsere, kulcsmenedzsment, hitelesítés, azonosítás, titok-megosztás, elektronikus szavazás, stb.
- alapfogalmak: bemeneti ábécé (input alphabet), nyílt szöveg (plaintext), üzenet (message), rejtjelezett szöveg (ciphertext), kulcs (key), titkosítás/rejtjelezés (encryption), visszafejtés (decryption), titkosító algoritmus (cypher).

A biztonság értelmezése

Mikor biztonságos egy titkosító rendszer?

- ha a támadó a titkosított szöveg alapján nem tudja meghatározni a rendszerben alkalmazott kulcsot,
- ha a támadó a titkosított szöveg alapján nem tudja meghatározni a nyílt-szöveget,
- ha a támadó a titkosított szöveg egy kis részének sem tudja meghatározni a megfelelő nyílt szövegrészét,
- ha a támadó a titkosított szöveg alapján nem tud következtetést levonni a nyílt szöveg tartalmára, értelmére, céljára, stb. vonatkozóan.

Kriptorendszerek osztályozása

Hogyan osztályozhatók a támadási típusok, aszerint, hogy mire képes egy támadó?

- passzív támadó
  - rejtjelezett szöveg alapú támadás (ciphertext-only attack): a támadó a rejtjelezett szöveg alapján próbálja meghatározni a nyílt-szöveget,
  - ismert nyílt-szöveg alapú támadás (known-plaintext attack): a támadó nyílt-szöveg és a megfelelő rejtjelezett-szöveg párok alapján próbálja meghatározni egy **más** rejtjelezett szöveghez tartozó nyílt szöveget,
- aktív támadó
  - választott nyílt-szöveg alapú támadás (chosen-plaintext attack): a támadó tetszőleges nyílt-szövegeknek képes meghatározni a rejtjelezett értékét és ezek alapján próbálja meghatározni egy **más** rejtjelezett szöveghez tartozó nyílt-szöveget,
  - választott rejtjelezett-szöveg alapú támadás (chosen ciphertext attack): a támadó képes adott rejelezett szövegeket visszafejteni és ezek alapján az infók alapján próbálja meghatározni egy **más** rejtjelezett szöveghez tartozó nyílt-szöveget,

A Caesar titkosító

- a titkosító azért viseli a Caesar nevet mert a $key = 3$ esetet adó rejtjelezést Julius Caesar római császár használta,
- a klasszikus kriptográfia fizikai úton továbbította a rejtjelezéshez használt kulcsot,
- a kulcsot hosszú ideig változatlanul használták és szigorúan őrizték,
- a Caesar-titkosító nem biztonságos több feltörési módszer is kivitelezhető, abban az esetben is, ha csak a rejtjelezett tartalmat ismeri a támadó:
  - az összes lehetséges kulcs kipróbálása (exhaustive key search): a titkosító összesen 26 különböző kulcsot tud kezelni
  - statisztikai elemzések: betű, betű-pár, betű-hármas, vagy szavak gyakoriság vizsgálatát kell elvégezni.

A Caesar titkosító

Az angol/latin ábécé 26 betűjének megfelelő számkód:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*

- az üzenetek halmaza: $M = C = \{0, 1, \ldots, 25\}^*$,
- a kulcsok halmaza: $K = \mathbb{Z}_{26} = \{0, 1, \ldots, 25\}$,
- kulcsgenerálás *Gen*: kiválasztunk egy $key \in K$ értéket,
- a titkosítási és visszafejtési képletet betünként, a betűk számkódjára alkalmazzuk,
- $Enc_{key}(m) = (m + key) \pmod{26} \rightarrow c$, ahol $m, c \in \mathbb{Z}_{26}$,
- $Dec_{key}(c) = (c + 26 - key) \pmod{26} \rightarrow m$,
- ha $key = 0$ nincs titkosítás, $key = 3$, az eredeti Caesar titkosító,
- a $26 - key$ értéket a *key* additív inverzének hívjuk $\pmod{26}$ szerint,

Példa:

- Ha a nyílt szöveg a következő: *THISISAPLAINTEXT*
- Ha a kulcs 5, akkor a titkosított szöveg: *YMNXNXFUQFNSYJCY*
- A megfelelő titkosító tábla:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
F	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*

Helyettesítő rejtjelezés

- $M = C = \{0, 1, \ldots, 25\}^*$
- K elemei: a 26 szimbólum összes permutációjának halmaza,
- *key* egy lehetséges permutáció,
- *Gen*: kiválasztunk egy permutációt,
- $Enc_{key}(m) = Perm(m) \rightarrow c$,
- $Dec_{key}(c) = Perm^{-1}(c) \rightarrow m$.

Példa, Keyword Caesar titkosító, ahol a kulcs két értékből tevődik össze:

- Ha a nyílt szöveg a következő: *THISISAPLAINTEXT*
- Ha a kulcs 7, *PASWD*, akkor a titkosított szöveg: *PLMZMZEVQEMTPIDP*
- A megfelelő titkosító tábla, ahol vegyük észre, hogy $26 - 19 = 7$:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
E	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*Q*	*R*	*T*	*U*	*V*	*X*	*Y*	*Z*	*P*	*A*	*S*	*W*	*D*	*B*	*C*

Feltörési módszerek:

- az összes lehetséges kulcs kipróbálása nem működik, mert a lehetséges kulcsok száma: 26! = 403291461126605635584000000
- működik: statisztikai elemzések alkalmazása.

Az Affine titkosító

- helyettesítő, monoalfabetikus rejtjelező,
- $M = C = \{0, 1, \ldots, 25\}^*, K = \{(a, b) \in \mathbb{Z}_{26}, gcd(a, 26) = 1\}$,
- $key = (a, b)$
- $Enc_{(a,b)}(m) = (a \cdot m + b) \pmod{26} \rightarrow c$, ahol $m, c \in \mathbb{Z}_{26}$,
- $Dec_{(a,b)}(c) = a^{-1} \cdot (c + 26 - b) \pmod{26}$.
- a^{-1}, az a multiplikatív inverze $\pmod{26}$ szerint, ami azt jelenti, hogy meg kell határozni azt az a^{-1} értéket, amelyre fennáll:

$$a \cdot a^{-1} = 1 \pmod{26}.$$

- a multiplikatív inverz akkor létezik, ha $gcd(a, 26) = 1$, ahol gcd - greatest common division/legnagyobb közös osztó
- Ha létezik multiplikatív inverz, akkor az meghatározható:
  - az összes érték kipróbálásával: 12 szorzás szükséges,
  - a kiterjesztett Eukleidészi algoritmussal,
  - az Euler tételt alkalmazva: $a^{-1} = a^{\phi(26)-1} = a^{11} \pmod{26}$, mert $\phi(26) = \phi(2) \cdot \phi(13) = 12$,
  - Pythonban: `pow(a, -1, 26)`

Az Affine titkosító - példa

- Ha a kulcs $(5, 2)$ és a nyílt-szöveg a következő:

$$AMATHEMATICIAN,$$

- akkor a titkosított-szöveg:

$$CKCTLWKCTQMQCP,$$

- ahol a titkosított-szöveg első 6 karakterét a következőképpen határoztuk meg:

$$\begin{array}{lllllll}
A & -> & C: & (5 \cdot 0 + 2) & = & 2 & \pmod{26} \\
M & -> & K: & (5 \cdot 12 + 2) & = & 10 & \pmod{26} \\
A & -> & C: & (5 \cdot 0 + 2) & = & 2 & \pmod{26} \\
T & -> & T: & (5 \cdot 19 + 2) & = & 19 & \pmod{26} \\
H & -> & L: & (5 \cdot 7 + 2) & = & 11 & \pmod{26} \\
E & -> & W: & (5 \cdot 4 + 2) & = & 22 & \pmod{26}
\end{array}$$

- A visszafejtéshez szükséges kulcs: $(21, 2)$, mert $5 \cdot 21 = 105 = 1 \pmod{26}$, azaz, 5 multiplikatív inverze $\pmod{26}$ szerint 21.