

LUCY &  
STEPHEN HAWKING



**GEORGE**

◀ ÉS A ▶

**FELTÖRHETETLEN KÓD**

**George és Annie elhagyják a Földet,  
hogy megmentsek a világegyetemet!**

LUCY &  
STEPHEN HAWKING



**GEORGE**  
**< ÉS A >**  
**FELTÖRHETETLEN KÓD**

***GARRY PARSONS ILLUSZTRÁCIÓIVAL***

Első kiadás 2022

**Könyvmolyképző Kiadó**

## A LEGÚJABB TUDOMÁNYOS ELMÉLETEK!

A történet során több érdekes írást is olvashatsz a tudományról. Ezeknek a tanulmányoknak a segítségével még jobban megértheted a könyvben érintett témaköröket.

Az alábbi híres tudósok írásait olvashatod:

### **Az én robotjaim, a te robotjaid . . . . . 56**

Prof. Peter W. McOwan  
Londoni Queen Mary Egyetem

### **Az élet története . . . . . 77**

Prof. Michael J. Reiss  
Oktatási Intézet, Londoni Egyetem

### **Kvantumszámítógépek . . . . . 122**

Dr. Raymond Laflamme  
Igazgató, Kvantumszámítási Intézet, Waterloo Egyetem

### **Az élet építőkövei . . . . . 145**

Dr. Toby Blench  
Kutatókémikus

### **3D nyomtatás . . . . . 216**

Dr. Tim Prestidge  
Totempole Consulting

### **Élet az univerzumban . . . . . 262**

Prof. Stephen Hawking  
Igazgató, Elméleti Kozmológiai Intézet, Cambridge-i Egyetem

A további anyagokért köszönet:

Dr. Stuart Rankinnek (Nagy Teljesítményű Számítástechnikai Szolgáltató Részleg, Cambridge-i Egyetem)



**E**gy másik bolygón remekül meg lehetett volna figyelni a csillagokat a faházikóból. Például egy olyan bolygón, ahol nincsenek szülők.

A faház a zöldségültetvény közepén álló almafa ágaira épült, és egy George-hoz hasonló fiú számára éppen tökéletes magasságban, helyszínen és szögben tette lehetővé az egész éjszakai csillagnézegetést. Szülei azonban mást találtak ki neki: házimunkát kellett végeznie, leckét írnia, aludnia, vacsoráznia, vagy „minőségi időt” töltenie ikerhúgaival. George-ot egyik tevékenység sem hozta lázba.

Egyetlen dolog érdekelte: hogy lefényképezhesse a Szaturnuszt. Egyetlen apró képet szeretett volna készíteni kedvenc bolygójáról, erről a hatalmas, jégből és porból álló, gyűrűkkel övezett, fagyott gázóriásról. Az évnek ebben a szakaszában azonban későn megy le a nap, és a Szaturnusz csak nem sokkal éjfél előtt válik láthatóvá az éjszakai égbolton. George-nak már ennél sokkal korábban ágyban kellett lennie. A szülei nem engednék meg, hogy éjfélig maradjon a faházikóban.

George a lábát lógatva ült a fapadló szélén. Sóhajtván próbálta kiszámolni, hány óra és nap múlva csinálhatja végre azt, amit akar.

– Mizu? – szakította félbe gondolatait egy vékony alak, aki éppen akkor kapaszkodott fel a faházikóba. Hosszú, bő, terepmintás nadrágot, kapucnis pulóvert és baseballsapkát viselt.

– Juhú! – vidult fel rögtön George. – Szia, Annie!

Annie azóta volt a legjobb barátja, hogy a lány családja néhány éve Foxbridge-be költözött. Annie a szomszédjukban lakott, de nem csak ezért voltak jó barátok. George bírta a lányt. Annie apukája tudós volt, Annie maga pedig vicces, okos, menő és bátor. Semmitől sem ijedt meg: egyetlen kalandra se mondott nemet, minden elméletet ellenőrizni akart, és minden állítást megkérdőjelezett.

– Mit csinálsz? – kérdezte George-tól.

– Semmit – mormolta a fiú. – Csak várakozom.

– Mire?

– Hogy történjen valami – mondta George szomorúan.

– Azt én is várom – értett egyet Annie. – Szerinted most, hogy már nem mehetünk úrkalandokra, elfeledkezett rólunk a világ-egyetem?

– Szerinted repülünk valaha megint az űrben? – sóhajtott fel George.

– Most biztosan nem – rázta a fejét Annie. – Lehet, hogy már eleget bolondoztunk. Tizenegy évesek vagyunk, most már mindig komolynak kell lennünk!

George felállt, érezte, hogy talpa alatt enyhén meghajlik a deszka. Majdnem biztos volt benne, hogy a faház biztonságos. Nagyon kevés az esély rá, hogy beszakad alattuk a padló, és Annie-vel együtt lezúgnak a mélybe. George és apja, Terence együtt építették a házat a helyi szeméttelpről megmentett fadarabokból. Egyszer, amikor apjával együtt azt a házrészét készítették, ahol most ő és Annie ültek, apja lába alatt összetört az egyik elkorhadt deszka. Szerencsére nem esett le a földre, de George-nak minden

erejére szüksége volt, hogy visszarángassa a padlóra. Odalenn, a földön ikerhúgai, Juno és Hera gurultak a nevetéstől.

A kis baleset után arra jutottak a szülei, hogy a faház nem biztonságos a kislányok számára, ezért nekik tilos volt felmászniuk a kötélhágcsón. George nagyon örült a döntésnek, mert ez azt jelentette, hogy a faház az ő birodalma, oda nem juthat be a családi ház káosza. Szülei szigorúan meghagyták, hogy mindig húzza fel maga után a létrát, nehogy bizonyos aprónépek utána mászszanak, csak hogy imádott bátyjukkal lehessenek. George nagyon ügyelt a biztonságra, sosem hagyta leengedve a létrát.

Ami azt is jelentette, hogy...

– Hé, te meg hogy másztál fel ide? – döbbsent rá hirtelen, hogy Annie-nek sem kellene itt lennie.

A lány elvigyorodott.

– Kisbaba koromban megcsípett egy pók! Csak most kezdem kiaknázni mágikus szupererőmet! – felelte színpadiasan.

George a legvastagabb ágon áthurkolt, csomózott kötéltre mutatott.

– Azt te csináltad?

– Igen – mondta Annie, most már normális hangon. – Kíváncsi voltam, fel tudok-e mászni.

– Neked leengedtem volna a létrát!

– Amikor utoljára kértelek, hogy engedj fel,



milliónyi jelszót kértél, és a végén még a fél Kit Katemet is neked kellett adnom!

– Az nem is Kit Kat volt! – emlékeztette George, és felemelte az ujjait, hogy idézőjelet imitáljon. – Csak egy darab „csokoládé”, amit a laborban próbáltál összehozni, aztán Kit Kat-papírba csomagoltad, mert kíváncsi voltál, kiszúrom-e a különbséget!

– Ha egy egér hátán lehet fület növeszteni, én miért ne tudnék Kit Katet növeszteni? – vitatkozott Annie. – Biztosan lehetséges olyan csokoládémolekulákat készíteni, amik folyamatosan képesek önmagukat másolni!

Annie bimbózó, lelkesen kísérletező kémikustehetség volt. Gyakran a konyhájukat használta laboratóriumként, amivel nemegyszer kergette örületbe anyját, Susant. Ha Annie anyukája ki akart venni a hűtőből egy doboz almalevet, könnyen egy üvegnyi kristályfehérje-telepre markolhatott.

– Csak hogy tudd, a Kit Katenek olyan íze volt, mint egy dinoszaurusz lábának... – csúfolódott George.

– Nem is! – kiáltott fel Annie. – Igenis finom volt a házi tenyésztésű csokoládém, nem tudom, miről beszélsz! Különbözik is, mikor ettél te dinoszauruszlábat?

– Lábkörmöt – fejezte be George. – Rémes íze van, pont olyan, mintha milliónyi éve fosszilizálódott volna!

– Hahaha! – felelte Annie a szemét forgatva. – Mekkora ínycseri itt valaki!

– Nem is tudod, mit jelent az, hogy ínycseri!

– Dehogynem!

– Akkor hadd halljam! – George biztos volt benne, hogy megnyerte ezt a csatát.

– Olyan, mint az ínycseri meg a nyérc együtt... tudod! – magyarázta Annie. – Totál ínycseri leszel tőle!

Ahogy befejezte, olyan hangos nevetésben tört ki, hogy még a babzsákról is leesett.

– Dilis vagy  
– mondta neki  
kedvesen George.  
– 152 IQ-s dilis.

Annie felva-  
karta magát  
a padlóról.  
A múlt héten  
volt IQ-tesz-  
ten, és véletle-  
nül sem mulasz-  
totta volna el,  
hogy mindenkinek  
az orra alá dörgölje  
az eredményt, aki csak az  
útgába akadt.



Hirtelen észrevette George holmijait.

– Mit keres itt ez a sok vacak?

– Összeszedem a cuccaim – mutatott George a felszerelésre,  
amit húgai apró kezecskéi közül menekít-  
tett ki a faház biztonságába. Ott hevert  
egy mindkét végén fekete karimás,  
fehér, 60 mm-es teleszkóp és egy  
fényképezőgép, amit a teleszkópra  
szeretett volna felszerelni, hogy  
fotózhasson vele. A telesz-  
kópot nagyjától, Mabel-  
től kapta, a fényképezőgépet  
azonban csodálatos módon a  
szeméttelepről mentette ki.  
– Ha besötétedik, lefotózhat-  
nám a Szaturnuszt! Persze csak





ha az unalmas szüleim nem küldenének be a házba... Erről szól az iskolai féléves projektem!

– Király! – Annie a teleszkóp képkeresőjébe hunyorgott, de rögtön fel is kiáltott. – Fúj! Ez ragad!

– Micsoda? – kiáltotta dühösen George, és alaposan szemügyre vette a teleszkópot. Valóban, a képkeresőn valami rózsaszín ragacs éktelenkedett.

– Elegem van ebből! – kiáltotta indulatosan a fiú. Leeresztette a kötélhágcsót, és leászott a házból.

– Hova mész? – kúszott utána Annie. – Nem nagy cucc, le tudjuk takarítani!

George ekkorra azonban már dühtől vöröslő arccal csörtetett a ház felé. Berontott a konyhába, ahol apja éppen Junót és Herát próbálta megteáztatni.

– És egyet apa kedvéért! – mondta Terence Herának, aki kinyitotta a száját, de rögtön vissza is köpte apjára a folyadékot,



majd nevetésben tört ki, kanalával lelkesen csapkodta az etetőszék tálcáját, amitől a tálcán landolt étel föl-le ugrált, mint a rajzfilmekben. Juno, aki mindig utánozta a testvérét, csatlakozott hozzá: kanalával a tálcát csapkodta, ajkával gusztustalan, pukizáshoz hasonló hangot adott ki.

Terence George-ra nézett, arcán kinnal vegyes öröm látszott. Szakálláról zöld trutyi csöpögött, egyenesen házilag varrt ingére.

George mély levegőt vett, és már éppen belekezdett volna a mások holmijait tönkretevő apróságokról szóló monológjába, de Annie éppen időben érkezett.

– Hahó, Mr. G! – mondta vidáman Terence-nek. – Helló, kisbabák!

A kislányok lelkes kanálcsapkodással és gurgulázással köszöntötték az újabb figyelemelterelést a vacsoráról.

– Meg akartam kérdezni, hogy George átjöhet-e hozzánk – csiripelte Annie. Megcsikizte Hera ragadós kis állát, mire a kislány féktelen nevetésben tört ki.

– És a teleszkópom? – morogta mögötte George mérgesen.

– Megoldjuk – felelte Annie halkan, de határozottan, majd ismét az ikrek felé fordult. – Milyen szerencsés vagy, hogy ikerhúgaid vannak! Bárcsak lennének csiklandós testvérkéim! Sajnos én csak egy magányos egyke vagyok...

Szavainak nyomatékot adva, eltúlzottan szomorú fejet vágott.

– Hmpf! – George mit nem adott volna, ha Annie-ék csendes, tudományközpontú, műszaki megszállott háztartásában élhetne, a tudós apjával és az egyre céltudatosabb anyukájával. Ott nem voltak babák, zaj, organikus zöldség és kupleráj – talán csak akkor, amikor Annie a konyhában „kísérletezett”.

– Ööö, persze, mehetsz, de időben gyere haza, hogy elvégezd a feladataidat! – mondta Terence. Megpróbált úgy tenni, mintha ő lenne a család feje.

– Szuper! – kiáltotta Annie lelkesen, és kitolta George-ot az ajtón.

A fiú már tudta: ha Annie-n rajta van a főnökösködés, kár tiltakoznia. Szívesen követte a lányt. Százszor inkább átment volna hozzá, mint hogy a szörnyű otthoni hangulatban üljön.

– Viszlát, Mr. G és kicsi G-k! Éreztétek jól magatokat! – süvöltötte Annie búcsúzól, amikor kiléptek a házból.

– George, ne felejtsd el, hogy csak akkor töltheted ki a jutalomdiagramodat, ha elvégzed a heti feladataidat! – Terence hangja gyengén szólt távolodó, legidősebb gyermeke után. – Még mindig üres a kördiagramod háromötöde!

George azonban ekkorra már messze járt, Annie nyomában sietett a Szomszéd Ház izgalmas világa felé. George szemében az a ház tele volt csúcskategóriás vonalbeli műszaki, tudományos és elektronikus csodákkal.



**A** két kertet elválasztó kerítés egyik lyukán bújtak át, úgy indultak Annie-ék háza felé. A lyuk akkor keletkezett, amikor Mabel nagyfi egy másik ajándéka, Freddy, a malac kitört Greenbyék hátsó kertjéből, hogy szabadulni próbáljon. George Freddy lábnyomait követve találkozott először Annie-vel és a családjával: apjával, Erikkel, a remek kutatóval és sztártudóssal, anyjával, a zenész Susannel, és Kozmosszal, a szuperszámítógéppel, ami akkora teljesítménnyel bírt, és olyan intelligens volt, hogy az univerzum bármely részébe vezető ajtókat tudott készíteni (persze ahhoz, hogy át is menjenek rajta, szkafandert kellett viselniük). George azóta már átutazta a Naprendszer egy üstökösön, járt a Marson, és leszámolt egy gonosz tudóssal is egy távoli naprendszerben. Ki lehetett jelenteni, hogy a találkozás óta minden megváltozott.

– Ne légy már ilyen undok a kishúgaiddal! – szólalt meg Annie menet közben.

– Mi? – George már teljesen megfélemedezett a húgairól. – Miről beszélsz? Nem is voltam undok!

– Csak azért nem, mert időben megállítottalak! – vádolta Annie. – Csupa gonoszságot akartál mondani!

– Mérgező voltam! – méltatlankodott George. – Nem szabad babrálniuk a cuccaimmal, és nem is mászhatnak fel a faházba!

– Szerencsés vagy, hogy egyáltalán van testvéred – mondta Annie szelíden. – Nekem semmim sincs.

– Dehogyanem! – tört ki George. – Annyi mindened van! Ott van Kozmosz, a számítógép, plusz gyakorlatilag saját laborod van, Xboxod, okostelefonod, laptopod, iPodod, iPaded, i-mindened! Van robotkutyád, motoros rollered... Nem t'om... Sok cuccod van!

– Az nem ugyanaz, mintha lenne egy testvérem – mondta hal-  
kan Annie.

– Ha lenne testvéred, tuti nem akarnád, hogy legyen – felelte George kétkedően.

A két barát a kertajtón át lépett be a konyhába.

– Hurrá! – kiáltott Annie, és a hatalmas hűtőhöz lépett, hogy kinyissa.

Belliséknél még a hűtő sem volt szimpla hűtő, inkább laborba illett volna. Hatalmas volt, acélból készült, óriási fiókjaiban és leválasztott fülkéiben sok mindent lehetett elkülönítve tárolni. Természetesen profi gépezet volt, csak annyi köze volt egy hétköznapi hűtőhöz, amennyi egy papírrepülőnek egy úrhajóhoz. George ezt is szerette Annie-ék házában: tele volt váratlan meglepetésekkel és tudományos furcsaságokkal, amiket Erik szerzett be vagy kapott sokéves munkája során.

George irigykedve nézte a különös kék fényvel világító hűtőt. Náluk talán még a legjobb műszaki berendezés sem volt képes olyan feldolgozási teljesítményre, amire Annie-ék hűtője. George eltűnődött ezen a szomorú tényen, de ekkor hangok szűrődtek ki a nappaliból.

– Annie! George! – Annie apja, Erik lépett be a konyhába. Szélesen mosolygott, vastag szemüvege mögött ragyogott a szeme. Nyakkendőjét meglazította, ingujját feltúrte. Kezében két kristály poharat tartott. – Csak újratöltöm a poharakat!

Egy poros, régi üvegért nyúlt. Hangoz pukkanással húzta ki a dugót. Ragacsos, barna folyadékot töltött a poharakba, és már fordult is, hogy visszamenjen a nappaliba.

– Köszönjétek a vendégemnek!  
 – mondta a gyerekeknek, arcán elmélyedtek a nevetőránccok.  
 – Azt hiszem, tudna olyat mondani, ami titeket is érdekelne!

George és Annie azonnal megfélekezett a futó vitáról, és követték Eriket a nappaliba. A szoba tele volt könyvekkel. Csodálatos helyiség volt, tele érdekes tárgyakkal, mint például Erik sárgaréz távcsöve. A nappaliban nem volt annyira látványos a ház többi részét uraló csúcstechnológia: nem annyira hűvös és futurisztikus, mint inkább kényelmes és hívogató volt. A kényelmes kanapén pedig – amit Erik még diákként vett – egy nagyon idős hölgy ült.

– Annie, George, bemutatom Beryl Wilde-ot – mondta Erik, és átadta a hölgynek a pohár sherryjét.





Beryl kecses mozdulattal vette át az italt, és rögtön bele is kortyolt.

– Szervusztok! – intett vidáman a gyerekeknek.

– Beryl korunk egyik legnagyobb matematikusa – mondta Erik ünnepélyesen, mire az idős hölgy nevetésben tört ki.

– Ne légy nevetséges!

– Pedig igaz! – bólogatott Erik. – Beryl matematikai géniusza nélkül milliók haltak volna meg!

– Milyen milliók? – kérdezte George. Annie előkapta a telefonját, és már kereste is Beryl Wilde Wikipédia-szócikkét.

– Hogy írja a vezetéknevét? – kérdezte Beryltől.

– Nem fogsz megtalálni – csóválta a fejét az idős nő, aki rájött, mire készül Annie. Világoskék szeme huncutul csillogott. – Még ennyi év után is kötelez a titokvédelmi törvény. Sehol sem fogsz megtalálni!

Erik a kanapé előtt álló kisasztal felé mutatott, amin egy furcsa, régi írógépre emlékeztető tárgy állt.

– Ez itt egy Enigma – mondta komolyan. – A második világháborúban használták üzenetek rejtjelezésére, így ha el is fogták az üzeneteket, senki sem érthette meg azokat. Beryl azonban egyike volt azoknak a matematikusoknak, akik feltörték a kódot. Ezért ért véget sokkal hamarabb a háború, mint ameddig elhúzódhatott volna, és sokkal kevesebb ember vesztette életét mindkét oldalon.



– Atyaég! – kiáltott fel Annie, ahogy felnézett a telefonjából. –

Tehát el lehetett olvasni a titkos üzeneteket anélkül, hogy a küldőik észrevették volna, hogy maga rájött, mit terveznek? Mintha valaki titokban elolvasná az e-mailjeimet? Persze, én nem háborúzom senkivel – tette hozzá. – Kivéve Orrtúró Karlát, aki miatt mindenki kinevetett, amikor valamit rosszul írtam a táblán...



– Pontosan – bólintott Beryl. – Elfogtuk az ellenség üzeneteit, és visszafejtettük őket. Így tudtuk meg, mire készülnek. Nagy előnyhöz jutottunk.



## SZÁMRENDSZEREK

### Decimális vagy tízes számrendszer

Mindennapjaink számrendszere, a tízes számrendszer, a 10-es tényezőn alapul. 1-től 9-ig számozunk, és a 10-es számokat már egy újabb oszlopban jelöljük.

$$36 = 3 \times 10 \text{ meg } 6 \times 1$$

$$48 = 4 \times 10 \text{ meg } 8 \times 1$$

$$148 = 1 \times 100 \text{ meg } 4 \times 10 \text{ meg } 8 \times 1$$

És így tovább.

### Bináris vagy kettes számrendszer

A korai számítógépek kettes számrendszert használtak. A kettes számrendszer a 2-es tényezőn alapul, ezért csak a 0 és a 1 számjegyeket használja.

$$10 = 1 \times 2 \text{ meg } 0 \times 1. \text{ Ez a tízes számrendszer 2-es száma.}$$

$$11 = 1 \times 2 \text{ meg } 1 \times 1. \text{ Ez a 3-as szám.}$$

$$111 = 1 \times 4 \text{ meg } 1 \times 2 \text{ meg } 1 \times 1. \text{ Ez a 7-es szám.}$$

A 0/1 számjegyeket a számítógépek áramköreinek kapcsolóihoz társították. A kettes számrendszerben írt kódok alapján az áramkörök képesek voltak szükség szerint ki- és bekapcsolni magukat a 0 = 'ki' és az 1 = 'be' utasításoknak megfelelően. Így hajtották végre számításukat is.

### Hexadecimális vagy tizenhatos számrendszer

A mai számítógépek már sokkal kifinomultabbak. Manapság a kódokat gyakran írják tizenhatos számrendszerben, ami a 16-os tényezőn alapul. 0-tól 9-ig számolunk, de tíz helyett A-t, tizenegy helyett B-t írunk, egészen F-ig, ami a tizenötöt jelenti.

A C a tízes számrendszerben a 12-t jelöli.

Hexadecimálisan a 10 jelöli a 16-ot.

$$11 = \text{tizenhét}$$

$$1F = 1 \times 16 \text{ meg } F \times 1 (15) = 31$$

$$20 = 2 \times 16 = 32$$

$$F7 = F \times 16 (15 \times 16 = 240) \text{ meg } 7 \times 1 = 247$$

$$100 = 256$$

## KÓDFEJTÉS

A kódfejtés során úgy fejtünk meg vagy törünk fel üzeneteket, hogy nincs hozzáférésünk a titkos kódkulcshoz, amivel a feladó az üzenetet küldte. Ezt a folyamatot *rejtjelelemzés*ként is ismerjük, a titkosítás egyik speciális módját pedig *rejtjelezés*nek nevezzük.

### A számítógépek kora előtt

A digitális komputerek elterjedése előtt betűket vagy betűket jelölő számokat titkosítottak, például egy üzenetet meg lehet úgy írni, hogy minden betűt egy másik betű helyettesít. Egy egyszerű kódban az A-t ki lehetne cserélni E-vel, a B-t F-fel, és így tovább az ábécé többi betűjével is, de az ábécét más rendszer alapján is össze lehet keverni.

Ezt a rejtjelezést úgy lehet megoldani, hogy megszámloljuk: az egyes betűk hányszor jelennek meg a titkosított szövegben (ezt gyakoriságelemzésnek nevezzük). Ezután megpróbáljuk kitalálni, melyik betű mit helyettesít. Például, ha az „e” betű sok szóban szerepel, és a kódolt üzenetben „s” betű található, akkor ez jelentheti azt, hogy az „s” = „e”. Akár már ennyi is elég, hogy helyesen fel tudjuk fejteni a többi behelyettesítést, mivel az eredeti üzenetnek értelmesnek kell maradnia.

A bonyolultabb rejtjelezések más módon is behelyettesíthetik az üzenet minden egyes betűjét, és rengeteg lehetőségük van választani: az ábécé 40 betűből áll, így az első betű esetében 40 lehetőség van, a második esetében 39, 38 a harmadik esetében, és így tovább.

### Modern kódfejtés

A modern módszerek nem betűkkel, hanem egy számítógép memóriájának bitjeivel (1-gyel és 0-val) dolgoznak. A titkosítás és a visszafejtés során titkos, hosszú bitekből (1 és 0) álló kulcsot használnak. Manapság egy 256 bitből álló kulcs már elég hatékonyan előzi meg, hogy egy szuperszámítógépet használó kódfejtő pusztán „nyers erővel” (pl. úgy, hogy minden egyes lehetséges kombinációt kipróbál) fejtsen meg egy kulcsot.

KÓDFEJTÉS  
LÖEGÉKTYFSZ  
(+ 1 betű)

GEORGE  
IGÓTIQ  
(+ 3 betű)

ANNIE  
ZSMMHD  
(- 1 betű)



## ENIGMA

### A háború titkai

A második világháború (1939–1945) idején a harcoló felek gépekkel rejtjelezték a fontos üzeneteket: Németországban az Enigma, Nagy-Britanniában a Typex szolgálta ezt a célt.

Az Enigma kezelője a gép billentyűin vitte be az üzenetet, a szerkezet pedig elkészítette a titkosított változatot: minden egyes behelyettesített betűt egy apró villanykörte felvillantásával jelzett. A titkosított üzenetet kézzel írták le, morzekóddá alakították, és rádión továbbították.



### Három rotor

Az Enigma három, bonyolult huzalozású rotorral – kerékkel – működött. A rotorokat el lehetett távolítani, majd más sorrendben visszarakni, és úgy forgatni, hogy a három közül bármelyik rotor a 26 lehetséges pozíció egyikében állhatott. Ez azt jelenti, hogy a három rotort hatféle módon lehetett elhelyezni ( $3 \times 2 \times 1$ ), majd minden betűre  $26 \times 26 \times 26$  pozíció kínált behelyettesítési lehetőséget. Hogy még bonyolultabb legyen a dolog, legfeljebb tíz rövid huzalt lehetett csatlakoztatni a gép első kapcsolótáblájához, és minden egyes huzal által teljesen új  $26 \times 26 \times 26$  elemből álló rejtjelkészlet állt rendelkezésre.

A fogadó oldalon szintén felállítottak egy ugyanúgy beállított Enigmát, és a rejtjelezett üzenetet gépelték be. Ezután már csak le kellett olvasni a felvillanó villanykörteket, és meg lehetett fejteni az eredeti üzenetet. A rendszer úgy működött, hogy az Enigmák kezelői mindennap tudták, aznap melyik rotort hogyan, milyen pozícióban kell a gépbe helyezni, illetve melyik huzalt kell a kapcsolótáblához kötni.





### **Az Enigma feltörése**

Ez a rejtjelrendszer közös titkon alapult: akit beavattak, az tudta, aznap hogyan kell beállítani és használni a gépet. A problémát az jelentette, hogyan osszák meg ezt az ismeretet biztonságosan más emberekkel is. Ha csak egyvalaki hibázik, akkor fontos információk szivároghatnak ki, ráadásul bárki ellophatta vagy eltéríthette a nyomtatott utasításokat is.

A németek által ejtett hibák, illetve a fejlett matematikai tudás és zsenialitás segítségével a kódfejtők – először Lengyelországban, majd később az angliai Bletchley Parkban – sikeresen nyomozták le az Enigma gépek beállításait, és képesek voltak megfejteni a németek üzeneteit. A megoldásban kulcsfontosságú szerepet játszott egy Bombe nevű gép, amit Alan Turing, a matematikus-zseni készített. A Bletchley Parkban fejlesztették a Colossus nevű fontos gépet is. Ez volt az első elektronikusan programozható, digitálisan számoló gépezet, amivel nem az Enigma, hanem egy másik német kódológép, a Lorenz üzeneteit fejtették meg.



## AZ UNIVERZÁLIS TURING-GÉP

### Egy elképzelt szerkezet

1936-ban a komputer még egy személy volt, aki elvégezte a számolási folyamatokat. A zseniális matematikus, Alan Turing által épített Turing-gép képzeletben működő gép: eredetileg azt a célt szolgálta, hogy utánozza az emberi számolási folyamatokat, és elvégezzék a számításokat, a gép ezért inkább elvont matematikai, semmint valós eszköz a számítások és annak megértéséhez, mit lehet elérni a számításokkal. A valóságban azonban nem létezhetne: a feltételezés szerint például végtelen „memóriával” rendelkezne, és időhatárok nélkül működne, de ezek a feltételek a valóságban nem teljesíthetőek.

### 0-k sorozata...

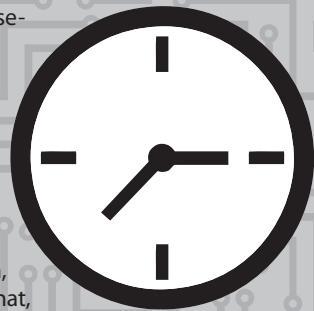
Egy gép működését elsősorban kódolt utasítások véges sora határozza meg. Képzeljünk el egy nagyon hosszú szalagot, amire 0-k hosszú sorát írták a szalag teljes hosszán keresztül. A szalag mindkét végén a végtelenbe vész (feltételezzük, hogy végtelen hosszúságú), és a számítását végző gép memóriáját jelképezi. A 0-k között fel-feltűnnek a véges számú 1-esek, amik a számítógépnek átadott „adatokat” jelképezik. A szalagon ül a feldolgozóeszköz (a processzor), ami csak azt az egy szimbólumot tudja leolvasni, ami közvetlenül alatta van. Hagyhatja változatlanul, vagy cserélheti 0-ra, illetve 1-esre.

A processzor órával is rendelkezik, ami folyamatosan ketyeg, és a processzor minden egyes ketyegésnél leolvassa az aktuálisan látható szimbólumot. Ezután, attól függően, mit lát, és hogy milyen állapotban van az adott pillanatban, az alábbi két dolog valamelyikét hajthatja végre:

- Megváltoztatja az alatta levő szimbólumot 0-ra vagy 1-re, majd egy pozícióval odébb lép a szalagon, jobbra vagy balra. Közben akár új állapotra is átválthat, miközben várja a következő ketyegést.
  - Elvégezheti ugyanezt a műveletet, de utána leáll (kikapcsol).
- Az, hogy végül mit tesz a processzor, attól függ, milyen szabályokat (programot) adunk neki, és hogy mit talál a szalagon.

Példaként feltételezzük, hogy a gép 0 állapotból indul, a szalagon 0-k hosszú sora áll, és valahol a szalag jobb oldalán néhány 0-t 1-re cseréltünk. Ezek az 1-ek mintát alkotnak, ami megegyezik a gépnek megadott bináris számjeggyel.

Kezdetnek felállíthatunk egy szabályt: ha a processzor 0 állapotban van, és 0-t olvas, akkor váltson 0 állapotra, írjon 0-t, és jobbra folytassa az olvasást.





Ez azt jelenti, hogy amikor a gép kezdetben 0-t lát (0 állapotban), akkor 0 állapotban marad, nem változtatja meg a szalagon olvasható 0-t, és egy lépést tesz jobbra. Ha a következő lépésben ismét 0 áll a szalagon, ugyanez történik: a gép 0 állapotban marad, változatlan állapotban hagyja a szalagot, és egy újabb lépést tesz jobbra.

Ez az óra minden egyes ketyegésénél folytatódik, egészen addig, amíg a gép nem találja meg az első 1-est a szalagon. Most már olyan szabályra van szüksége, ami megmondja neki, mit tegyen, ha 0 állapotban 1-est olvas le a szalagról. A legegyszerűbb szabály ez lehetne: a processzor maradjon 0 állapotban, írjon 1-et, lépjen egyet jobbra, és álljon le. A gép bal oldalán ekkor megjelenik az 1, mint a számítás eredménye.

Ezt az egyszerű számítást úgy írhatnánk le: „írj 1-et, ha a bemenet érvényes”. Az érvényes ebben az esetben azt jelenti, hogy „legalább egy 1-est tartalmaz”. Ha a gép jobb oldalán nincsenek 1-esek, amikor a gép elindul, akkor a gép tovább keresné az 1-est, akár örökké is: nem áll meg, de eredmény nélkül dolgozik! Ez egy valódi számítógéppel is megtörténhet: egy program belekeveredhet egy végtelen ciklusba (loop'-ba vagy spin'-be), amíg le nem fagy a teljes berendezés.

Ez a lehetőség sajnos alapvető tulajdonsága a Turing-gépeknek és a valódi számítógépeknek is, de megakadályozhatjuk, hogy hasonló eset történjen azáltal, hogy kikötjük: az érvényes bemenetnek legalább egy darab 1-est kell tartalmaznia. Ily módon az első szabályt nem lehetséges örökké használni.

## **Minden lehetséges számítás**

Ha elegendő idő áll rendelkezésre, és lehetséges annyi 1-est írni a szalagra, amennyi szükséges, minden elképzelhető, egész számokkal végrehajtott mechanikai műveletet el lehet végezni, ha a Turing-gépbe betápláljuk a bemeneti számot a gép jobb oldalán; majd elindítjuk az órát, megvárjuk, amíg leáll a gép, és leolvassuk az eredményt a gép bal oldalán. Ebben minden aritmetikai számítás benne van, amit egy ember papírral és tollal valaha el tud végezni. Alan Turing azt állította, hogy amit az ő Turing-gépe ki tud számolni, az definícióként szolgálhat mindenre, amit egyáltalán ki lehet számolni. Lenyűgöző, hogy elméletei után majdnem nyolcvan évvel ez még mindig helyes definíciónak számít, mert a digitális számítógépek minden egyes ismert modellje csak azt tudja kiszámolni, amit a Turing-gép is ki tudott számolni.

Turing azt is bebizonyította matematikai úton, hogy még egy Turing-gép sem tud minden problémát megoldani! Ez azt jelenti, hogy vannak matematikai problémák, amiket a gépek nem tudnak kiszámítani, így egyelőre a matematikusokat sem fogják felváltani a számítógépek.

– Azta! Maga nagyon menő, Bez! – kiáltott fel Annie, majd orrát ismét a telefonjába dugta.

– Ez egy valódi Enigma? – meredt George a szerkezetre áhítatosan. El sem hitte, hogy egy újabb csodálatos gépezet került Bellisék házába. Már vagy milliomodszorra kívánta, hogy bárcsak ebbe a családba született volna, nem a sajátjába.

– Valódi, igen – mosolygott rá Beryl. – Eriknek hoztam ajándékba.

Erik levegőért kapkodott, mostanáig láthatóan fogalma sem volt az asszony szándékáról.

– Ez lehetetlen! – kiáltotta. – Nem adhatod nekem!

– Dehogynem – mondta határozottan Beryl. – A matematika tanszéked kiváló hasznát fogja venni az egyetemen. Te vagy a legjobb személy, akihez kerülhet, hiszen kvantumszámítógépekkel foglalkozol! Jobb helye nem is lehetne!

– Mi az a kvantumszámítógép? – kérdezte George. Még sosem hallott ilyen eszközről, és azonnal fellelkesült. Eszébe jutott, hogy Erik már egy ideje titkolózik a munkájával kapcsolatban. Valahányszor megkérdezte a kiváló tudóst, mivel foglalkozik, csak kurta válaszokat tudott kicsikarni belőle.

Ma este azonban Erik a szokásosnál sokkal beszédesebbnek tűnt.

– A kvantumszámítógép a változás új szele – magyarázta George-nak. – Már végbement az információ digitális forradalma, és most a kvantumforradalom küszöbén állunk. Ha készíthetnénk és irányíthatnánk egy kvantumszámítógépet – ez utóbbi jelenleg igen nehéz feladatnak tűnik –, olyan dolgokra lennénk képesek, amik a jelenlegi komputertechnológiával még elképzelhetetlenek lennének!

– Például milyen dolgokra? – kérdezte George.

– Egy kvantumszámítógéppel minden kódot fel tudnánk törni! A Föld egyetlen biztonsági rendszere se tudna minket

megállítani! – magyarázta Erik lelkesen. – Csodás dolgokra lennénk képesek az információfeldolgozásban, a gyógyszerészetben, a fizikában, a mérnöki tudományokban és a matematikában. Ez az emberiség újabb nagy lépése!

– De mi köze ennek az Enigmához? – kérdezősködött tovább George.

– Az Enigma minden későbbi, izgalmas technológia előfutára – válaszolt Beryl. – És természetesen az Enigma létező és működő eszköz. Sajnálatos módon azonban a kvantumszámítógép jelenleg egyik kritériumnak sem felel meg.

– Hát igen, hehehe... – nevetgélt Erik. – Jelenleg a munkám nagy része főleg kvantumhiba-kereséssel telik.

– Apád talán az egyetlen ember a Földön, aki képes lenne kezelni egy kvantumszámítógépet – szolt közbe Beryl. – Már persze, ha létezne a kvantumszámítógép.

Erik elégedettnek tűnt.

– A kvantumhiba-keresés tulajdonképpen azt jelenti, hogy amikor sikerül működésre bírni egy kvantumszámítógépet, akkor vezérelni is képesek legyünk, de ez jelen pillanatban nem tűnik megvalósíthatónak! Az Enigmával bezzeg nem volt ilyen gond.

– Használhatnánk az Enigmát? Küldhetünk egymásnak Annie-vel rejtjelezett üzeneteket? – merengett el George.

– Az Enigma nem képes üzenetküldésre – itta ki Beryl a sherryje maradékát. – Titkosítja és megfejti az üzeneteket, de elküldeni máshogy kell őket. Akik használták az Enigmát, főleg morzekódként, rádión keresztül továbbították. Manapság már rendelkezünk olyan technológiával, ami mindkettőre képes: minden másodpercben milliányi üzenetet titkosít, és kábeleken vagy rádióhullámokon át küldi el őket, majd a fogadó számítógépek fejtik vissza az üzeneteket. Minden e-mail, minden weboldalhoz érkező felkérés és minden számítógépes parancs kódolt üzenet. Noha vannak olyan kódok, amiket mindenki megérthet



### Titkok kódjai

A történelem folyamán az emberek akkor használtak kódokat, amikor üzeneteket akartak rejtjelezni. Ennek során a hétköznapi szövegeket úgy alakították át, hogy azok számára, akiknek fogalmuk sem volt a kódkulcsról, érthetatlenné váljon. Így tudtak szövetségeseiknek titkos üzeneteket küldeni.

Ha manapság online vásárolunk – zenét, könyvet vagy ajándékot –, ugyanezt tesszük, hogy az internetes bűnözők ne tudják lenyomozni a hitelkártyánkat, és az adatokat használva ne tudják ellopni a pénzünket. A digitális komputer nemcsak el tudja rejteni az üzenetek részleteit (például a fizetési információkat), de azt is könnyű felfedezni, ha egy üzenetbe csaló nyúlt bele, vagy éppen egy csaló küldte az üzenetet.

Ezek a módszerek nem betűkkel, hanem bitekkel működnek. Olyan rejtjelkulcsokat használnak, amiket a komputer könnyedén használ, de a kulcs ismerete nélkül elképesztően nehéz feltörni. Persze ettől még sokan próbálkoznak a megfejtéssel, így lehet, hogy hamarosan ezeket a kulcsokat is feltörik. Ebben az esetben új rejtjelkulcsokat kell majd kialakítani.





## Számítógépes nyelvek

Egy matematikus számára a kódolás az a folyamat, melynek során egy szimbólumkészletet megadott szabályok mentén egy másik szimbólumkészletté alakítanak át.

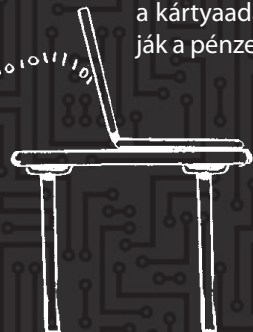
Bármilyen számítógép működéséhez alapvetően szükséges az utasítások és adatok kódolása, de hogyan tudjuk ezeket 0 és 1 formában bemutatni, hogy a számítógép processzora is el tudja olvasni az utasításokat? Ezen szabályok határozzák meg a processzor gépi kódját.

A szabálykészleteket algoritmusoknak nevezzük. Ezek segítségével egy türelmes ember és a digitális számítógép is képes kódolni – előbbi papírral és tollal, utóbbi az embernél valószínűleg sokkal gyorsabban.

Az emberek olvasható számítógépes nyelvekben írnak programokat, ilyen például a C és a FORTRAN. Mindkét nyelvben angol szavakat és karaktereket használnak 1 és 0 helyett. Az évek során sok-sok programnyelvet fejlesztettek ki, amelyek segítségével a programozók „beszélhetnek” a számítógéphez. Manapság a „számítógépes kód” alatt gyakran az ezen nyelvek valamelyikén kódolt programot értjük.

A fordítóprogramok (compilerek) speciális programok, amelyek elolvassák a magas szintű programnyelven írt programokat, és gépi kódon alapuló programmá alakítják őket, amiket aztán közvetlenül be lehet táplálni a processzorba. A gépi kódokat ma már a legtöbbször hexadecimális (tizenhatos) számrendszerben írják.

Ha ezt a kódot feltörik, akkor a program működése sikertelen, vagy váratlan eredményeket produkál. Az internetes csalók gyakran próbálkoznak ezzel a taktikával, hogy rosszindulatból vagy bűnelkövetési szándékkal jogosulatlanul férjenek hozzá egy számítógéphez (például a kártyaadataidhoz – ha megszerzik a bankkártyád számát, ellophatják a pénzedet!).



## ALGORITMUSOK

Az algoritmus egy lépésről lépésre haladó folyamat, amelynek során egyértelmű szabályok határozzák meg, hogy az egyes lépések során hogyan konvertáljunk egy szimbólumokból álló listát egy másik szimbólumrendszerbe. Például a nagy számok szorzása vagy osztása során ismerős lépésekkel találkozol, mert megtanultad őket az iskolában: ezek a lépések is algoritmusok. Minden problémát ugyanúgy kell megoldani: minden lépésnél le kell írni egy papírra a számokat, majd szükség szerint új számsort alkotni, egészen addig, amíg el nem jutsz a megoldásig.

Az algoritmus ősi találmány. Eukleidész már Kr. e. 300-ban leírt egy algoritmust, hogy megtalálja, mi két egész szám legnagyobb közös osztója (bár ez az algoritmus valószínűleg még ennél is régebbi).

Maga az *algoritmus* szó egy 9. századi perzsa matematikustól, Muhammad ibn Músza al-Hvárizmitől származik, aki az aritmetikai műveletek végrehajtásának eszközeként írta le az algoritmusokat, és többek között az algebrai módszereket is ő dolgozta ki.

A huszadik századi matematikusok megpróbálkoztak az algoritmus matematikai meghatározásával, de minden korai próbálkozás a Turing-gép kapacitásáig jutott: egyetlen ismert komputer sem képes ennél többre!

Minden számítógépes program egy algoritmusra vezethető vissza, ami minden egyes processzorciklus alatt megváltoztatja a számítógép memóriájának bitmintázatát.

– ezek nélkül elég nehéz lenne használni az internetet –, ha például zoknit veszel egy webáruházban, te is elvárod, hogy titkosítsák a hitelkártyád számát, különben könnyen ellophatják a pénzedet. Gondolj bele, hogy a világ számítógépei hogyan vezérlik a dolgokat: az elektromosságot, a közlekedést, a honvédelmet, csak hogy három példát mondjak! Minden esetben titkosítást használnak, nehogy avatatlan kezek zavarják össze ezeket a folyamatokat. Ha fel tudnád törni ezeket a kódokat, az egész világtól váltságdíjat kérhetnél!

– Csak ne adj nekik ötleteket – mondta Erik tettetett komolysággal. – Nincs kedvem kiadatási kérvényekkel vesződni, csak mert a két jómadár sikeresen feltört egy szupertitkos kormányprogramot, és felbosszantott néhány hivatalnokot!



– Pedig milyen jó móka lenne!  
– kiáltott fel Beryl. – Remélem, megteszik!

George Annie-re nézett. Beryl biztosan sok csodálatos dologról tudna mesélni.

– Tőled aztán elleshetnék a mikéntjét, igaz? – mondta Erik Berylnek, de távolról sem tűnt dühösnek, sőt, vidám volt. – Hess innen, gyerekek, mielőtt még Beryl beszervez titeket a titkosszolgálat ifi osztályába!

– Ne már, apa! – nyafogott Annie. Most már elég kíváncsi volt ahhoz, hogy eltegye a telefonját. – Én szeretnék csatlakozni a titkosszolgálathoz, az az életem fő célja! Nem maradhatnánk itt?

– Te csak ne hisztizz! – mondta határozottan Erik. – Menjetek, játsszatok olyat, amiért nem tenyerel a csengőmre a hírszerzés!

# **TETSZIK? MI IS NAGYON SZERETJÜK.**

Szívből ajánljuk,  
ha öröme és felszabadult percekre vágysz!

**Már rendelhető!  
ÉLVEZD MIHAMARABB!**

**MOST  
KEDVEZMÉNNYEL**

lehet a tiéd!

[Megnézem.](#)

**NE HAGYD KI!**

Rendeld meg most a kiadónál!

**Még több jó könyv**

megjelenését támogatom veled.

[Imádom a jó könyveket. Kérem máris!](#)

Én nem James Bond vagyok, hanem fizikaprofesszor, ezt ne felejtétek el!

– Kinn már sötét van – mondta George, ahogy kilesett az ablakon. – Menjünk ki a faházba, és fényképezzük le a Szaturnuszt!

– Kiváló ötlet – bólintott Erik. – Egy távoli bolygó fényképezésével talán még ti sem kerültök bajba!

Beryl kuncogni kezdett.

– De azért kérlek, próbáljatok bajba kerülni – kacintott Annie-re és George-ra. – Sokkal izgalmasabb az élet, ha néha van egy kis kalamajka. Úgy sokkal érdekesebb az egész!

– Menjetek, gyerekek! – szólt rájuk ekkor Erik, és ezúttal nem színlelte a kimerültséget.