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!

1. Hozza létre szövegszerkesztő program segítségével az `enigma` nevű dokumentumot a program alapértelmezett formátumában! Olvassa be a dokumentumba ékezethelyesen az `eniforr.txt` szöveges állomány tartalmát!
2. 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!
3. 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.)
4. 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!
5. 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

6. Hozzon létre egy új bekezdésstílust *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!
7. A főcím utáni első bekezdésben ***(„Az Enigma üzenetek sifrírozására…”)*** 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!

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 desifrírozásához 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.

Minta az Enigma feladathoz:

Az Enigma

Az Enigma üzenetek sifrírozására (titkosítására, kriptográfiai kódolására, rejtjelezésére) és desifrírozására (visszafejtésére) használt német gyártmányú, forgótárcsás, elektromechanikus berendezés.*

Fejlesztése és története

Az Enigma nem egyetlenegy berendezés volt, hanem számos modellből álló termékcsalád. Az első Enigma gépeket kereskedelmi célokra készítették az 1920-as évek elején. Az 1920-as évek közepétől a német haderő különféle fegyvernemei is használni kezdték, és a biztonság növelésére több változtatást is végrehajtottak. Más országok is használták vagy az Enigmát, vagy az Enigma alapján tervezett saját titkosító gépüket.

Az Enigma

A kereskedelmi Enigma

1918. február 23-án Arthur Scherbius német mérnök egy forgótárcsás titkosító gépre jegyzett be szabadalmat, és E. Richard Ritterrel együtt megalapította a Scherbius & Ritter céget. A találmánnyal megkeresték a német haditengerészetet és a külügyminisztériumot, de egyiket sem érdekelte a dolog. A szabadalmi jogokat átruházták a Gewerkschaft Securitasra, amely 1923. július 9-én megalapította a Chiffriermaschinen Aktien-Gesselschaftot (Sifrírozógép Részvénytársaság). Scherbius és Ritter a cég igazgatótanácsába kerültek.

A Chiffriermaschinen AG az Egyetemes Postaegyesület 1923-as és 1924-es kongresszusán is kiállította a tárcsás sifrírozógépét, az Enigma A-t. Ez az írógéppel felszerelt első változat nehéz és ormótlan volt: 65×45×35 centiméter, közel 50 kilogramm. A B modell is hasonlóan nézett ki. Bár mindkettőt Enigmának hívták, az A és a B modell nem sokban hasonlított a későbbiekre: nem csak nagyobbak és nehezebbek voltak, de kriptográfiai szempontból is eltértek, mivel nem volt bennük fordító.

A fordító ötletét Willi Korn, Scherbius egyik kollégája vetette fel, és az 1926-ban megjelent Enigma C-t már fordítóval is felszerelték. A fordító az Enigma gépek egyik kulcsfontosságú alkatrésze.

Az Enigma C az elődjeinek kisebb méretű és könnyebben hordozható változata volt. A súly csökkentése érdekében már nem rendelkezett írógéppel – az operátor az Enigma-művelet utáni betűket kis lámpákból olvasta ki. Az A, B és C modellek az Enigma D 1927-es megjelenésével hamar eltűntek. A D modell átütő kereskedelmi sikert aratott, többek között használták Svédországban, Hollandiában, az Egyesült Királyságban, Japánban, Olaszországban, Spanyolországban, az Egyesült Államokban és Lengyelországban.

A katonai Enigma

A német fegyveres erők közül elsőként a haditengerészet vezette be az Enigmát. A Funkschlüssel C nevet kapott rendszert 1925-ben kezdték el gyártani, és a következő évben rendszeresítették.

1928. július 15-ére a német hadsereg, a Reichswehr hadrendbe állította a saját Enigma-változatát, az Enigma G-t – ezt 1930 júniusában Enigma I-re nevezték át. Emellett az Enigma I-et még Wehrmacht-Enigmaként is ismert volt, a hadseregen kívül számos egyéb katonai és polgári szervezet használta – többek között például a német vasút, a Deutsche Reichsbahn. Az Enigma I és a kereskedelmi Enigma közötti lényeges különbség a

* Az „Enigma" szó a görög αἴνιγμα szóból ered, melynek jelentése: rejtély, rejtvény.

kapocstáblában rejlett, mivel a be
mérete 28×34×15 centiméter volt,

Más országok is bevezették az Eni
spanyol polgárháború alatt a spany
brit kódfejtők. A svájciak a keres
diplomáciai célokra. Ezt a kódot
Nagy-Britannia és az USA. A japár
K japán használatra módosított vál

Becslések szerint több mint 100000
még biztonságosnak hitt Enigmáka

Az Enigma főbb típusai

Modell	Év				
Enigma I.	1930				
Enigma II.	1932				
Enigma A.	1923				
Enigma B.	1924				
Enigma C.	1926				
Enigma D.	1927				
Enigma G.	1936				
Enigma K.	1938				
Enigma M.	1934				
Enigma M1.	1934				
Enigma M2.	1938				
Enigma M3.	1939				
Enigma M4.	1942				
Enigma M5.	(1945)				
Enigma M10.	(1945)	4 a 12-ből	23760	2 rögzített	választható
Enigma T.	1942	3 a 8-ból	336	1 cserélhető	5
Enigma Z.	1931	3 a 3-ból	6	1 cserélhető	1

Részei

Az Enigma forgótárcsás rejtjelező gép, amely a sifrírozáshoz mechanikus és elektromos elemeket egyaránt használ. A berendezés mechanikus része egy alfanumerikus billentyűzetből, néhány, közös tengelyen forgó tárcsából, valamint egy, a billentyűk leütésével működtetett tárcsaléptető mechanizmusból áll.

Működése

Maga a mechanizmus modellről modellre változott: a jobb oldali tárcsa minden egyes leütés után egyet lépett, míg a többi tárcsa adott leütésenként lépett csak egy-egyet. Az egymáshoz képest eltérően elforduló tárcsák hatására az egyes leütésekkel sifrírozott betű mindig más-más lett. Egy billentyű leütésekor az akkumulátorból

Minta az Enigma feladathoz:

áram folyt át a kapocstáblán, ahol – a billentyűzet és a tárcsa között – további betűcserét lehetett végrehajtani. A Wehrmacht Enigmájában három, a Kriegsmarine és az Abwehr Enigmájában négy forgótárcsa volt, amelyeken az áram eljutott a tárcsák végén található fordítóhoz. A fordító egy teljesen más úton küldte vissza az áramot újra a tárcsákon, valamint egy esetleges másik kapocstábla átkötésén át a sifrírozott betű lámpájáig.

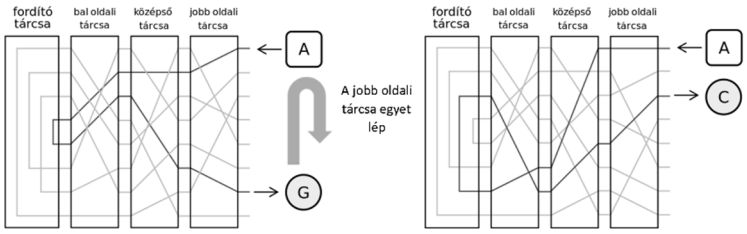
Az állandóan elforduló tárcsák miatt az Enigma polialfabetikus rejtjelet hozott létre: ez lényegesen megnövelte az Enigma-kód biztonságát.

Tárcsák

A tárcsák adták az Enigma gép jelentőségét. Mindegyik tárcsa egy nagyjából 10 cm átmérőjű keménygumi (ebonit) vagy bakelit korong volt, amelynek egyik oldalán rugós bronz tüskék, a másikon pedig ugyanannyi elektromos érintkező kapott helyet. A tüskék és az érintkezők az ábécé betűinek feleltek meg (rendszerint 26 betűnek, A-tól Z-ig). A tárcsákat egy közös tengelyre helyezték úgy, hogy az egyik tárcsa tüskéi hozzáérjenek a szomszédos tárcsa érintkezőihez. Ily módon létrejött az áramkör. Magán a tárcsán belül egy kábelkorbács 26 ere kapcsolta az egyik oldal tüskéit a másik oldal érintkezőihez. A tárcsákat általában római számokkal azonosították, és az összes azonos számú tárcsa ugyanúgy volt behuzalozva.

Önmagában egy tárcsa csupán egy egyszerű helyettesítő rejtjelet állít elő: egy betűt kicserél egy másikra. Az E betű tüskéje egy adott tárcsán például megfelelhetett a T betű érintkezőjének. Az Enigma összetettségét és kriptográfiai nehézségét a több tárcsa egyidejű használata, valamint az egyes tárcsák egymáshoz képest eltérő elfordítása adta, így polialfabetikus helyettesítő rejtjel jött létre.

Egy Enigmába minden egyes tárcsát 26 különböző helyzetben lehetett behelyezni. Behelyezése után a tárcsát egy forgatókoronggal kézzel tovább lehetett léptetni. Mindegyik tárcsa peremére felvittek egy „ábécé-gyűrűt", amelyből mindenkor csak egy betű látszott az Enigma fedelén vágott nyílásban, így a kezelő ismerte a tárcsa pozícióját. A korai Enigma modelleknél az ábécé-gyűrűt a tárcsához rögzítették, néhány későbbi modellnél még ezt is el lehetett forgatni. A gyűrű beállítását a Ringstellung adta meg, és többek között ezt is be kellett állítani az Enigma használata előtt.



Léptetés

A léptetéshez egy kilincsműves megoldást használtak. Minden egyes tárcsának 26 foga volt, amik minden leütésnél megpróbáltak elfordulni. A második és harmadik tárcsán a továbbléptető kilincs beakadását egy fémlemez akadályozta meg, így az
Az első tárcsán ilyen lemez nem v

Három tárcsa – és az első és máso
leütésenként ismételte önmagát (
üzenetek általában csak néhány
üzeneten belül kétszer forduljon el

Fordító

A korai „A" és „B" modellek kivé
az egyik érintkezőjén beérkező jel

Tartalomjegyzék

Az Enigma 1
Fejlesztése és története 1
A kereskedelmi Enigma 1
A katonai Enigma 1
Az Enigma főbb típusai 2
Részei 2
Működése 2
Tárcsák 3
Léptetés 3
Fordító 3
Kapocstábla 4
Tartozékok 4
Használata 4
Feltörése 4
Lengyel titkosszolgálat 4
Bletchley Park 5
A Colossus 5
Tartalomjegyzék 7