

Kriptográfia és Információbiztonság

1. előadás

MÁRTON Gyöngyvér

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

2024

Követelmények, osztályozás

- vizsgajegy = (dolgozatjegy + laborjegy) / 2
- dolgozatjegy:
 - legalább 4, de nem több mint 6 oldalas dolgozat bemutatására adott jegy (A4 lapméret, 11-es font, 1.5 sorköz),
 - tartalma tudományos jellegű kell legyen, kapcsolódnia kell a 21. századi adatbiztonsághoz,
 - kötelező a megfelelő hivatkozások elhelyezése,
 - bemutatáskor szabadon kell beszélni, tilos olvasni
 - határidőre kell beküldeni, és 10-15 percben kell bemutatni,
 - beküldési határidő: 9. oktatási hét vége
 - bemutatási időpontok, megegyezés szerint az utolsó oktatási héten, illetve a vizsgaidőszakban.

Követelmények, osztályozás

- **laborjegy:** három feladat bemutatására kapott jegy
 - az első feladatot az első három laborsorból kell kiválasztani, és az első két hét valamelyik laboróráján kell bemutatni.
 - a második feladatot a 4, 5, 6 laborsorból kell kiválasztani, és 3., 4., 5. hét valamelyik laboróráján kell bemutatni.
 - a harmadik feladatot a 7, 8, 9, 10 laborsorból kell kiválasztani, és 6., 7., 8. hét valamelyik laboróráján kell bemutatni.
- akiknél a vizsgajegy átmenő, azoknál plusz pontokat is figyelembe fogok venni,
- **egy jegynek megfelelő plusz pont:** akkor szereshető, ha előadáson feltett három kérdésre helyes válaszoltunk.

Követelmények, osztályozás

pótvizsgák:

- $\text{vizsgajegy} = (\text{szóbelijegy} + \text{laborjegy}) / 2$
- szóbelijegy: egy tételsor megválaszolására kapott jegy. Egy tételsor három, a törzsanyagból vett kérdést fog tartalmazni, amelyet a diák szóban kell kifejtсен.
- laborjegy: ha az oktatási időszakban ezt a diák nem teljesítette, akkor 3 feladatot kell bemutatni, egyet az első három laborsorból kell kiválasztani, egyet a 4, 5, 6 laborsorból, és a harmadikat a 7, 8, 9, 10 laborsorból.

Kriptográfia és információbiztonság

- 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 (Encrypting File System) titkosítása, régebbi verziókban DESX, az újabbakban AES, SHA, ECC
- A Blu-ray, DVD, CD tartalmak biztonsága: AACS (Advanced Access Control System) másolásvédelmi technológia, a lemezen és a készüléken titkosító kulcsok vannak beállítva, amelyeket a lejáratí idő után meg kell újítani
- ...










Kriptográfia, törzsanyag

- Klasszikus kriptográfiai rendszerek (Caesar és változatai, Affin, Hill)
- Titkos-kulcsú titkosító rendszerek (secret-key encryption systems, symmetric encryption systems)
 - matematikai modell, biztonság, tervezés
 - folyam-titkosító rendszerek (stream ciphers): OTP, RC4, LFSR, A5/1, Salsa20,
 - 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): HMAC, CMAC,
- Hash-függvények (hash functions): követelmények, biztonság, tervezés, az SHA függvénycsalád

Kriptográfia, törzsanyag

- Nyilvános-kulcsú kriptorendszerek (public-key cryptography, asymmetric cryptography)
 - Titkosító rendszerek (public-key encryption systems):
 - 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

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
-  Buttyán L., Vajda I.: Kriptográfia és alkalmazásai, Typotex, Budapest, 2004.
-  Márton Gy, Kriptográfiai alapismeretek, Scientia Kiadó, Kolozsvár, 2008.
-  Buchmann J., Introduction to cryptography, Springer, 2002.
-  Boneh D.: Introduction to Cryptography. Online Cryptography.
<https://www.coursera.org/>
-  Hoffstein J. , Pipher J., Silverman J.H., An Introduction to Mathematical Cryptography, Springer, 2008.
-  Menezes J., van Oorschot P.C., Vanstone S.A., Handbook of Applied Cryptography, CRC Press, Boca Raton, Florida, 1997.

Könyvészet II



Stallings W., Cryptography and network security. Principles and practice, Pearson, 2011.



Stamp M., Information security. Principles and practice, John Wiley&Sons, 2006.



Stinson D.R., Cryptography theory and practice, Chapman&HallCRC, 2006.

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 alapl műveletei: 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

Bevezető

- Klasszikus kriptográfia:
 - alkalmazásuk: diplomáciai-katonai életben, csak titkosítást végeztek,
 - könnyen feltörhetőek statisztikai számítások segítségével.
- Modern kriptográfia: a számítógépek elterjedésével jelenik meg, tudományos alapokon nyugszik, fő alapelvei:
 - pontosan kell értelmezni a biztonság fogalmát,
 - ha a biztonság valamely feltételtől függ, azt pontosan kell értelmezni,
 - a rendszerek helyességének, biztonságának meg kell adni a bizonyítását.
- A modern adatbiztonság további feladatai: kulcscsere, kulcsmenedzsment, hitelesítés, azonosítás, titok-megosztás, elektronikus szavazás, stb.
- Alapfogalmak: bemeneti ábécé (input alphabet), nyílt-szöveg (plaintext), rejtjelezett-szöveg (ciphertext), kulcs (key), titkosítás/rejtjelezés (encryption), visszafejtés (decryption),
- Kerchoff elv: a titkosító, a hitelesítő algoritmus nyilvános, csak a rendszerben alkalmazott kulcsok titkosak.
- Alapelv: standardizált rendszerek, nyílt forráskódú kriptográfiai könyvtár csomagok alkalmazása.

Biztonság-értelmezés

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 alapján egy tetszőlegesen kicsi részét sem tudja meghatározni a nyílt-szövegnek,
- 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 rejtjelezett szövegeket visszafejteni és ezek alapján az infók alapján próbálja meghatározni egy **más** rejtjelezett szöveghez tartozó nyílt-szöveget,