# Az Enigma

Az Enigma[[1]](#footnote-1)\* 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.

Az Enigma

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 bevezették az Enigmát. Az olasz haditengerészet a kereskedelmi Enigmát vette meg, ahogy a spanyol polgárháború alatt a spanyol haditengerészet is. Ezeket a kapocstábla nélküli változatokat feltörték a brit kódfejtők. A svájciak a kereskedelmi Enigma D-hez sokban hasonló K modellt használták katonai és diplomáciai célokra. Ezt a kódot számos ország megfejtette, többek között Lengyelország, Franciaország, Nagy-Britannia és az USA. A japánok számára készült az Enigma T („Tirpitz”), amely a kereskedelmi Enigma K japán használatra módosított változata.

Becslések szerint több mint 100000 Enigma gép készült. A második világháború után a szövetségesek az akkor még biztonságosnak hitt Enigmákat számos fejlődő országnak adták el.

### Az Enigma főbb típusai

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Modell** | **Év** | **Tárcsák** | **Helyzetek** | **Fordító** | **Vágatok** |
| Enigma I. | 1930 | 3 a 3 (5)-ból | 6 (60) | 1 (3) rögzített | 1 |
| Enigma II. | 1932 | 3 a 3-ból | 6 | 1 rögzített | 1 |
| Enigma A. | 1923 | 4 (8) | 1 | nincs | hajtott |
| Enigma B. | 1924 | 2×4 | 1 | nincs | hajtott |
| Enigma C. | 1926 | 3 | 1 | 1 rögzített | 1 |
| Enigma D. | 1927 | 3 | 1 | 1 cserélhető | 1 |
| Enigma G. | 1936 | 3 a 3-ból | 6 | forgó | 11, 15, 17 |
| Enigma K. | 1938 | 3 a 3-ból | 6 | 1 rögzített | 1 |
| Enigma M. | 1934 | 3 az 5-ből | 60 | 1 rögzített | 1 |
| Enigma M1. | 1934 | 3 a 6-ból | 120 | 1 rögzített | 1 (2) |
| Enigma M2. | 1938 | 3 a 7-ből | 210 | 1 rögzített | 1 (2) |
| Enigma M3. | 1939 | 3 a 8-ból | 336 | 1 rögzített | 1 (2) |
| Enigma M4. | 1942 | 4 a 8+2-ből | 1344 | 2 cserélhető | 1 (2) |
| Enigma M5. | (1945) | 4 a 12-ből | 23760 | 2 rögzített | választható |
| 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.

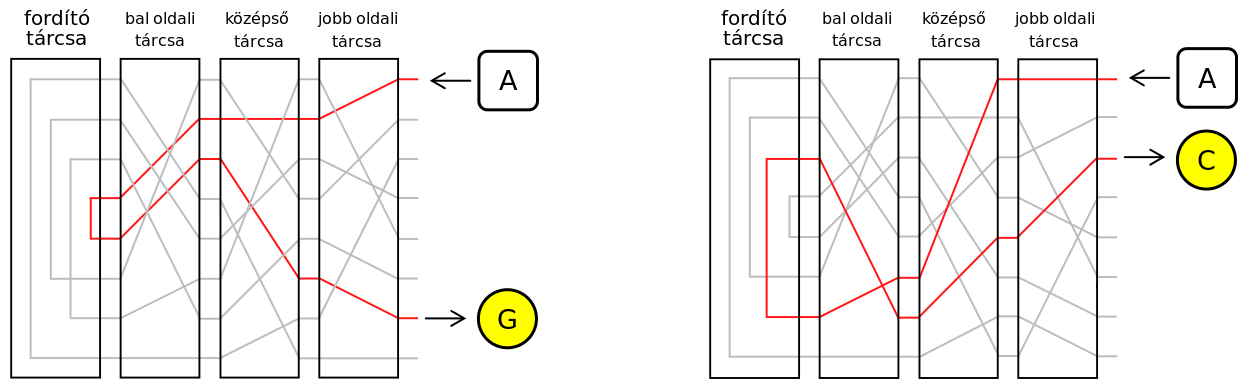
Az állandóan elforduló tárcsák miatt az Enigma polialfabetikus rejtjelet hozott létre: ez lényegesen megnövelte az Enigma-kód biztonságát.

### 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.



A jobb oldali tárcsa egyet lép

### 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 azok nem minden leütésnél fordultak el, csak amikor a lemez nem volt útban. Az első tárcsán ilyen lemez nem volt, így az minden leütésnél elfordult.

Három tárcsa – és az első és második tárcsánál egy továbbléptető bevágás – esetén a gép 26×25×26 = 16900 leütésenként ismételte önmagát (a kettős léptetés miatt 25 a középső tárcsa állásainak száma). Mivel az üzenetek általában csak néhány száz betűből álltak, nem volt arra esély, hogy ugyanaz a tárcsaállás egy üzeneten belül kétszer forduljon elő, ezért a helyettesítő rejtjel megoldásait itt nem lehetett alkalmazni.

### Fordító

A korai „A” és „B” modellek kivételével az utolsó tárcsa a fordítóhoz (Umkehrwalze) csatlakozott. A fordító az egyik érintkezőjén beérkező jelet egy másik érintkezőjén vezette vissza a tárcsákba. A fordító segítségével a titkosítás kétirányúvá vált: a nyílt szöveget beírva kapható a titkosított szöveg, a titkosított szöveg beírásával pedig újra a nyílt szöveg. A fordító használata miatt egyetlen betű sem egyezett meg sifrírozott változatával. Erre támaszkodva törték fel később a kódot.

### Kapocstábla

A kapocstábla hüvelyeit összekötő kábellel betűpárokat lehetett felcserélni, például az E-t és a Q-t. A csere a tárcsás titkosítás előtt és után is megtörtént. Átlagosan tíz betűpárt cseréltek fel. A kapocstábla felső sorában a billentyűzet, az alsó sorában az első tárcsa hüvelysora helyezkedett el, és ezek összekötésével lehetett a betűcseréket elvégezni.

### Tartozékok

Az M4 Enigmához készült egy írógép. A Schreibmax egy vékony papírcsíkra 26 betűt nyomtatott, így nem volt szükség második kezelőre, aki korábban az Enigmán felvillanó fényekhez tartozó betűket vetette papírra. A Schreibmaxot az Enigma tetejére kellett helyezni, és a lámpák helyére csatlakozott. Felszereléséhez le kellett venni a lámpák burkolatát és kicsavarni az összes égőt. A kényelmi szempont mellett operatív haszna is volt: az írógépet úgy is el lehetett helyezni, hogy az Enigma kezelője ne lássa a desifrírozott, nyílt szöveget.

## 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.

## Feltörése

Az Enigmát használói abszolút biztonságosnak tartották, mivelhogy a géppel gyártott szövegek kézi erővel megfejthetetlenek voltak az 1918 előtt használt kódokkal ellentétben. Nem számoltak azonban azzal, hogy a gép által generált titkos szöveget egy másik gép segítségével meg lehet fejteni.

### Lengyel titkosszolgálat

1932-ben a Franciaországnak kémkedő német Hans-Thilo Schmidt átadta a francia kriptográfusoknak, és később Gustave Bertrand tábornoknak a szeptemberi és októberi kulcstáblát, a használati utasítást (H.Dv.g.13 = Heeres-Dienstvorschrift, geheim, Nr.13) és kulcsvezetést (H.Dv.g.14). Akkoriban még csak három tárcsa volt beépítve, és a tárcsák beállítását negyedévenként változtatták. Csak 1936-tól tértek át a napi beállításra. A francia titkosszolgálat továbbította az információkat a lengyeleknek és az angoloknak.

Az Enigma feltörhetetlennek tartott kódolását az angolok és a franciák kudarcai után először a lengyel Marian Rejewski által vezetett, kriptográfusokból és más matematikusokból álló csoport törte fel 1932-ben. Ehhez a kereskedelmi Enigma D modelljét használta fel, aminek betűsorrendje megegyezett a forgalomban levő német írógépekkel. Rejewski megtalálta a hadsereg által használt huzalozási sorrendet, ami az angol Dillwyn „Dilly” Knoxnak is gondot okozott még 1939-ben is. Emellett Rejewski a permutációkról való szakértelmét bevetve a három tárcsa és a fordító huzalozását is kitalálta.

Emellett még a tárcsák beállítását és helyzetét is ki kellett találni. Ehhez Rejewski és társai, Jerzy Różycki és Henryk Zygalski a németek egy eljárási hibáját használta fel: kétszer küldték el az üzenet elején a három betűs kulcsot rejtjelezve. Ezért a nyílt szövegben megegyezett az első és a negyedik, a második és az ötödik, a harmadik és a hatodik betű. Az erre a célra épített gépekkel, a ciklométerrel és a „bombával” minden lehetséges állást kipróbáltak erre a hat betűre. Ezzel nagy mértékben csökkentették a kulcsra vonatkozó bizonytalanságot. Több adás lehallgatásával a konkrét kulcsot is megtalálták.

### Bletchley Park

Miután a németek 1938. szeptember 15-én megváltoztatták az eljárást, és három hónappal később bevezették az öttárcsás gépet, a lengyelek már nem tudták megfejteni az üzeneteket, és az Enigma újra biztonságos volt. A fenyegető veszélyt látva összes tudásukat átadták szövetségeseiknek még hazájuk lerohanása előtt.

A lengyelek munkája alapján a későbbi változatokat a Bletchley Parkban állomásozó szövetséges csoport törte fel. A csoport a lengyelektől megtudott fontos információk, különösen a huzalozásokról való tudás birtokában a tízezer, majd tizennégyezer férfi és nő, az úgynevezett Turing-bomba segítségével és Alan Turing vezetésével végezte ezt a fontos munkát. Turingnak az az ötlete támadt, hogy a kapocstáblát több, legtöbbször tizenkét tárcsával szimulálja. Ezzel nagymértékben tudta csökkenteni a több mint 200 trilliárd lehetőséget.

A Turing-bomba a lengyel „bomba” továbbfejlesztése, egy elektromechanikus számítógép. Ha el lehet tekinteni a kapocstáblától és a tárcsák beállításától, akkor már csak 1 054 560 lehetőséget kell átvizsgálni. Ez kézzel még mindig reménytelen, de a Turing-bomba motorja 120-at fordult percenkét, és minden fordulattal 26 lehetőséget vizsgált át, így egy Turing-bomba 1 054 560/(26×120) perc alatt végzett az összes lehetőséggel. Ez kerekítve hat óra. Hatvan Turing-bombával ez az idő hat percre rövidült. Valójában a háború végéig csak Nagy-Britanniában 210 Turing-bombát üzemeltettek. Az átlagosnál sokkal gyakrabban előforduló szavak (angolul cribs) különleges fontossággal bírtak a Turing-bombák használatában. Ehhez segítségükre volt az, hogy a katonai üzeneteket sztereotípen fogalmazták, és gyakoriak voltak az olyan kifejezések, mint például az „OBERKOMMANDODERWEHRMACHT” („A haderő főparancsnoksága”). Profitáltak a rutinszerű üzenetekből, például a mindig ugyanonnan, ugyanabban az időpontban sugárzott üzenetekből. Az egyik helyről érkező időjárás-jelentések a: „WETTERVORHERSAGEBEREICHSIEBEN” szavakkal kezdődtek. Ezek a jelentések ugyanolyanok voltak az angolok számára, mintha a németek a napi kulcsot adták volna a tudtukra. Az angolok később provokálták is ezeket az üzeneteket, és az ismert tartalmú választ használták fel. Ezt nevezték „gardening”-nek (kertészkedés). Így 1940-től kezdve a világháború végéig a legtöbb német üzenetet meg tudták fejteni. 1943-ban havonta 80 000 üzenetet törtek fel; ez mintegy napi 2500 üzenet.

### A Colossus

A Colossus számítógépek elektronikus úton működő első példánya 1943 végére készült el. Lényege annyi volt, hogy a németek által kódolt információkat egyszerűen minden létező kombinációban megpróbálták visszafejteni („nyers erő” módszer). A 1054560 lehetőség átvizsgálásával a Colossus másodpercenkénti 25000 karakteres sebességével 1054560/25000=42,18 másodperc alatt végzett. Összesen tíz darab készült. A gépeket és leírásaikat megsemmisítették a háború után, egyetlen leírás maradt fenn, amelynek titkosságát csak 2000(!) szeptemberében oldotta fel a brit kormány.

A németek által forgalmazott hatalmas mennyiségű titkosított üzenetekből nem mindet sikerült megfejteni (néhányat a mai napig nem), de az így nyert, a britektől ULTRA kódnevet kapott hírszerzési információknak köszönhetően a szövetségesek a háborúban jelentős előnyhöz jutottak.

A lengyel ciklométer és a „bomba” egyszerű mechanikus szerkezet volt. (A „bomba” nevet az időzítőhöz hasonló ketyegéséről kapta.) A német üzenetkezdés hibáját használták ki, mivel ismerték az első hat betű összefüggését. Az angol és később az amerikai Turing-bomba már algoritmus szerint dolgozott, és elektromechanikus számítógépként működött. Ezek a gépek már logikai függvényeket használtak. Ezen túlmenően alapvető különbség még a gépek sebességében volt. A Colossus elektronikus elven működő, programozható, digitális számítógép volt, Turing algoritmusát felhasználva és továbbfejlesztve építették meg.

## Tartalomjegyzék

[Az Enigma 1](#_Toc501737801)

[Fejlesztése és története 1](#_Toc501737802)

[A kereskedelmi Enigma 1](#_Toc501737803)

[A katonai Enigma 1](#_Toc501737804)

[Az Enigma főbb típusai 2](#_Toc501737805)

[Részei 2](#_Toc501737806)

[Működése 2](#_Toc501737807)

[Tárcsák 3](#_Toc501737808)

[Léptetés 3](#_Toc501737809)

[Fordító 3](#_Toc501737810)

[Kapocstábla 4](#_Toc501737811)

[Tartozékok 4](#_Toc501737812)

[Használata 4](#_Toc501737813)

[Feltörése 4](#_Toc501737814)

[Lengyel titkosszolgálat 4](#_Toc501737815)

[Bletchley Park 5](#_Toc501737816)

[A Colossus 5](#_Toc501737817)

[Tartalomjegyzék 7](#_Toc501737818)

1. \* Az „Enigma” szó a görög αίνιγμα szóból ered, melynek jelentése: rejtély, rejtvény. [↑](#footnote-ref-1)