Miskolci Egyetem
Gépészmérnöki és Informatikai Kar
Informatikai Intézet
Általános Informatikai Intézeti Tanszék

Neptunkód: ***GEIAL506M***

Javasolt félév: 4
Kredit: 5

Kontakt órák száma / hét: 2 előadás, 2 labor gyakorlat / 8 előadás, 8 gyakorlat

Informatikai rendszerek védeleme

Szak: *Mérnökinformatikus mesterszak*

Hét	Előadás	Gyakorlat
1.	Elméleti bevezetés, követelményrendszer ismertetése; Adat és információ fogalmi kérdései;	Blokk titkosítási algoritmusok
2.	Információ biztonság társadalmi és általános kérdései	Weboldali aozonosítások
3.	Információ játékelméleti modellezése	Kripto-vírusok
4.	Redundancia és tömörítés; Bináris kódolás	Az AVI szerkezete
5.	Jogosulatlan hozzáférés és behatolások	Matematikai problémák I.
6.	Nevezetes biztonsági esetek	Matematikai problémák II.
7.	Kriptográfia és hibajavító kódok; kételemű és más véges számrendszerek	Kriptográfiai algoritmusok
8.	Kriptográfia egyszerű számtani algoritmusai	Fizetési protokollok
9.	Kriptográfiában használatos alapvető függvények	Protokollok II.
10.	Kriptográfia	PGP használata
11.	Elektronikus és digitális aláírás	Mp3 szerkezete
12.	Algoritmusok bonyolultsága és információ biztonság	Nagy számok aritmetikája
13.	Összefoglalás	Realtime multimédia továbbítás IP hálózaton
14	Választott téma előadása	Választott téma előadása, számonkérés a gyakorlati foglalkozások elméletéből

A kurzus aláírással és kollokviummal zárul

Az aláírás feltétele:

- Legalább 10 gyakorlaton való részvétel;
- legalább 10 elfogadható szintű órai feladat beadás.
- A választott téma előadása, anyagainak leadása;
- a számonkérés legalább elégséges szintű teljesítése;

Az aláíráspótlás idejében pótolható: a leadott, de nem elfogadható szintű órai feladat, illetve a nem elégséges szintű számonkérés. Nem leadott feladatot nem lehet javítani.

Kollokviumjegy meghatározása: (vizsga + gyakorlati foglalkozás) /2

A számítás módja részletesen:

1. Gyakorlati foglalkozás: 70% az utolsó gyakorlaton megírt számonkérés eredménye
   30% a választott feladat kidolgozásának eredménye.
2. Előadás: A vizsgaidőszakban az írásbeli (szükség szerint szóbeli) vizsga eredménye

Mind a gyakorlati foglalkozás, mind az előadás részének minimum elégségesnek kell lennie.
Az értékelés:

0% - 50%: elégtelen
51% - 62%: elégséges
63% - 75%: közepes
76% - 88%: jó
89% - 100%: jeles

Elégtelen írásbeli elégtelen vizsgajegyet jelent. A szóbelin a megjelenés kötelező.

A HKR 50. § (5) bekezdése értelmében, előadások esetén 40%-ot, gyakorlatok esetén 30%-ot meghaladó igazolatlan hiányzás esetén a tanszék kezdeményezi az aláírás végleges megtagadását. A végleges aláírás megtagadás bejegyzése után a hallgató a mulasztását nem pótolhatja, ismételten fel kell vennie és le kell hallgatnia a tantárgyat ahhoz, hogy az aláírást megszerezze.

Kötelező irodalom:

- Almási János: Elektronikus aláírás és társai
- John R. Vacca: Computer and Information Security Handbook
- Bruce Schneier: Applied Cryptography
- Virrasztó Tamás: Titkosítás és adatrejtés
- Simon Singh: Kódkönyv
- Alan G. Konheim: Computer Security and Cryptography
- J. H. Allen, S. Barnum, R. J. Ellison, G. McGraw, N. R. Mead: Software Security Engineering

Informatikai rendszerek védelme
Vizsgazárthelyi mintafeladat

1. Adja meg a következő fogalmak meghatározását: kriptográfia, kriptoanalízis! (2 p)
2. Rajzolja le a nyilvános kommunikációs csatornára épülő, a titkosítást, megfejtést, és a lehetséges támadási formákat is tartalmazó ábrát! (2 p)
3. Magyarázza meg a következőket: (5p)
    - passzív behatoló:
    - aktív behatoló:
    - CIA elv komponensei:
4. Mikor nevezünk egy algoritmust feltétel nélkül biztonságosnak? (2p)
5. Kriptográfiai protokollok leírásában a következő személyek használatosak: Alice, Bob, Carol, Dave, Eve, Mallory, Trent, Walter, Peggy, Victor. Legalább 7 esetében adja meg szokásos szerepüket! (4 p)
6. Ismertesse a döntőbírós protokollt! (5 p)
7. Sorolja fel, rövid magyarázattal egészítse ki a digitális aláírással szembeni elvárásokat! (4 p)

Kidolgozási idő: 60 perc

Max: 24 pont 0-12: elégtelen; 13-15: elégséges; 16-18:közepes; 19-21: jó; 22-24: jeles

Informatikai rendszerek védelme
Vizsgazárthelyi mintafeladat megoldás

1. Adja meg a következő fogalmak meghatározását: kriptográfia, kriptoanalízis! (2 p)
   Kriptográfia: az információvédelem algoritmikus oldala. Azoknak a matematikai eljárásoknak, algoritmusoknak, biztonsági rendszabályoknak a kutatását jelenti, amelyek elsődleges célja az információnak illetéktelenek előli elrejtése.
   Kriptoanalízis: kódolt szövegeknek kulcs nélküli megfejtése

2. Rajzolja le a nyilvános kommunikációs csatornára épülő, a titkosítást, megfejtést, és a lehetséges támadási formákat is tartalmazó ábrát! (2 p)

3. Magyarázza meg a következőket: (5p)
   - *passzív betolakodó: a behatoló a behatolás után nem változtat meg semmit a rendszerben, sem az ott található dokumentumokon. Emiatt nehezebb detektálni, akár hosszú időn keresztül is szivárogtathat ki információkat.*
   - *aktív betolakodó: a behatoló a behatolás után módosításokat hajt végre a rendszeren, és/vagy az ott tárol dokumentumokon*
   - *CIA:*
     - *C: (Confidentiality: bizalmasság): az információhoz csak az férhessen hozzá, akinek engedélye van.*
     - *I: (Integrity: sértetlenség): cél az információ sértetlenségének megőrzése. Ehhez érzékelni kell tudni a sérülést.*
     - *A: (Availability: rendelkezésre állás): az információ a szükséges helyen és időben legyen hozzáférhető*

4. Mikor nevezünk egy algoritmust feltétel nélkül biztonságosnak? (2p)
   Egy biztonsági algoritmus akkor feltétel nélkül biztonságos, ha a támadó tetszőleges számítási kapacitás (erőforrás) mellett sem képes feltörni azt.

5. Kriptográfiai protokollok leírásában a következő személyek használatosak: Alice, Bob, Carol, Dave, Eve, Mallory, Trent, Walter, Peggy, Victor. Legalább 7 esetében adja meg szokásos szerepüket! (4 p)
   Alice: a feladó
   Bob: a címzett
   Carol, Dave: további kommunikáló felek
   Eve: passzív támadó
   Mallory: aktív támadó
   Trent: választott döntőbíró, abszolút megbízható
   Walter: felügyelő
   Peggy: bizonyító (egy vagy több állítás teljesülését bizonyítja)
   Victor: ellenőrző, aki ellenőrzi Peggy bizonyító eljárását

6. Ismertesse a döntőbírós protokollt! (5 p)
   A döntőbírós protokoll esetében a kommunikáló felek egy megbízható döntőbíróval egészülnek ki. A döntőbíró a két kommunikáló fél között helyezkedik el. Emiatt a

protokoll lassabb lesz, mint nélküle. Szerepétől függően lehet időigényesebb, mint a protokoll többi szereplője, vagyis szűk keresztmetszetet okozhat.
Digitális aláírás esetén ellenőrzi az aláírást, majd időpecséttel látja el, és küldi tovább a címzettnek. Szerepe miatt általában hozzá kell tudnia férnie az üzenet titkosítatlan változatához.

7. Sorolja fel, rövid magyarázattal egészítse ki a digitális aláírással szembeni elvárásokat! (4 p)
   - *Hiteles: az aláíró saját akaratából írta alá*
   - *Hamisíthatatlan: az aláírás az aláírótól és nem mástól származik*
   - *Nemhasználható fel újra, nem vihető át másik dokumentumra*
   - *az aláírt dokumentum megváltoztathatatlan, vagy változtatás esetén a változtatás érzékelhető*
   - *Nem tagadható le: az aláíró nem állíthatja később, hogy az aláírás nem tőle származik*

Kidolgozási idő: 60 perc

Max: 24 pont 0-12: elégtelen; 13-15: elégséges; 16-18:közepes; 19-21: jó; 22-24: jeles