

E5) Az alábbiak közül melyik írja le a „beágyazott aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe
- b) az aláírásba ágyazódnak bele az aláírandó információk
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele

1 pont

E6) Az alábbiak közül melyik írja le a „különálló aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe, és együtt mozog vele
- b) az aláírásba ágyazódnak bele az aláírandó információk
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve

1 pont

E7) Meddig érvényes egy tanúsítvány?

- a) amíg vissza nem vonják
- b) amíg fel nem függesztik
- c) a lejáratí időpontig
- d) a kezdeti időpontig

1 pont

E8) Melyik tanúsítvány hibás?

- a) amelyik nem tartalmazza a tanúsítvány birtokosának nevét, csak egy álnevet
- b) amelyet nem minősített hitelesítésszolgáltató adta ki
- c) amelyik más című webszerverre van kiállítva, mint amelyen található
- d) amelyikkel nem lehet aláírni, csak titkosítani

1 pont

E9) Mi az a tanúsítási lánc?

- a) a hitelesítésszolgáltató Nemzeti Hírközlési Hatóság általi minősítése
- b) a szoftvereken szereplő aláírások
- c) a tanúsítványtárban szereplő gyökértanúsítványok
- d) a tanúsítványkibocsátók felülről lefelé építkező aláírásai

1 pont

E10) Mi az elektronikus aláírás definíciója az eIDAS szerint?

- a) minden olyan adat, amelyet az aláíró aláírásra használ
- b) hitelesítés céljából elektronikus adathoz csatolt vagy az elektronikus adattal logikailag összerendelt elektronikus adat
- c) a digitális aláírás és az üzenethitelesítő kód együttesen
- d) aszimmetrikus kriptográfiai eszközöket alkalmazó hitelesítési eljárás, mely az elektronikus adattal logikailag elektronikus adatot rendel össze

1 pont

B – Gyakorlati feladatok**Instrukciók:**

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájlal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

- | | | |
|-------|--|--------|
| GY1) | Nyissa meg az ALMA fájlt! Írja le az aláíráshoz használt tanúsítványnak a sorozatszámát! | 2 pont |
| GY2) | Nyissa meg a BIRSALMA fájlt! Mi az aláírás készítőjének a neve (CN)? | 2 pont |
| GY3) | Nyissa meg a BANAN fájlt! Van-e hiteles aláírás a fájlban? | 2 pont |
| GY4) | Nyissa meg az ANANASZ dossziét! Mennyi időbélyeg van a teljes dosszién? | 2 pont |
| GY5) | Nyissa meg a DINNYE dossziét! Hány aláírás van a dossziében? | 2 pont |
| GY6) | Nyissa meg a https://www.magyarorszag.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő SHA1-ujjlenyomat? | 2 pont |
| GY7) | Nyissa meg a https://www.magyarorszag.hu honlapot! Írja le az oldal SSL-tanúsítványának sorozatszámát? | 2 pont |
| GY8) | Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítvány érvényességi idejének kezdete? | 2 pont |
| GY9) | Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítványnak a neve (CN)? | 2 pont |
| GY10) | Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) KEAASZ segítségével! | 2 pont |
| GY11) | Írja alá a az ALMA fájlt a(z) KEAASZ segítségével! | 2 pont |

E5) Hol van a tanúsítvány visszavonási lista feltalálási helye?

- a) a minősített aláírásban
- b) az időbélyegben 1 pont
- c) a fokozott biztonságú aláírásban
- d) a tanúsítványban

E6) Ki írja alá a felhasználói tanúsítványt?

- a) a felhasználó a saját titkos kulcsával
- b) a hitelesítésszolgáltató a saját titkos kulcsával 1 pont
- c) a hitelesítésszolgáltató a nyilvános kulcsával
- d) a tanúsítványok önaláírtak

E7) Ki töltheti le a tanúsítványokat a bizalmi szolgáltatótól?

- a) csak a tulajdonosuk
- b) a tulajdonos munkáltatója 1 pont
- c) bárki
- d) csak állami hatóságok

E8) Meddig érvényes egy tanúsítvány?

- a) amíg vissza nem vonják
- b) amíg fel nem függesztik 1 pont
- c) a lejáratási időpontig
- d) a kezdeti időpontig

E9) Melyik tanúsítvány hibás?

- a) amelyik nem tartalmazza a tanúsítvány birtokosának nevét, csak egy álnevet 1 pont
- b) amelyiket nem minősített hitelesítésszolgáltató adta ki
- c) amelyik más című webszerverre van kiállítva, mint amelyen található
- d) amelyikkel nem lehet aláírni, csak titkosítani

E10) Mi az a tanúsítási lánc?

- a) a hitelesítésszolgáltató Nemzeti Hírközlési Hatóság általi minősítése
- b) a szoftvereken szereplő aláírások 1 pont
- c) a tanúsítványtárban szereplő gyökértanúsítványok
- d) a tanúsítványkibocsátók felülről lefelé építkező aláírásai

B – Gyakorlati feladatok

Instrukciók:

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájlal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

- | | | |
|-------|--|--------|
| GY1) | Nyissa meg a DATOLYA fájlt! Írja le az aláíráshoz használt tanúsítványnak a kiállítóját (CN)! | 2 pont |
| GY2) | Nyissa meg a GESZTENYE fájlt! Mi az aláírás készítőjének a neve (CN)? | 2 pont |
| GY3) | Nyissa meg az EPER fájlt! Van-e hiteles aláírás a fájlban? | 2 pont |
| GY4) | Nyissa meg a DINNYE dossziét! Mennyi időbélyeg van a dossziében? | 2 pont |
| GY5) | Nyissa meg az ANANASZ dossziét! Hány aláírás van a teljes dosszién? | 2 pont |
| GY6) | Nyissa meg a https://www.njszt.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő sorozatszám? | 2 pont |
| GY7) | Nyissa meg a https://www.njszt.hu honlapot! Írja le az oldal SSL-tanúsítványának kiállítóját (CN)? | 2 pont |
| GY8) | Nyissa meg a https://www.magyarorszag.hu honlapot! Mi az SSL-tanúsítvány érvényességi idejének vége? | 2 pont |
| GY9) | Nyissa meg a https://www.magyarorszag.hu honlapot! Mi az SSL-tanúsítványnak a neve (CN)? | 2 pont |
| GY10) | Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) KEAASZ segítségével! | 2 pont |
| GY11) | Írja alá a DATOLYA fájlt a(z) KEAASZ segítségével! | 2 pont |

E5) Az alábbiak közül melyik írja le a „beágyazott aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe
- b) az aláírásba ágyazódnak bele az aláírandó információk
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele

1 pont

E6) Az alábbiak közül melyik írja le a „különálló aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe, és együtt mozog vele
- b) az aláírásba ágyazódnak bele az aláírandó információk
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve

1 pont

E7) Az alábbiak közül melyik írja le az „ellenjegyző aláírás” fogalmát?

- a) az aláírások egymás után, mintegy egymásba becsomagolódva helyezkednek el, és ellenőrzésüknél is csak kívülről befelé lehet haladni
- b) a meglévők felett álló, azoktól függő módon azokra ráakódó aláírás
- c) a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól
- d) a dokumentumtól teljesen külön van kezelve, de együtt mozog vele

1 pont

E8) Az üzenethitelesítő kód biztosítja

- a) a módosítások felderíthetőségét
- b) a tartalom megváltoztathatatlanágát
- c) az eredeti tartalom visszaállíthatóságát
- d) a kód személyhez köthetőségét

1 pont

E9) Meddig érvényes egy tanúsítvány?

- a) amíg vissza nem vonják
- b) amíg fel nem függesztik
- c) a lejáratú időpontig
- d) a kezdeti időpontig

1 pont

E10) Melyik tanúsítvány hibás?

- a) amelyik nem tartalmazza a tanúsítvány birtokosának nevét, csak egy álnevet
- b) amelyiket nem minősített hitelesítésszolgáltató adta ki
- c) amelyik más című webszerverre van kiállítva, mint amelyen található
- d) amelyikkel nem lehet aláírni, csak titkosítani

1 pont

B – Gyakorlati feladatok**Instrukciók:**

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájlal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

GY1)	Nyissa meg a MAZSOLA fájlt! Írja le az aláíráshoz használt tanúsítványnak a érvényességi idejének végét!	2 pont
GY2)	Nyissa meg a MAZSOLA fájlt! Mi az aláírás készítőjének a városa (L)?	2 pont
GY3)	Nyissa meg a BANAN fájlt! Van-e hiteles időbélyeg a fájlban?	2 pont
GY4)	Nyissa meg a DINNYE dossziét! Mennyi aláírás van a dossziében?	2 pont
GY5)	Nyissa meg a SZEDER dossziét! Hány időbélyeg van a teljes dosszién?	2 pont
GY6)	Nyissa meg a https://www.magyarorszag.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő SHA1-ujjlenyomat?	2 pont
GY7)	Nyissa meg a https://www.magyarorszag.hu honlapot! Írja le az oldal SSL-tanúsítványának érvényességi idejének végét?	2 pont
GY8)	Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítvány kiállítójának neve (CN)?	2 pont
GY9)	Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítványnak a városa (L)?	2 pont
GY10)	Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) KEAASZ segítségével!	2 pont
GY11)	Írja alá a MAZSOLA fájlt a(z) KEAASZ segítségével!	2 pont

E5) Az üzenethitelesítő kód biztosítja

- a) a módosítások felderíthetőségét
- b) a tartalom megváltoztathatatlanságát
- c) az eredeti tartalom visszaállíthatóságát
- d) a kód személyhez köthetőségét

1 pont

E6) Ki írja alá a felhasználói tanúsítványt?

- a) a felhasználó a saját titkos kulcsával
- b) a hitelesítésszolgáltató a saját titkos kulcsával
- c) a hitelesítésszolgáltató a nyilvános kulcsával
- d) a tanúsítványok önaláírtak

1 pont

E7) Meddig érvényes egy tanúsítvány?

- a) amíg vissza nem vonják
- b) amíg fel nem függesztik
- c) a lejáratidőpontig
- d) a kezdeti időpontig

1 pont

E8) Melyik tanúsítvány hibás?

- a) amelyik nem tartalmazza a tanúsítvány birtokosának nevét, csak egy álnevet
- b) amelyet nem minősített hitelesítésszolgáltató adta ki
- c) amelyik más című webszerverre van kiállítva, mint amelyen található
- d) amelyikkel nem lehet aláírni, csak titkosítani

1 pont

E9) Mi az a tanúsítási lánc?

- a) a hitelesítésszolgáltató Nemzeti Hírközlési Hatóság általi minősítése
- b) a szoftvereken szereplő aláírások
- c) a tanúsítványtárban szereplő gyökértanúsítványok
- d) a tanúsítványkibocsátók felülről lefelé építkező aláírásai

1 pont

E10) Mi az elektronikus aláírás definíciója az eIDAS szerint?

- a) minden olyan adat, amelyet az aláíró aláírásra használ
- b) hitelesítés céljából elektronikus adathoz csatolt vagy az elektronikus adattal logikailag összerendelt elektronikus adat
- c) a digitális aláírás és az üzenethitelesítő kód együttesen
- d) aszimmetrikus kriptográfiai eszközt alkalmazó hitelesítési eljárás, mely az elektronikus adattal logikailag elektronikus adatot rendel össze

1 pont

B – Gyakorlati feladatok

Instrukciók:

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájllal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

- | | | |
|-------|---|--------|
| GY1) | Nyissa meg a SARGABARACK fájlt! Írja le az aláíráshoz használt tanúsítványnak a érvényességi idejének kezdetét! | 2 pont |
| GY2) | Nyissa meg a MAZSOLA fájlt! Mi az aláírás készítőjének a neve (CN)? | 2 pont |
| GY3) | Nyissa meg az EPER fájlt! Van-e ellenjegyző aláírás a fájlban? | 2 pont |
| GY4) | Nyissa meg a MALNA dossziét! Mennyi aláírás van a teljes dosszién? | 2 pont |
| GY5) | Nyissa meg a SZEDER dossziét! Hány időbélyeg van a dossziében? | 2 pont |
| GY6) | Nyissa meg a https://www.njszt.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő aláíró algoritmus? | 2 pont |
| GY7) | Nyissa meg a https://www.njszt.hu honlapot! Írja le az oldal SSL-tanúsítványának érvényességi idejének kezdetét? | 2 pont |
| GY8) | Nyissa meg a https://www.magyarorszag.hu honlapot! Mi az SSL-tanúsítvány aláíró algoritmus? | 2 pont |
| GY9) | Nyissa meg a https://www.magyarorszag.hu honlapot! Mi az SSL-tanúsítványnak a neve (CN)? | 2 pont |
| GY10) | Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) KEAASZ segítségével! | 2 pont |
| GY11) | Írja alá a SARGABARACK fájlt a(z) KEAASZ segítségével! | 2 pont |

E4) Az alábbiak közül melyik írja le a „különálló aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe, és együtt mozog vele
- b) az aláírásba ágyazódnak bele az aláírandó információk 1 pont
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve

E5) Az üzenethitelesítő kód biztosítja

- a) a módosítások felderíthetőségét
- b) a tartalom megváltoztathatatlanságát 1 pont
- c) az eredeti tartalom visszaállíthatóságát
- d) a kód személyhez köthetőségét

E6) Hol van a tanúsítvány visszavonási lista feltalálási helye?

- a) a minősített aláírásban
- b) az időbélyegben 1 pont
- c) a fokozott biztonságú aláírásban
- d) a tanúsítványban

E7) Ki írja alá a felhasználói tanúsítványt?

- a) a felhasználó a saját titkos kulcsával
- b) a hitelesítésszolgáltató a saját titkos kulcsával 1 pont
- c) a hitelesítésszolgáltató a nyilvános kulcsával
- d) a tanúsítványok önaláírtak

E8) Ki töltheti le a tanúsítványokat a bizalmi szolgáltatótól?

- a) csak a tulajdonosuk
- b) a tulajdonos munkáltatója 1 pont
- c) bárki
- d) csak állami hatóságok

E9) Meddig érvényes egy tanúsítvány?

- a) amíg vissza nem vonják
- b) amíg fel nem függesztik 1 pont
- c) a lejáratási időpontig
- d) a kezdeti időpontig

E10) Melyik tanúsítvány hibás?

- a) amelyik nem tartalmazza a tanúsítvány birtokosának nevét, csak egy álnevet
- b) amelyet nem minősített hitelesítésszolgáltató adta ki
- c) amelyik más című webszerverre van kiállítva, mint amelyen található
- d) amelyikkel nem lehet aláírni, csak titkosítani

1 pont

B – Gyakorlati feladatok

Instrukciók:

A Vizsgázónak több, a **VIZSGAJEL** könyvtárban előre elkészített fájlal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

GY1)	Nyissa meg az ALMA fájlt! Írja le az aláíráshoz használt tanúsítványnak a sorozatszámát!	2 pont
GY2)	Nyissa meg az ALMA fájlt! Mi az aláírás készítőjének a neve (CN)?	2 pont
GY3)	Nyissa meg a MEGGY fájlt! Van-e hiteles aláírás a fájlban?	2 pont
GY4)	Nyissa meg a DINNYE dossziét! Mennyi időbélyeg van a teljes dosszién?	2 pont
GY5)	Nyissa meg az ANANASZ dossziét! Hány aláírás van a dossziében?	2 pont
GY6)	Nyissa meg a https://www.magyarország.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő SHA1-ujjlenyomat?	2 pont
GY7)	Nyissa meg a https://www.magyarország.hu honlapot! Írja le az oldal SSL-tanúsítványának sorozatszámát?	2 pont
GY8)	Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítvány érvényességi idejének kezdete?	2 pont
GY9)	Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítványnak a neve (CN)?	2 pont
GY10)	Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) KEAASZ segítségével!	2 pont
GY11)	Írja alá a az ALMA fájlt a(z) KEAASZ segítségével!	2 pont

<p>A VIZSGÁZTATÓ TÖLTI KI!</p> <p>ADATOK:</p> <p>VIZSGA DÁTUMA: ÉV HÓ NAP</p> <p>VIZSGAKÖZPONT AZONOSÍTÓJA:</p> <p>VIZSGÁZTATÓ NEVE:</p>	<p>A VIZSGÁZTATÓ TÖLTI KI!</p> <p>ÉRTÉKELÉS:</p> <p>ÖSSZPONTSZÁM: / MAX.: 32 PONT</p> <p style="text-align: center;">MEGFELELT / NEM FELELT MEG</p> <p>VIZSGÁZTATÓ ALÁÍRÁSA:</p>
	<p>VIZSGÁZÓ NEVE:</p>

06. FELADATSOR

A – Elméleti kérdések

Instrukciók:

Nyissa meg a **VIZSGA** fájlt és írja be válaszainak a betűjeleit a fájlban lévő táblázat E1)-E10) soraiba. Mentse el a kitöltött táblázatot ugyanezen a néven!

E1) A digitális aláírás sikeres ellenőrzéséből mely állítás nem következik?

- a) az aláírt adatok ugyanazok, amit a küldő elküldött
- b) az aláírást biztonságos aláíráslétrehozó eszközzel végezték
- c) az aláírást a nyilvános kulcshoz tartozó titkos kulccsal végezték
- d) megfelelő tanúsítvánnyal az a fizikai személy is ismert, aki aláírta az adatokat

1 pont

E2) A digitális aláírás ellenőrzésének sikertelenségéből melyik állítás következhet?

- a) az adatok a küldés során nem változtak meg
- b) a tanúsítvány lejárt
- c) az ellenőrzéskor ugyanazt a kulcsot és algoritmust használták
- d) a nyilvános kulcshoz tartozó tanúsítványt a fogadó megbízhatóvá tette

1 pont

E3) A digitális aláírás során

- a) az aláíró a titkos kulcs birtokosa, a fogadó a nyilvános kulcsot használja
- b) a fogadó a titkos kulcs birtokosa, az aláíró a nyilvános kulcsot használja
- c) a fogadó titkosít a titkos kulccsal, az aláíró megoldja azt a nyilvános kulccsal
- d) a titkos üzenetet csak az adott felhasználó képes elolvasni

1 pont

E4) Az alábbiak közül melyik írja le a „különálló aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe, és együtt mozog vele
- b) az aláírásba ágyazódnak bele az aláírandó információk 1 pont
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve

E5) Az alábbiak közül melyik írja le az „ellenjegyző aláírás” fogalmát?

- a) az aláírások egymás után, mintegy egymásba becsomagolódva helyezkednek el, és ellenőrzésüknél is csak kívülről befelé lehet haladni
- b) a meglévők felett álló, azoktól függő módon azokra ráakódó aláírás 1 pont
- c) a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól
- d) a dokumentumtól teljesen külön van kezelve, de együtt mozog vele

E6) Az üzenethitelesítő kód biztosítja

- a) a módosítások felderíthetőségét
- b) a tartalom megváltoztathatatlanágát 1 pont
- c) az eredeti tartalom visszaállíthatóságát
- d) a kód személyhez köthetőségét

E7) Hol van a tanúsítvány visszavonási lista feltalálási helye?

- a) a minősített aláírásban
- b) az időbélyegben 1 pont
- c) a fokozott biztonságú aláírásban
- d) a tanúsítványban

E8) Ki töltheti le a tanúsítványokat a bizalmi szolgáltatótól?

- a) csak a tulajdonosuk
- b) a tulajdonos munkáltatója 1 pont
- c) bárki
- d) csak állami hatóságok

E9) Melyik tanúsítvány hibás?

- a) amelyik nem tartalmazza a tanúsítvány birtokosának nevét, csak egy álnevet
- b) amelyiket nem minősített hitelesítésszolgáltató adta ki 1 pont
- c) amelyik más című webszerverre van kiállítva, mint amelyen található
- d) amelyikkel nem lehet aláírni, csak titkosítani

E10) Mi az elektronikus aláírás definíciója az eIDAS szerint?

- a) minden olyan adat, amelyet az aláíró aláírásra használ
- b) hitelesítés céljából elektronikus adathoz csatolt vagy az elektronikus adattal logikailag összerendelt elektronikus adat
- c) a digitális aláírás és az üzenethitelesítő kód együttesen
- d) aszimmetrikus kriptográfiai eszközöket alkalmazó hitelesítési eljárás, mely az elektronikus adattal logikailag elektronikus adatot rendel össze

1 pont

B – Gyakorlati feladatok**Instrukciók:**

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájlal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

- | | | |
|-------|--|--------|
| GY1) | Nyissa meg a BIRSALMA fájlt! Írja le az aláíráshoz használt tanúsítványnak a kiállítóját (CN)! | 2 pont |
| GY2) | Nyissa meg a BIRSALMA fájlt! Mi az aláírás készítőjének a városa (L)? | 2 pont |
| GY3) | Nyissa meg a SZILVA fájlt! Van-e hiteles időbélyeg a fájlban? | 2 pont |
| GY4) | Nyissa meg a MALNA dossziét! Mennyi időbélyeg van a dossziében? | 2 pont |
| GY5) | Nyissa meg a DINNYE dossziét! Hány aláírás van a teljes dosszién? | 2 pont |
| GY6) | Nyissa meg a https://www.njszt.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő sorozatszám? | 2 pont |
| GY7) | Nyissa meg a https://www.njszt.hu honlapot! Írja le az oldal SSL-tanúsítványának kiállítóját (CN)? | 2 pont |
| GY8) | Nyissa meg a https://www.magyarorszag.hu honlapot! Mi az SSL-tanúsítvány érvényességi idejének vége? | 2 pont |
| GY9) | Nyissa meg a https://www.magyarorszag.hu honlapot! Mi az SSL-tanúsítványnak a városa (L)? | 2 pont |
| GY10) | Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) KEAASZ segítségével! | 2 pont |
| GY11) | Írja alá a BIRSALMA fájlt a(z) KEAASZ segítségével! | 2 pont |

E5) Az alábbiak közül melyik írja le a „különálló aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe, és együtt mozog vele
- b) az aláírásba ágyazódnak bele az aláírandó információk 1 pont
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve

E6) Az alábbiak közül melyik írja le a „szekvenciális aláírás” fogalmát?

- a) egymás után, egymásba becsomagolódva elhelyezkedő aláírások
- b) a meglévők felett álló, azoktól függő módon arra ráarakódó aláírások 1 pont
- c) a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól
- d) a dokumentumtól teljesen külön kezelt, de együtt mozgó aláírás

E7) Meddig érvényes egy tanúsítvány?

- a) amíg vissza nem vonják
- b) amíg fel nem függesztik 1 pont
- c) a lejáratí időpontig
- d) a kezdeti időpontig

E8) Melyik tanúsítvány hibás?

- a) amelyik nem tartalmazza a tanúsítvány birtokosának nevét, csak egy álnevet 1 pont
- b) amelyet nem minősített hitelesítésszolgáltató adta ki
- c) amelyik más című webszerverre van kiállítva, mint amelyen található
- d) amelyikkel nem lehet aláírni, csak titkosítani

E9) Mi az a tanúsítási lánc?

- a) a hitelesítésszolgáltató Nemzeti Hírközlési Hatóság általi minősítése
- b) a szoftvereken szereplő aláírások 1 pont
- c) a tanúsítványtárban szereplő gyökértanúsítványok
- d) a tanúsítványkibocsátók felülről lefelé építkező aláírásai

E10) Mi az elektronikus aláírás definíciója az eIDAS szerint?

- a) minden olyan adat, amelyet az aláíró aláírásra használ
- b) hitelesítés céljából elektronikus adathoz csatolt vagy az elektronikus adattal logikailag összerendelt elektronikus adat 1 pont
- c) a digitális aláírás és az üzenethitelesítő kód együttesen
- d) aszimmetrikus kriptográfiai eszközöket alkalmazó hitelesítési eljárás, mely az elektronikus adattal logikailag elektronikus adatot rendel össze

B – Gyakorlati feladatok

Instrukciók:

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájlal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

- | | | |
|-------|---|--------|
| GY1) | Nyissa meg a DATOLYA fájlt! Írja le az aláíráshoz használt tanúsítványnak a aláíró algoritmusát! | 2 pont |
| GY2) | Nyissa meg a DATOLYA fájlt! Mi az aláírás készítőjének a városa (L)? | 2 pont |
| GY3) | Nyissa meg a MEGGY fájlt! Van-e ellenjegyző aláírás a fájlban? | 2 pont |
| GY4) | Nyissa meg a SZEDER dossziét! Mennyi aláírás van a dossziében? | 2 pont |
| GY5) | Nyissa meg a ANANASZ dossziét! Hány időbélyeg van a teljes dosszién? | 2 pont |
| GY6) | Nyissa meg a https://www.magyarország.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő SHA1-ujjlenyomat? | 2 pont |
| GY7) | Nyissa meg a https://www.magyarország.hu honlapot! Írja le az oldal SSL-tanúsítványának aláíró algoritmusát? | 2 pont |
| GY8) | Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítvány kiállítójának neve (CN)? | 2 pont |
| GY9) | Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítványnak a városa (L)? | 2 pont |
| GY10) | Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) KEAASZ segítségével! | 2 pont |
| GY11) | Írja alá a DATOLYA fájlt a(z) KEAASZ segítségével! | 2 pont |

E5) Az alábbiak közül melyik írja le a „különálló aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe, és együtt mozog vele
- b) az aláírásba ágyazódnak bele az aláírandó információk 1 pont
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve

E6) Az alábbiak közül melyik írja le a „szekvenciális aláírás” fogalmát?

- a) egymás után, egymásba becsomagolódva elhelyezkedő aláírások
- b) a meglévők felett álló, azoktól függő módon arra ráarakódó aláírások 1 pont
- c) a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól
- d) a dokumentumtól teljesen külön kezelt, de együtt mozgó aláírás

E7) Az alábbiak közül melyik írja le az „ellenjegyző aláírás” fogalmát?

- a) az aláírások egymás után, mintegy egymásba becsomagolódva helyezkednek el, és ellenőrzésüknél is csak kívülről befelé lehet haladni
- b) a meglévők felett álló, azoktól függő módon azokra ráarakódó aláírás 1 pont
- c) a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól
- d) a dokumentumtól teljesen külön van kezelve, de együtt mozog vele

E8) Az üzenethitelesítő kód biztosítja

- a) a módosítások felderíthetőségét
- b) a tartalom megváltoztathatatlanágát 1 pont
- c) az eredeti tartalom visszaállíthatóságát
- d) a kód személyhez köthetőségét

E9) Meddig érvényes egy tanúsítvány?

- a) amíg vissza nem vonják
- b) amíg fel nem függesztik 1 pont
- c) a lejáratú időpontig
- d) a kezdeti időpontig

E10) Mi az a tanúsítási lánc?

- a) a hitelesítésszolgáltató Nemzeti Hírközlési Hatóság általi minősítése
- b) a szoftvereken szereplő aláírások 1 pont
- c) a tanúsítványtárban szereplő gyökértanúsítványok
- d) a tanúsítványkibocsátók felülről lefelé építkező aláírásai

B – Gyakorlati feladatok**Instrukciók:**

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájlal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

- | | | |
|-------|--|--------|
| GY1) | Nyissa meg az ALMA fájlt! Írja le az aláíráshoz használt tanúsítványnak a érvényességi idejének kezdetét! | 2 pont |
| GY2) | Nyissa meg a GESZTENYE fájlt! Mi az aláírás készítőjének a neve (CN)? | 2 pont |
| GY3) | Nyissa meg a SZILVA fájlt! Van-e hiteles aláírás a fájlban? | 2 pont |
| GY4) | Nyissa meg a MALNA dossziét! Mennyi időbélyeg van a dossziében? | 2 pont |
| GY5) | Nyissa meg az ANANASZ dossziét! Hány aláírás van a teljes dosszién? | 2 pont |
| GY6) | Nyissa meg a https://www.njszt.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő aláíró algoritmus? | 2 pont |
| GY7) | Nyissa meg a https://www.njszt.hu honlapot! Írja le az oldal SSL-tanúsítványának érvényességi idejének kezdetét? | 2 pont |
| GY8) | Nyissa meg a https://www.magyarorszag.hu honlapot! Mi az SSL-tanúsítvány aláíró algoritmus? | 2 pont |
| GY9) | Nyissa meg a https://www.magyarorszag.hu honlapot! Mi az SSL-tanúsítványnak a neve (CN)? | 2 pont |
| GY10) | Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) KEAASZ segítségével! | 2 pont |
| GY11) | Írja alá a az ALMA fájlt a(z) KEAASZ segítségével! | 2 pont |

E5) Mi az elektronikus aláírás definíciója az eIDAS szerint?

- a) minden olyan adat, amelyet az aláíró aláírásra használ
- b) hitelesítés céljából elektronikus adathoz csatolt vagy az elektronikus adattal logikailag összerendelt elektronikus adat
- c) a digitális aláírás és az üzenethitelesítő kód együttesen
- d) aszimmetrikus kriptográfiai eszközöket alkalmazó hitelesítési eljárás, mely az elektronikus adattal logikailag elektronikus adatot rendel össze

1 pont

E6) A digitális aláírás biztosítja

- a) az aláírás személyhez köthetőségét
- b) a tartalom megváltoztathatatlanágát
- c) a módosítások felderíthetőségét
- d) az eredeti tartalom visszaállíthatóságát

1 pont

E7) A digitális aláírás sikeres ellenőrzéséből mely állítás nem következik?

- a) az aláírt adatok ugyanazok, amit a küldő elküldött
- b) az aláírást biztonságos aláíráslétrehozó eszközzel végezték
- c) az aláírást a nyilvános kulcshoz tartozó titkos kulccsal végezték
- d) megfelelő tanúsítvánnyal az a fizikai személy is ismert, aki aláírta az adatokat

1 pont

E8) A digitális aláírás ellenőrzésének sikertelenségéből melyik állítás következhet?

- a) az adatok a küldés során nem változtak meg
- b) a tanúsítvány lejárt
- c) az ellenőrzéskor ugyanazt a kulcsot és algoritmust használták
- d) a nyilvános kulcshoz tartozó tanúsítványt a fogadó megbízhatóvá tette

1 pont

E9) A digitális aláírás során

- a) az aláíró a titkos kulcs birtokosa, a fogadó a nyilvános kulcsot használja
- b) a fogadó a titkos kulcs birtokosa, az aláíró a nyilvános kulcsot használja
- c) a fogadó titkosítja a titkos kulccsal, az aláíró megoldja azt a nyilvános kulccsal
- d) a titkos üzenetet csak az adott felhasználó képes elolvasni

1 pont

E10) Az alábbiak közül melyik írja le a „szekvenciális aláírás” fogalmát?

- a) egymás után, egymásba becsomagolódva elhelyezkedő aláírások
- b) a meglévők felett álló, azoktól függő módon arra rárakódó aláírások
- c) a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól
- d) a dokumentumtól teljesen külön kezelt, de együtt mozgó aláírás

1 pont

B – Gyakorlati feladatok

Instrukciók:

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájjal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

GY1)	Nyissa meg a BIRSALMA fájlt! Írja le az aláíráshoz használt tanúsítványnak a sorozatszámát!	2 pont
GY2)	Nyissa meg az OSZIBARACK fájlt! Mi az aláírás készítőjének a városa (L)?	2 pont
GY3)	Nyissa meg a BANAN fájlt! Van-e hiteles aláírás a fájlban?	2 pont
GY4)	Nyissa meg a SZEDER dossziét! Mennyi időbélyeg van a teljes dosszién?	2 pont
GY5)	Nyissa meg a DINNYE dossziét! Hány aláírás van a dossziében?	2 pont
GY6)	Nyissa meg a https://www.magyarország.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő SHA1-ujjlenyomat?	2 pont
GY7)	Nyissa meg a https://www.magyarország.hu honlapot! Írja le az oldal SSL-tanúsítványának sorozatszámát?	2 pont
GY8)	Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítvány érvényességi idejének kezdete?	2 pont
GY9)	Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítványnak a városa (L)?	2 pont
GY10)	Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) AVDH segítségével!	2 pont
GY11)	Írja alá a BIRSALMA fájlt a(z) AVDH segítségével!	2 pont

E5) Mi az elektronikus aláírás definíciója az eIDAS szerint?

- a) minden olyan adat, amelyet az aláíró aláírásra használ
- b) hitelesítés céljából elektronikus adathoz csatolt vagy az elektronikus adattal logikailag összerendelt elektronikus adat
- c) a digitális aláírás és az üzenethitelesítő kód együttesen
- d) aszimmetrikus kriptográfiai eszközöket alkalmazó hitelesítési eljárás, mely az elektronikus adattal logikailag elektronikus adatot rendel össze

1 pont

E6) A digitális aláírás biztosítja

- a) az aláírás személyhez köthetőségét
- b) a tartalom megváltoztathatatlanágát
- c) a módosítások felderíthetőségét
- d) az eredeti tartalom visszaállíthatóságát

1 pont

E7) A digitális aláírás sikeres ellenőrzéséből mely állítás nem következik?

- a) az aláírt adatok ugyanazok, amit a küldő elküldött
- b) az aláírást biztonságos aláíráslétrehozó eszközzel végezték
- c) az aláírást a nyilvános kulcshoz tartozó titkos kulccsal végezték
- d) megfelelő tanúsítvánnyal az a fizikai személy is ismert, aki aláírta az adatokat

1 pont

E8) Az alábbiak közül melyik írja le a „beágyazott aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe
- b) az aláírásba ágyazódnak bele az aláírandó információk
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele

1 pont

E9) Az alábbiak közül melyik írja le a „szekvenciális aláírás” fogalmát?

- a) egymás után, egymásba becsomagolódva elhelyezkedő aláírások
- b) a meglévők felett álló, azoktól függő módon arra ráarakódó aláírások
- c) a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól
- d) a dokumentumtól teljesen külön kezelt, de együtt mozgó aláírás

1 pont

E10) Az üzenethitelesítő kód biztosítja

- a) a módosítások felderíthetőségét
- b) a tartalom megváltoztathatatlanágát
- c) az eredeti tartalom visszaállíthatóságát
- d) a kód személyhez köthetőségét

1 pont

B – Gyakorlati feladatok

Instrukciók:

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájlal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

- | | | |
|-------|--|--------|
| GY1) | Nyissa meg a DATOLYA fájlt! Írja le az aláíráshoz használt tanúsítványnak a kiállítóját (CN)! | 2 pont |
| GY2) | Nyissa meg a BIRSALMA fájlt! Mi az aláírás készítőjének a neve (CN)? | 2 pont |
| GY3) | Nyissa meg a BANAN fájlt! Van-e hiteles időbélyeg a fájlban? | 2 pont |
| GY4) | Nyissa meg a MALNA dossziét! Mennyi időbélyeg van a teljes dosszién? | 2 pont |
| GY5) | Nyissa meg a SZEDER dossziét! Hány aláírás van a dossziében? | 2 pont |
| GY6) | Nyissa meg a https://www.njszt.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő sorozatszám? | 2 pont |
| GY7) | Nyissa meg a https://www.njszt.hu honlapot! Írja le az oldal SSL-tanúsítványának kiállítóját (CN)? | 2 pont |
| GY8) | Nyissa meg a https://www.magyarorszag.hu honlapot! Mi az SSL-tanúsítvány érvényességi idejének vége? | 2 pont |
| GY9) | Nyissa meg a https://www.magyarorszag.hu honlapot! Mi az SSL-tanúsítványnak a neve (CN)? | 2 pont |
| GY10) | Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) AVDH segítségével! | 2 pont |
| GY11) | Írja alá a DATOLYA fájlt a(z) AVDH segítségével! | 2 pont |

A VIZSGÁZTATÓ TÖLTI KI! ADATOK: VIZSGA DÁTUMA: ÉV HÓ NAP VIZSGAKÖZPONT AZONOSÍTÓJA: VIZSGÁZTATÓ NEVE:	A VIZSGÁZTATÓ TÖLTI KI! ÉRTÉKELÉS: ÖSSZPONTSZÁM: / MAX.: 32 PONT MEGFELELT / NEM FELELT MEG VIZSGÁZTATÓ ALÁÍRÁSA:
	VIZSGÁZÓ NEVE:

11. FELADATSOR

A – Elméleti kérdések

Instrukciók:

Nyissa meg a **VIZSGA** fájlt és írja be válaszainak a betűjeleit a fájlban lévő táblázat E1)-E10) soraiba. Mentse el a kitöltött táblázatot ugyanezen a néven!

E1) Hol van a tanúsítvány visszavonási lista feltalálási helye?

- a) a minősített aláírásban
- b) az időbélyegben 1 pont
- c) a fokozott biztonságú aláírásban
- d) a tanúsítványban

E2) Ki írja alá a felhasználói tanúsítványt?

- a) a felhasználó a saját titkos kulcsával
- b) a hitelesítésszolgáltató a saját titkos kulcsával 1 pont
- c) a hitelesítésszolgáltató a nyilvános kulcsával
- d) a tanúsítványok önaláírtak

E3) Ki töltheti le a tanúsítványokat a bizalmi szolgáltatótól?

- a) csak a tulajdonosuk
- b) a tulajdonos munkáltatója 1 pont
- c) bárki
- d) csak állami hatóságok

E4) Meddig érvényes egy tanúsítvány?

- a) amíg vissza nem vonják
- b) amíg fel nem függesztik 1 pont
- c) a lejáratí időpontig
- d) a kezdeti időpontig

E5) Melyik tanúsítvány hibás?

- a) amelyik nem tartalmazza a tanúsítvány birtokosának nevét, csak egy álnevet
- b) amelyet nem minősített hitelesítésszolgáltató adta ki
- c) amelyik más című webszerverre van kiállítva, mint amelyen található
- d) amelyikkel nem lehet aláírni, csak titkosítani

1 pont

E6) A digitális aláírás biztosítja

- a) az aláírás személyhez köthetőségét
- b) a tartalom megváltoztathatatlanágát
- c) a módosítások felderíthetőségét
- d) az eredeti tartalom visszaállíthatóságát

1 pont

E7) A digitális aláírás ellenőrzésének sikertelenségéből melyik állítás következhet?

- a) az adatok a küldés során nem változtak meg
- b) a tanúsítvány lejárt
- c) az ellenőrzéskor ugyanazt a kulcsot és algoritmust használták
- d) a nyilvános kulcshoz tartozó tanúsítványt a fogadó megbízhatóvá tette

1 pont

E8) A digitális aláírás során

- a) az aláíró a titkos kulcs birtokosa, a fogadó a nyilvános kulcsot használja
- b) a fogadó a titkos kulcs birtokosa, az aláíró a nyilvános kulcsot használja
- c) a fogadó titkosít a titkos kulccsal, az aláíró megoldja azt a nyilvános kulccsal
- d) a titkos üzenetet csak az adott felhasználó képes elolvasni

1 pont

E9) Az alábbiak közül melyik írja le a „beágyazott aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe
- b) az aláírásba ágyazódnak bele az aláírandó információk
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele

1 pont

E10) Az üzenethitelesítő kód biztosítja

- a) a módosítások felderíthetőségét
- b) a tartalom megváltoztathatatlanágát
- c) az eredeti tartalom visszaállíthatóságát
- d) a kód személyhez köthetőségét

1 pont

B – Gyakorlati feladatok

Instrukciók:

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájlal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

GY1)	Nyissa meg a GESZTENYE fájlt! Írja le az aláíráshoz használt tanúsítványnak a aláíró algoritmusát!	2 pont
GY2)	Nyissa meg a DATOLYA fájlt! Mi az aláírás készítőjének a városa (L)?	2 pont
GY3)	Nyissa meg az EPER fájlt! Van-e ellenjegyző aláírás a fájlban?	2 pont
GY4)	Nyissa meg a SZEDER dossziét! Mennyi időbélyeg van a dossziében?	2 pont
GY5)	Nyissa meg az ANANASZ dossziét! Hány aláírás van a teljes dosszién?	2 pont
GY6)	Nyissa meg a https://www.magyarország.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő SHA1-ujjlenyomat?	2 pont
GY7)	Nyissa meg a https://www.magyarország.hu honlapot! Írja le az oldal SSL-tanúsítványának aláíró algoritmusát?	2 pont
GY8)	Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítvány kiállítójának neve (CN)?	2 pont
GY9)	Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítványnak a városa (L)?	2 pont
GY10)	Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) AVDH segítségével!	2 pont
GY11)	Írja alá a a GESZTENYE fájlt a(z) AVDH segítségével!	2 pont

E5) Melyik tanúsítvány hibás?

- a) amelyik nem tartalmazza a tanúsítvány birtokosának nevét, csak egy árnevet
- b) amelyet nem minősített hitelesítésszolgáltató adta ki
- c) amelyik más című webszerverre van kiállítva, mint amelyen található
- d) amelyikkel nem lehet aláírni, csak titkosítani

1 pont

E6) A digitális aláírás biztosítja

- a) az aláírás személyhez köthetőségét
- b) a tartalom megváltoztathatatlanágát
- c) a módosítások felderíthetőségét
- d) az eredeti tartalom visszaállíthatóságát

1 pont

E7) A digitális aláírás ellenőrzésének sikertelenségéből melyik állítás következhet?

- a) az adatok a küldés során nem változtak meg
- b) a tanúsítvány lejárt
- c) az ellenőrzéskor ugyanazt a kulcsot és algoritmust használták
- d) a nyilvános kulcshoz tartozó tanúsítványt a fogadó megbízhatóvá tette

1 pont

E8) Az alábbiak közül melyik írja le a „beágyazott aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe
- b) az aláírásba ágyazódnak bele az aláírandó információk
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele

1 pont

E9) Az alábbiak közül melyik írja le a „különálló aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe, és együtt mozog vele
- b) az aláírásba ágyazódnak bele az aláírandó információk
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve

1 pont

E10) Az alábbiak közül melyik írja le a „különálló aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe, és együtt mozog vele
- b) az aláírásba ágyazódnak bele az aláírandó információk
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve

1 pont

B – Gyakorlati feladatok**Instrukciók:**

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájlal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

- | | | |
|-------|---|--------|
| GY1) | Nyissa meg a MAZSOLA fájlt! Írja le az aláíráshoz használt tanúsítványnak a érvényességi idejének kezdetét! | 2 pont |
| GY2) | Nyissa meg a GESZTENYE fájlt! Mi az aláírás készítőjének a neve (CN)? | 2 pont |
| GY3) | Nyissa meg a BANAN fájlt! Van-e hiteles aláírás a fájlban? | 2 pont |
| GY4) | Nyissa meg az ANANASZ dossziét! Mennyi aláírás van a dossziében? | 2 pont |
| GY5) | Nyissa meg a DINNYE dossziét! Hány időbélyeg van a teljes dosszién? | 2 pont |
| GY6) | Nyissa meg a https://www.njszt.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő aláíró algoritmus? | 2 pont |
| GY7) | Nyissa meg a https://www.njszt.hu honlapot! Írja le az oldal SSL-tanúsítványának érvényességi idejének kezdetét? | 2 pont |
| GY8) | Nyissa meg a https://www.magyarorszag.hu honlapot! Mi az SSL-tanúsítvány aláíró algoritmus? | 2 pont |
| GY9) | Nyissa meg a https://www.magyarorszag.hu honlapot! Mi az SSL-tanúsítványnak a neve (CN)? | 2 pont |
| GY10) | Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) AVDH segítségével! | 2 pont |
| GY11) | Írja alá a MAZSOLA fájlt a(z) AVDH segítségével! | 2 pont |

E5) Mi az elektronikus aláírás definíciója az eIDAS szerint?

- a) minden olyan adat, amelyet az aláíró aláírásra használ
- b) hitelesítés céljából elektronikus adathoz csatolt vagy az elektronikus adattal logikailag összerendelt elektronikus adat
- c) a digitális aláírás és az üzenethitelesítő kód együttesen
- d) aszimmetrikus kriptográfiai eszközöket alkalmazó hitelesítési eljárás, mely az elektronikus adattal logikailag elektronikus adatot rendel össze

1 pont

E6) A digitális aláírás biztosítja

- a) az aláírás személyhez köthetőségét
- b) a tartalom megváltoztathatatlanágát
- c) a módosítások felderíthetőségét
- d) az eredeti tartalom visszaállíthatóságát

1 pont

E7) A digitális aláírás ellenőrzésének sikertelenségéből melyik állítás következhet?

- a) az adatok a küldés során nem változtak meg
- b) a tanúsítvány lejárt
- c) az ellenőrzéskor ugyanazt a kulcsot és algoritmust használták
- d) a nyilvános kulcshoz tartozó tanúsítványt a fogadó megbízhatóvá tette

1 pont

E8) Az alábbiak közül melyik írja le a „beágyazott aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe
- b) az aláírásba ágyazódnak bele az aláírandó információk
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele

1 pont

E9) Az alábbiak közül melyik írja le a „különálló aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe, és együtt mozog vele
- b) az aláírásba ágyazódnak bele az aláírandó információk
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve

1 pont

E10) Az alábbiak közül melyik írja le a „szekvenciális aláírás” fogalmát?

- a) egymás után, egymásba becsomagolódva elhelyezkedő aláírások
- b) a meglévők felett álló, azoktól függő módon arra rárakódó aláírások
- c) a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól
- d) a dokumentumtól teljesen külön kezelt, de együtt mozgó aláírás

1 pont

B – Gyakorlati feladatok

Instrukciók:

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájlal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

-
- | | | |
|-------|---|--------|
| GY1) | Nyissa meg az OSZIBARACK fájlt! Írja le az aláíráshoz használt tanúsítványnak a érvényességi idejének végét! | 2 pont |
| GY2) | Nyissa meg a MAZSOLA fájlt! Mi az aláírás készítőjének a neve (CN)? | 2 pont |
| GY3) | Nyissa meg az EPER fájlt! Van-e hiteles időbélyeg a fájlban? | 2 pont |
| GY4) | Nyissa meg a DINNYE dossziét! Mennyi aláírás van a teljes dosszién? | 2 pont |
| GY5) | Nyissa meg a MALNA dossziét! Hány időbélyeg van a dossziében? | 2 pont |
| GY6) | Nyissa meg a https://www.magyarország.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő SHA1-ujjlenyomat? | 2 pont |
| GY7) | Nyissa meg a https://www.magyarország.hu honlapot! Írja le az oldal SSL-tanúsítványának érvényességi idejének végét? | 2 pont |
| GY8) | Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítvány érvényességi idejének kezdete? | 2 pont |
| GY9) | Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítványnak a neve (CN)? | 2 pont |
| GY10) | Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) AVDH segítségével! | 2 pont |
| GY11) | Írja alá a az OSZIBARACK fájlt a(z) AVDH segítségével! | 2 pont |

<p>A VIZSGÁZTATÓ TÖLTI KI!</p> <p>ADATOK:</p> <p>VIZSGA DÁTUMA: ÉV HÓ NAP</p> <p>VIZSGAKÖZPONT AZONOSÍTÓJA:</p> <p>VIZSGÁZTATÓ NEVE:</p>	<p>A VIZSGÁZTATÓ TÖLTI KI!</p> <p>ÉRTÉKELÉS:</p> <p>ÖSSZPONTSZÁM: / MAX.: 32 PONT</p> <p style="text-align: center;">MEGFELELT / NEM FELELT MEG</p> <p>VIZSGÁZTATÓ ALÁÍRÁSA:</p> <hr/> <p>VIZSGÁZÓ NEVE:</p>
--	--

14. FELADATSOR

A – Elméleti kérdések

Instrukciók:

Nyissa meg a **VIZSGA** fájlt és írja be válaszainak a betűjeleit a fájlban lévő táblázat E1)-E10) soraiba. Mentse el a kitöltött táblázatot ugyanezen a néven!

E1) Az üzenethitelesítő kód biztosítja

- a) a módosítások felderíthetőségét
- b) a tartalom megváltoztathatatlanságát
- c) az eredeti tartalom visszaállíthatóságát
- d) a kód személyhez köthetőségét

1 pont

E2) Hol van a tanúsítvány visszavonási lista feltalálási helye?

- a) a minősített aláírásban
- b) az időbélyegben
- c) a fokozott biztonságú aláírásban
- d) a tanúsítványban

1 pont

E3) Ki írja alá a felhasználói tanúsítványt?

- a) a felhasználó a saját titkos kulcsával
- b) a hitelesítésszolgáltató a saját titkos kulcsával
- c) a hitelesítésszolgáltató a nyilvános kulcsával
- d) a tanúsítványok önaláírtak

1 pont

E4) Melyik tanúsítvány hibás?

- a) amelyik nem tartalmazza a tanúsítvány birtokosának nevét, csak egy árnevet
- b) amelyiket nem minősített hitelesítésszolgáltató adta ki
- c) amelyik más című webszerverre van kiállítva, mint amelyen található
- d) amelyikkel nem lehet aláírni, csak titkosítani

1 pont

E5) Mi az elektronikus aláírás definíciója az eIDAS szerint?

- a) minden olyan adat, amelyet az aláíró aláírásra használ
- b) hitelesítés céljából elektronikus adathoz csatolt vagy az elektronikus adattal logikailag összerendelt elektronikus adat
- c) a digitális aláírás és az üzenethitelesítő kód együttesen
- d) aszimmetrikus kriptográfiai eszközöket alkalmazó hitelesítési eljárás, mely az elektronikus adattal logikailag elektronikus adatot rendel össze

1 pont

E6) A digitális aláírás biztosítja

- a) az aláírás személyhez köthetőségét
- b) a tartalom megváltoztathatatlanágát
- c) a módosítások felderíthetőségét
- d) az eredeti tartalom visszaállíthatóságát

1 pont

E7) A digitális aláírás sikeres ellenőrzéséből mely állítás nem következik?

- a) az aláírt adatok ugyanazok, amit a küldő elküldött
- b) az aláírást biztonságos aláíráslétrehozó eszközzel végezték
- c) az aláírást a nyilvános kulcshoz tartozó titkos kulccsal végezték
- d) megfelelő tanúsítvánnyal az a fizikai személy is ismert, aki aláírta az adatokat

1 pont

E8) Az alábbiak közül melyik írja le a „beágyazott aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe
- b) az aláírásba ágyazódnak bele az aláírandó információk
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele

1 pont

E9) Az alábbiak közül melyik írja le a „szekvenciális aláírás” fogalmát?

- a) egymás után, egymásba becsomagolódva elhelyezkedő aláírások
- b) a meglévők felett álló, azoktól függő módon arra ráakódó aláírások
- c) a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól
- d) a dokumentumtól teljesen külön kezelt, de együtt mozgó aláírás

1 pont

E10) Az alábbiak közül melyik írja le az „ellenjegyző aláírás” fogalmát?

- a) az aláírások egymás után, mintegy egymásba becsomagolódva helyezkednek el, és ellenőrzésüknél is csak kívülről befelé lehet haladni
- b) a meglévők felett álló, azoktól függő módon azokra ráakódó aláírás
- c) a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól
- d) a dokumentumtól teljesen külön van kezelve, de együtt mozog vele

1 pont

B – Gyakorlati feladatok

Instrukciók:

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájlal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

GY1)	Nyissa meg az ALMA fájlt! Írja le az aláíráshoz használt tanúsítványnak a tulajdonosát (CN)!	2 pont
GY2)	Nyissa meg az OSZIBARACK fájlt! Mi az aláírás készítőjének a városa (L)?	2 pont
GY3)	Nyissa meg a MEGGY fájlt! Van-e ellenjegyző aláírás a fájlban?	2 pont
GY4)	Nyissa meg a DINNYE dossziét! Mennyi időbélyeg van a dossziében?	2 pont
GY5)	Nyissa meg a SZEDER dossziét! Hány aláírás van a teljes dosszién?	2 pont
GY6)	Nyissa meg a https://www.njszt.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő sorozatszám?	2 pont
GY7)	Nyissa meg a https://www.njszt.hu honlapot! Írja le az oldal SSL-tanúsítványának tulajdonosát (CN)?	2 pont
GY8)	Nyissa meg a https://www.magyarország.hu honlapot! Mi az SSL-tanúsítvány érvényességi idejének vége?	2 pont
GY9)	Nyissa meg a https://www.magyarország.hu honlapot! Mi az SSL-tanúsítványnak a városa (L)?	2 pont
GY10)	Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) AVDH segítségével!	2 pont
GY11)	Írja alá a az ALMA fájlt a(z) AVDH segítségével!	2 pont

<p>A VIZSGÁZTATÓ TÖLTI KI!</p> <p>ADATOK:</p> <p>VIZSGA DÁTUMA: ÉV HÓ NAP</p> <p>VIZSGAKÖZPONT AZONOSÍTÓJA:</p> <p>VIZSGÁZTATÓ NEVE:</p>	<p>A VIZSGÁZTATÓ TÖLTI KI!</p> <p>ÉRTÉKELÉS:</p> <p>ÖSSZPONTSZÁM: / MAX.: 32 PONT</p> <p style="text-align: center;">MEGFELELT / NEM FELELT MEG</p> <p>VIZSGÁZTATÓ ALÁÍRÁSA:</p> <hr/> <p>VIZSGÁZÓ NEVE:</p>
--	--

15. FELADATSOR

A – Elméleti kérdések

Instrukciók:

Nyissa meg a **VIZSGA** fájlt és írja be válaszainak a betűjeleit a fájlban lévő táblázat E1)-E10) soraiba. Mentse el a kitöltött táblázatot ugyanezen a néven!

E1) Hol van a tanúsítvány visszavonási lista feltalálási helye?

- a) a minősített aláírásban
- b) az időbélyegben
- c) a fokozott biztonságú aláírásban
- d) a tanúsítványban

1 pont

E2) Ki töltheti le a tanúsítványokat a bizalmi szolgáltatótól?

- a) csak a tulajdonosuk
- b) a tulajdonos munkáltatója
- c) bárki
- d) csak állami hatóságok

1 pont

E3) Meddig érvényes egy tanúsítvány?

- a) amíg vissza nem vonják
- b) amíg fel nem függesztik
- c) a lejáratú időpontig
- d) a kezdeti időpontig

1 pont

E4) Melyik tanúsítvány hibás?

- a) amelyik nem tartalmazza a tanúsítvány birtokosának nevét, csak egy árnevet
- b) amelyiket nem minősített hitelesítésszolgáltató adta ki
- c) amelyik más című webszerverre van kiállítva, mint amelyen található
- d) amelyikkel nem lehet aláírni, csak titkosítani

1 pont

E5) Mi az elektronikus aláírás definíciója az eIDAS szerint?

- a) minden olyan adat, amelyet az aláíró aláírásra használ
- b) hitelesítés céljából elektronikus adathoz csatolt vagy az elektronikus adattal logikailag összerendelt elektronikus adat
- c) a digitális aláírás és az üzenethitelesítő kód együttesen
- d) aszimmetrikus kriptográfiai eszközöket alkalmazó hitelesítési eljárás, mely az elektronikus adattal logikailag elektronikus adatot rendel össze

1 pont

E6) A digitális aláírás sikeres ellenőrzéséből mely állítás nem következik?

- a) az aláírt adatok ugyanazok, amit a küldő elküldött
- b) az aláírást biztonságos aláíráslétrehozó eszközzel végezték
- c) az aláírást a nyilvános kulcshoz tartozó titkos kulccsal végezték
- d) megfelelő tanúsítvánnyal az a fizikai személy is ismert, aki aláírta az adatokat

1 pont

E7) A digitális aláírás ellenőrzésének sikertelenségéből melyik állítás következhet?

- a) az adatok a küldés során nem változtak meg
- b) a tanúsítvány lejárt
- c) az ellenőrzéskor ugyanazt a kulcsot és algoritmust használták
- d) a nyilvános kulcshoz tartozó tanúsítványt a fogadó megbízhatóvá tette

1 pont

E8) A digitális aláírás során

- a) az aláíró a titkos kulcs birtokosa, a fogadó a nyilvános kulcsot használja
- b) a fogadó a titkos kulcs birtokosa, az aláíró a nyilvános kulcsot használja
- c) a fogadó titkosít a titkos kulccsal, az aláíró megoldja azt a nyilvános kulccsal
- d) a titkos üzenetet csak az adott felhasználó képes elolvasni

1 pont

E9) Az alábbiak közül melyik írja le a „beágyazott aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe
- b) az aláírásba ágyazódnak bele az aláírandó információk
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás az aláírandó információktól teljesen külön van kezelve, de együtt mozog vele

1 pont

E10) Az alábbiak közül melyik írja le a „különálló aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe, és együtt mozog vele
- b) az aláírásba ágyazódnak bele az aláírandó információk
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve

1 pont

B – Gyakorlati feladatok

Instrukciók:

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájlal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

- | | | |
|-------|---|--------|
| GY1) | Nyissa meg a BIRSALMA fájlt! Írja le az aláíráshoz használt tanúsítványnak a kiállítóját (CN)! | 2 pont |
| GY2) | Nyissa meg a BIRSALMA fájlt! Mi az aláírás készítőjének a városa (L)? | 2 pont |
| GY3) | Nyissa meg a SZILVA fájlt! Van-e hiteles időbélyeg a fájlban? | 2 pont |
| GY4) | Nyissa meg a DINNYE dossziét! Mennyi időbélyeg van a dossziében? | 2 pont |
| GY5) | Nyissa meg a DINNYE dossziét! Hány aláírás van a teljes dosszién? | 2 pont |
| GY6) | Nyissa meg a https://www.magyarország.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő SHA1-ujjlenyomat? | 2 pont |
| GY7) | Nyissa meg a https://www.magyarország.hu honlapot! Írja le az oldal SSL-tanúsítványának kiállítóját (CN)? | 2 pont |
| GY8) | Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítvány kiállítójának neve (CN)? | 2 pont |
| GY9) | Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítványnak a városa (L)? | 2 pont |
| GY10) | Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) AVDH segítségével! | 2 pont |
| GY11) | Írja alá a BIRSALMA fájlt a(z) AVDH segítségével! | 2 pont |

<p>A VIZSGÁZTATÓ TÖLTI KI!</p> <p>ADATOK:</p> <p>VIZSGA DÁTUMA: ÉV HÓ NAP</p> <p>VIZSGAKÖZPONT AZONOSÍTÓJA:</p> <p>VIZSGÁZTATÓ NEVE:</p>	<p>A VIZSGÁZTATÓ TÖLTI KI!</p> <p>ÉRTÉKELÉS:</p> <p>ÖSSZPONTSZÁM: / MAX.: 32 PONT</p> <p style="text-align: center;">MEGFELELT / NEM FELELT MEG</p> <p>VIZSGÁZTATÓ ALÁÍRÁSA:</p> <hr/> <p>VIZSGÁZÓ NEVE:</p>
--	--

16. FELADATSOR

A – Elméleti kérdések

Instrukciók:

Nyissa meg a **VIZSGA** fájlt és írja be válaszainak a betűjeleit a fájlban lévő táblázat E1)-E10) soraiba. Mentse el a kitöltött táblázatot ugyanezen a néven!

E1) Hol van a tanúsítvány visszavonási lista feltalálási helye?

- a) a minősített aláírásban
- b) az időbélyegben 1 pont
- c) a fokozott biztonságú aláírásban
- d) a tanúsítványban

E2) Ki írja alá a felhasználói tanúsítványt?

- a) a felhasználó a saját titkos kulcsával
- b) a hitelesítésszolgáltató a saját titkos kulcsával 1 pont
- c) a hitelesítésszolgáltató a nyilvános kulcsával
- d) a tanúsítványok önaláírtak

E3) Ki töltheti le a tanúsítványokat a bizalmi szolgáltatótól?

- a) csak a tulajdonosuk
- b) a tulajdonos munkáltatója 1 pont
- c) bárki
- d) csak állami hatóságok

E4) Meddig érvényes egy tanúsítvány?

- a) amíg vissza nem vonják
- b) amíg fel nem függesztik 1 pont
- c) a lejáratí időpontig
- d) a kezdeti időpontig

E5) Mi az a tanúsítási lánc?

- a) a hitelesítésszolgáltató Nemzeti Hírközlési Hatóság általi minősítése
- b) a szoftvereken szereplő aláírások 1 pont
- c) a tanúsítványtárban szereplő gyökértanúsítványok
- d) a tanúsítványkibocsátók felülről lefelé építkező aláírásai

E6) A digitális aláírás biztosítja

- a) az aláírás személyhez köthetőségét
- b) a tartalom megváltoztathatatlanságát 1 pont
- c) a módosítások felderíthetőségét
- d) az eredeti tartalom visszaállíthatóságát

E7) A digitális aláírás ellenőrzésének sikertelenségéből melyik állítás következhet?

- a) az adatok a küldés során nem változtak meg
- b) a tanúsítvány lejárt 1 pont
- c) az ellenőrzéskor ugyanazt a kulcsot és algoritmust használták
- d) a nyilvános kulcshoz tartozó tanúsítványt a fogadó megbízhatóvá tette

E8) Az alábbiak közül melyik írja le a „különálló aláírás” fogalmát?

- a) az aláírás beágyazódik egy magasabb szintű aláírt egységbe, és együtt mozog vele
- b) az aláírásba ágyazódnak bele az aláírandó információk 1 pont
- c) az aláírás beágyazódik egy dokumentumba
- d) az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve

E9) Az alábbiak közül melyik írja le az „ellenjegyző aláírás” fogalmát?

- a) az aláírások egymás után, mintegy egymásba becsomagolódva helyezkednek el, és ellenőrzésüknél is csak kívülről befelé lehet haladni
- b) a meglévők felett álló, azoktól függő módon azokra ráakódó aláírás 1 pont
- c) a meglévőkkel egyenrangú aláírás, és nem függ semmilyen módon a korábbiaktól
- d) a dokumentumtól teljesen külön van kezelve, de együtt mozog vele

E10) Az üzenethitelesítő kód biztosítja

- a) a módosítások felderíthetőségét
- b) a tartalom megváltoztathatatlanságát 1 pont
- c) az eredeti tartalom visszaállíthatóságát
- d) a kód személyhez köthetőségét

B – Gyakorlati feladatok**Instrukciók:**

A Vizsgázónak több, a **VIZSGAFAJLOK** könyvtárban előre elkészített fájlal és előre telepített tanúsítvánnyal kell dolgoznia a vizsga közben, melyeket a Vizsgaközpont bocsát a rendelkezésére. Minden Vizsgázónak a megadott munkakönyvtárban kell dolgoznia! Az előre elkészített fájlok módosítása tilos!

A fájlokat pontosan a feladatban előírt módon kell elnevezni! Kisebb hibák (elírások, helyesírási hibák) nem jelentenek hibapontokat! A munkaközi fájlok nem lesznek kiértékelve!

Írja be válaszait a **VIZSGA** fájlban lévő táblázat GY1)-GY7) soraiba. A GY8)-GY11) sorokat hagyja üresen! Mentse el a fájlt a válaszok beírása után!

Mentse el és zárja be az összes fájlt, valamint zárja be az összes programot a vizsga befejezésével!

- | | | |
|-------|---|--------|
| GY1) | Nyissa meg a DATOLYA fájlt! Írja le az aláíráshoz használt tanúsítványnak a aláíró algoritmusát! | 2 pont |
| GY2) | Nyissa meg a DATOLYA fájlt! Mi az aláírás készítőjének a városa (L)? | 2 pont |
| GY3) | Nyissa meg a MEGGY fájlt! Van-e ellenjegyző aláírás a fájlban? | 2 pont |
| GY4) | Nyissa meg a SZEDER dossziét! Mennyi aláírás van a dossziében? | 2 pont |
| GY5) | Nyissa meg a ANANASZ dossziét! Hány időbélyeg van a teljes dosszién? | 2 pont |
| GY6) | Nyissa meg a https://www.magyarország.hu honlapot! Mi az oldal SSL-tanúsítványában szereplő SHA1-ujjlenyomat? | 2 pont |
| GY7) | Nyissa meg a https://www.magyarország.hu honlapot! Írja le az oldal SSL-tanúsítványának aláíró algoritmusát? | 2 pont |
| GY8) | Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítvány kiállítójának neve (CN)? | 2 pont |
| GY9) | Nyissa meg a https://www.njszt.hu honlapot! Mi az SSL-tanúsítványnak a városa (L)? | 2 pont |
| GY10) | Készítsen a VIZSGA dokumentumból egy PDF fájlt! Írja alá a VIZSGA.pdf dokumentumot a(z) AVDH segítségével! | 2 pont |
| GY11) | Írja alá a DATOLYA fájlt a(z) AVDH segítségével! | 2 pont |