Enigma 20 pont

Ebben a feladatban egy weboldalt kell készítenie az Enigma bemutatására a feladatleírás és a minta szerint. Ehhez következő fájlokat kell felhasználnia: `eniforras.txt`, `enitabla.txt` és `enigma.css` UTF-8 kódolású szöveges állományt, valamint az `eni.jpg`, `eni2.png` és a `fel.ico` nevű képeket. Ahol a feladat másként nem kéri, a formázási beállításokat az `enigma.css` stílusállományban végezze el!

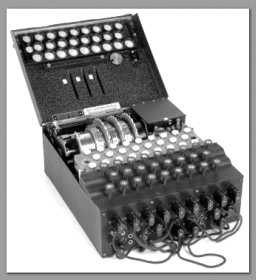
1. Hozzon létre HTML oldalt `enigma.html` néven! Állítsa be az oldal nyelvét magyarra és a kódolását UTF-8-ra! A böngésző címsorában megjelenő cím *„Enigma”* legyen! A weboldal fejrészében helyezzen el hivatkozást az `enigma.css` stíluslapra!
2. Az oldal törzsébe másolja be az `eniforr.txt` állomány tartalmát! Az `enitabla.txt` szövegben a weboldalon található táblázat kódját találja. Illessze be a kódot a megfelelő helyre!
3. Alakítsa ki a címet, alcímeket a minta szerint! A weboldal címe *(„Az Enigma”)* 1-es szintű címsor, az alcímek *(„Fejlesztése és története”, „Részei”, „Használata”)* 2-es szintű címsor és azok alcímei *(„A kereskedelmi Enigma”, „A katonai Enigma”, „Az Enigma főbb típusai”, „Működése”)* 3-as szintű címsorok legyenek!
4. Szúrjon be vonalakat a mintán látható helyekre! Alakítsa ki a szöveg bekezdéseit a minta szerint!
5. Az első bekezdést lássa el `meghatarozas` nevű azonosítóval! Az *„Enigma”* szót tegye `<span></span>` tag-ek közé! A tag-hez adjon hozzá `kiemelt` nevű osztálykijelölőt! Ha a szó fölé visszük az egeret, akkor jelenjen meg az *"Az 'Enigma' szó a görög αίνιγμα szóból ered, melynek jelentése: rejtély, rejtvény."* szöveg!
6. A *„Fejlesztése és története”* cím alatti bekezdésbe helyezze el az `eni.jpg` képet, és lássa el `jobbkep` osztálykijelölővel! Az egérrel a kép fölé állva jelenjen meg az *„Enigma”* szöveg!
7. A táblázat alá, és a dokumentum legvégére illessze be az `fel.ico` képet! Alakítsa a nyilakat linkké, amelyek visszamutatnak az oldal tetejére!
8. A megfelelő helyre egy külön bekezdésbe illessze be az `eni2.png` képet a minta alapján! A bekezdést a `kozep` nevű osztálykijelölővel formázza!
9. A dokumentum végén a forrásoldal hivatkozásának címét tartalmazó szöveget is helyezze egy bekezdésbe, amelyet lásson el `forras` osztálykijelölővel! Alakítsa linkké a forrásként megadott webcímet, amely új ablakban nyíljon meg!
10. A következő beállításokat, módosításokat az `enigma.css` stíluslapon végezze el!
    a. A weboldal háttérszínét állítsa #669966 színkódra, a szöveg színét pedig #FFFFCC színkódra!
    b. A táblázat szélessége 80% legyen!
    c. Hozzon létre osztálykijelölőt `kiemelt` néven, és a szöveg színét állítsa #00CC00 színkódra!
    d. Minden képet #FFFFFF színkódú 2 pont vastagságú folytonos vonal keretezzen!
    e. a `meghatarozas` nevű azonosítójelölő részben a szöveget állítsa dőltre!

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.

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 kapocstáblában rejlett, mivel a betűcseréléssel lényegesen megnövekedett a gép kriptográfiai ereje. A gép mérete 28×34×15 centiméter volt, tömege 12 kilogramm.

Más országok is bevezett
polgárháború alatt a spar
svájciak a kereskedelmi E
számos ország megfejtett
készült az Enigma T („Tirp

Becslések szerint több m
biztonságosnak hitt Enigm

Az Enigma főbb típu

Modell
Enigma I.
Enigma II.

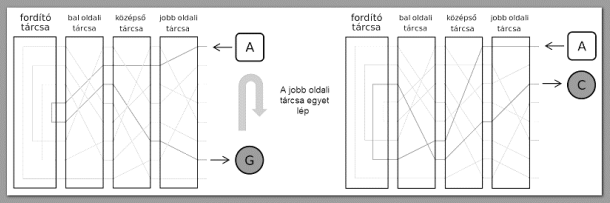
Enigma M10.	(1945)	4 a 12-ből	23760	2 rögzített	választható
Enigma T.	1942	3 a 8-ból	336	1 cserélhető	5
Enigma Z.	1931	3 a 3-ból	6	1 cserélhető	1

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 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.



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 10114 (nagyjából 2380 bit). A huzalozás – és egyéb operatív megkötések – ismeretében ez a szám 1023 (276 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.

Forrás: https://hu.wikipedia.org/wiki/Enigma_(gép)