

| | | | | | | | | | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| | | | | | | | | | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

1. Enigma

Az Enigma üzenetek rejtjelezésére használt, német gyártmányú elektromechanikus berendezés. Feltörése komoly gondot okozott a szövetségeseknek a II. világháborúban, és többek között az egyik első számítógép, a Colossus kifejlesztéséhez vezetett. Ebben a feladatban egy Enigmáról szóló cikket kell elkészítenie az alábbi leírásnak és a mintának megfelelően. Ehhez használja fel az *eniforr.txt* UTF-8 kódolású szöveges állományt, valamint az *eni1.jpg*, *eni2.png* és a *nyil.png* nevű képeket!

- Hozza létre szövegszerkesztő program segítségével az *enigma* nevű dokumentumot a program alapértelmezett formátumában! Olvassa be a dokumentumba ékezhelyesen az *eniforr.txt* szöveges állomány tartalmát!
- A dokumentum legyen álló tájolású és A4-es lapméretű! Az alsó és a felső margót állítsa 2,6 cm-re, a bal és a jobb margót pedig 2 cm-re!
- Formázza meg a teljes beolvasott szöveget 11 pontos betűméretű Times New Roman (Nimbus Roman) betűtípussal, állítson be egyszeres sorközt, továbbá a bekezdések előtt 6 pontos, a bekezdések után 0 pontos térközt! A bekezdések legyenek sorkizártak! (A beállításokat egyes szövegrészek esetén a feladat további előírásai módosíthatják.)
- Alkalmazza a dokumentum szövegére a *Címsor 1*, *Címsor 2* és *Címsor 3* stílusokat az ábrán szereplő tagolásnak megfelelően (balról jobbra: *Címsor 1*, *Címsor 2*, *Címsor 3*)! A címsorok megkeresését segíti, hogy előttük egy üres bekezdést talál. Ezeket az üres bekezdéseket törölje a dokumentumból!
- Módosítsa az alkalmazott stílusokat az alábbi leírásnak megfelelően:

| stílus | karakterformátum | bekezdésformátum |
|----------|--|--|
| Címsor 1 | Arial (Nimbus Sans), 18 pontos, félkövér, fekete színű | előtte 0 pontos, utána 24 pontos térköz, egyszeres sorköz |
| Címsor 2 | Arial (Nimbus Sans), 14 pontos, félkövér, dőlt, fekete színű | előtte 18 pontos, utána 12 pontos térköz, egyszeres sorköz |
| Címsor 3 | Arial (Nimbus Sans), 12 pontos, félkövér, fekete színű | előtte 12 pontos, utána 6 pontos térköz, egyszeres sorköz |

- Hozzon létre egy új bekezdésszínt *bevezet* néven a következő beállításokkal: a bekezdés betűtípusa legyen Times New Roman (Nimbus Roman), betűstílusa dőlt, betűmérete 11 pontos, betűszíne sötétszürke! A bekezdések igazítása legyen sorkizárt, bal és jobb oldali behúzása egyaránt 1 cm! Formázza meg *bevezet* stílussal a főcím utáni, valamint a „*Részei*” és a „*Feltörése*” címek utáni első bekezdést!
- A főcím utáni első bekezdésben („*Az Enigma üzenetek sifírozására...*”) az Enigma szó első előfordulásához illesztve szúrja be lábjegyzetként a bekezdést követő kapcsos zárójelek közötti részt! A lábjegyzet-hivatkozás szimbóluma „*” karakter legyen! A kapcsos zárójeleket tartalmazó bekezdést törölje!

| |
|--------------------------|
| Az Enigma |
| Fejlesztése és története |
| A kereskedelmi Enigma |
| A katonai Enigma |
| Az Enigma főbb típusai |
| Részei |
| Működése |
| Tárcsák |
| Léptetés |
| Fordító |
| Kapocstábla |
| Tartozékok |
| Használata |
| Feltörése |
| Lengyel titkosszolgalat |
| Bletchley Park |
| A Colossus |

| | | | | | | | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| | | | | | | | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

8. „**Az Enigma főbb típusai**” című rész szövegét alakítsa 6 oszlopos és 18 soros táblázattá! A táblázatot kívül dupla, belül szimpla vonallal szegélyezze, az első sorát pedig emelje ki félkövér betűkkel!
9. A „**Használata**” című részben az „**Üzenetküldés vagy -fogadás előtt...**” kezdetű bekezdést követő öt bekezdést alakítsa felsorolássá, a felsorolást jelző szimbólum a „+” műveleti jel legyen! Ennek a résznek az utolsó bekezdésében szereplő kitevőket tegye felső indexbe!

Használata

A német katonák az Enigmával – változó beállítással – több különböző hálózaton végeztek rádióforgalmazást. (Ezeket a hálózatokat a kódtörő Bletchley Park kutatói többek között a „Red”, „Chaffinch” és a „Shark” névvel illették.) A forgalmazónak rendelkezésére állt az adott időszakra érvényes Enigma-kód. Az üzenetek megfelelő kódolásához és deszifrázásához mindkét félnek azonos módon kellett az Enigmát beállítania: egyforma tárcsákat kellett ugyanabban a sorrendben és megegyező kezdeti helyzetben használniuk, és ugyanazokat a betűket kellett felcserélniük a kapocstáblán. A beállításokat előre meghatározták és kódkönyvekben rögzítették.

Üzenetküldés vagy -fogadás előtt az alábbi beállítások voltak elvégzendők az Enigmán:

- + a tárcsák kiválasztása és sorrendje (Walzenlage);
- + a tárcsák kezdeti helyzete (a kezelő állította be; minden egyes üzenetnél más és más volt);
- + az ábécé-gyűrűknek a tárcsákhoz viszonyított helyzete (Ringstellung);
- + a kapocstábla-átkötések (Steckerverbindungen);
- + a fordító beállításai (csak a nagyon késői változatoknál).

Az Enigmát elvileg még akkor sem lehetett feltörni, ha a tárcsák huzalozását az ellenség ismeri. (A németek nagy erőfeszítéseket tettek a tárcsahuzalozás titokban tartására.) A huzalozás ismerete nélkül a lehetséges kombinációk száma 10^{114} (nagyjából 2^{380} bit). A huzalozás – és egyéb operatív megkötések – ismeretében ez a szám 10^{23} (2^{76} bit). Az Enigma tervezői a kombinációk csillagászati száma miatt bíztak a rendszer feltörhetetlenségében. Abban az időben a kód nyers erővel – minden egyes kombináció kipróbálásával – való feltörése kivitelezhetetlen volt.

10. Helyezze el az első oldal felső részére – a mintának megfelelően – jobbra igazítva az *eni1.jpg* képet az oldalarányok megtartásával 6 cm szélesre átméretezve! A kép és a szöveg távolsága a kép bal oldalán legyen 5 mm! A kép alatt hozza létre középre zártan az „**Az Enigma**” ábraszöveget!
11. Illessze be az *eni2.png* képet a „**Tárcsák**” című rész utolsó bekezdése után egy üres bekezdésbe az oldalarányok megtartásával a szöveg teljes szélességében! Helyezze el az ábra középső részén – a mintának megfelelően – a *nyil.png* képet az oldalarányok megtartásával 2 cm magasra átméretezve! Illessze be mellette 9 pontos betűkkel „**A jobb oldali tárcsa egyet lép**” szöveget úgy, hogy az ne takarjon az ábrából alakzatot, vagy alakzat egy részét sem!
12. A dokumentum élőfejébe szúrjon be oldalszámozást úgy, hogy az a páros oldalakon balra, a páratlan oldalakon jobbra zártan helyezkedjen el! Az élőfej alá helyezzen el a szöveg teljes szélességében egy vízszintes vonalat! Az első oldalon az élőfej maradjon üres!
13. A dokumentum végére illesszen be egy új oldalt, és írja a tetejére a „**Tartalomjegyzék**” szöveget, amelyet formázzon meg *Címsor 2* stílussal! Szúrjon be alá – a szövegszerkesztő program eszközeinek felhasználásával – egy tartalomjegyzéket a mintának megfelelően!

30 pont

A feladathoz a minták a következő oldalakon láthatók.

