

2. Elektronikus aláírás

Az elektronikus aláírás segítségével lehetőségünk van digitális dokumentumokat a kézi aláírással egyenértékű módon hitelesíteni. Ennek a rendszernek a bemutatásához kell készítenie egy prezentációt. Az elkészítéséhez használja fel a *diaszoveg.txt* UTF-8 kódolású szövegállományt és az *alairt.png*, *dokumentum.png*, *hasheles.png*, *hitelesito.png*, *kodolt.png*, *pki.png*, *tanusitvany.png*, *tkulcs.png* képeket!

1. Hozza létre a bemutatókészítő program segítségével az *e_alairas* nevű 4 diából álló bemutatót a program alapértelmezett formátumában, 16:9-es diaméterarányal!
 2. A diák hátere egységesen szürkés-kék RGB (219, 225, 228) kódú színű legyen! A karakterek és egyéb alakzatok vonal- és kitöltőszíne sötét-kék RGB(39, 49, 53) kódú színű legyen, ahol a feladat másképp nem kéri!
 3. A diákon Arial (Nimbus Sans) betűtípust alkalmazzon 60, 40, 26, 22, 16 pontos méretben! A diák címei félkövér betűstílusúak legyenek!
 4. Másolja vagy gépelje be a diákra a szövegeket! A diák címeit igazítsa a minta szerint!
 5. Az első dián a cím függőlegesen és vízszintesen is középen jelenjen meg!
 6. A második és harmadik dián alakítson ki kétszintű felsorolást a minta szerint 26 és 22 pontos betűmérettel! A harmadik dián a kétszintű felsorolást tartalmazó szövegdoboz szélességét állítsa 16,5 cm szélességűre!
 7. Szúrja be a harmadik diára rendre a *pki.png*, *hitelesito.png*, *hasheles.png* képeket! A képeket helyezze el a megfelelő felsorolás mellé a mintának megfelelően! A képek méretét az arányok megtartása mellett, állítsa be úgy, hogy azok ne érjenek a szöveghez és ne lógnak ki a diáról! A képeket igazítsa egymáshoz képest vízszintesen közepre!
 8. A negyedik dián a minta alapján készítse el az elektronikus aláírás készítés folyamatának ábráját! Ehhez használja fel az *alairt.png*, *dokumentum.png*, *hasheles.png*, *kodolt.png*, *tanusitvany.png* és *tkulcs.png* képeket a mintának megfelelő számban! A képek méretét úgy állítsa be, hogy azok kitöltsék a dia szélességét, de egymást ne érintsék és ne lógnak ki a diáról!
 9. Az alakzatok közül szúrja be a plusz- és egyenlőség jeleket, a nyilat a kellő számban és két kitöltés nélküli téglalapot! Az alakzatokat a következőképpen állítsa be!
 - a. A pluszjelek mérete 1,4×1,4 cm legyen!
 - b. Az egyenlőségjel mérete 1,4 cm magas és 1,8 cm széles legyen!
 - c. A nyíl magasságát 0,6-0,8 cm között, a szélességét pedig 1,6-2 cm közöttire állítsa be!
 - d. A téglalapok méretét úgy válassza meg, hogy a benne lévő alakzatokat, képeket sehol ne érintsék! A téglalapok vonalvastagsága 3 pontos legyen!
 - e. Az alakzatok vonal- és kitöltőszíne a fent megadott sötét-kék színű legyen!
 10. A negyedik dián elkészített két sorban lévő ábrákat soronként igazítsa egymáshoz képest függőlegesen közepre!
 11. Készítse el a négy feliratot 16 pontos betűmérettel a minta alapján a negyedik diára! A feliratok szövege a már megadott tulajdonságok mellett legyen félkövér betűstílusú! A feliratokat helyezze el a mintának megfelelően az adott alakzatokhoz!
-

12. Készítsen animációt a harmadik diára a következőképpen!

- A felsorolások első szintenként egyszerű helyben történő animációval jelenjenek meg a második szinttel együtt, kattintásra!
- Az egyes fogalmak szövegének megjelenése után a hozzá tartozó képek automatikusan ússzanak be jobbról!

30 pont

Minta:

Elektronikus aláírás

Fogalmak

- Elektronikus aláírás
 - elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.
- Aláírás-létrehozó adat
 - kriptográfiai magánkulcs, az aláíró az elektronikus aláírás létrehozásához használja.
- Aláírás-ellenőrző adat
 - kriptográfiai nyilvános kulcs, az elektronikusan aláírt elektronikus dokumentum aláírás ellenőrzésére használják.
- Aláírás-létrehozó eszköz
 - olyan hardver, illetve szoftver eszköz, melynek segítségével az elektronikus aláírás létrehozható.

1. dia

2. dia

Megvalósítása

- Nyilvános kulcsú infrastruktúra
 - Az aláírást létrehozónak van egy titkos (aláírás-létrehozó adat) és egy nyilvános kulcsa (aláírás-ellenőrző adat)
- Hitelesítésszolgáltató
 - Az aláírást létrehozót hitelesíti, egy tanúsítványt állít ki, amely többek között az aláírást létrehozó nyilvános kulcsát tartalmazza.
- Hash
 - Olyan függvény, amely tetszőleges hosszúságú adatból egy adott hosszúságú adatot képez.

3. dia

Az elektronikus aláírás folyamata

Dokumentum

Aláírás

4. dia