

Ilustroval Garry Parsons

# GREGOROV NEROZLÚŠTITELNÝ KÓD



**LUCY & STEPHEN  
HAWKINGOVCI**



**GREGOROV**  
**NEROZLÚŠTITELNÝ**  
**KÓD**

Lucy a Stephen Hawkingovci spolu napísali aj:

***GREGOROVE TAJNÉ VÝPRAVY  
DO VESMÍRU***

***GREGOROVA VESMÍRNA NAHÁŇAČKA  
ZA POKLADOM***

***GREGOR A VEĽKÝ TRESK***

*„Dramatický dobrodružný príbeh...  
pre všetkých budúcich kozmológov.“*

GUARDIAN

*„Nechat si ujsť túto knihu by bola naozaj škoda!“*

CAROUSEL

# GREGOROV NEROZLUŠTITELNÝ KÓD



**LUCY A STEPHEN  
HAWKINGOVCI**

**ILUSTROVAL GARRY PARSONS**

**slovart**

Copyright © Lucy Hawking, 2014  
First published as *George and the Unbreakable Code*  
by Random House Children's Publishers UK  
a division of The Random House Group Ltd.  
Translation © Dagmar Šajtyová 2015  
Slovak edition © Vydavateľstvo SLOVART, spol. s r. o., Bratislava 2016

Všetky práva vyhradené. Žiadna časť tejto knihy sa nesmie reprodukovat  
ani šíriť v nijakej forme ani nijakými prostriedkami, či už elektronickými  
alebo mechanickými, vo forme fotokópií či nahrávok, respektíve  
prostredníctvom súčasného alebo budúceho informačného systému  
a podobne bez predchádzajúceho písomného súhlasu vydavateľa.

ISBN 978-80-556-1406-9

*Všetkým, ktorí sa pozreli na nočnú oblohu  
a premýšľali...*



## NAJNOVŠIE VEDECKÉ TEÓRIE!

Pri čítaní príbehu narazíte na niekoľko úžasných vedeckých štúdií a informácií, z ktorých sa môžete veľa dozvedieť o rozličných témach. Napísali ich títo poprední vedci:

### **Môj robot, tvoji roboti**

**str. 62**

napísal profesor Peter W. McOwan,  
Londýnska univerzita kráľovnej Márie, Veľká Británia

### **História života**

**str. 85**

napísal profesor Michael J. Reiss,  
Inštitút vzdelávania, Univerzita v Londýne, Veľká Británia

### **Kvantové počítače**

**str. 136**

napísal Dr. Raymond Laflamme, riaditeľ Inštitútu kvantovej počítačovej vedy na Univerzite vo Waterloo, Veľká Británia

### **Stavebné prvky života**

**str. 165**

napísal Dr. Toby Blench,  
výskumný chemik

### **3D tlač**

**str. 248**

napísal Dr. Tim Prestidge,  
Totempole Consulting

### **Život vo vesmíre**

**str. 300**

napísal profesor Stephen Hawking,  
riaditeľ Inštitútu teoretickej kozmológie,  
Univerzita v Cambridgei, Veľká Británia

Za doplňujúci materiál ďakujem:

Dr. Stuartovi Rankinovi, Oddelenie vysokovýkonných počítačov,  
Univerzita v Cambridgei, Veľká Británia





**N**a inej planéte by bol domček na strome ideálnym miestom na pozorovanie hviezd. Napríklad planéta bez rodičov by bola úplne skvelá. Domček na strome – na veľkej jabloni uprostred zeleninových hriadok – mal správnu výšku, miesto aj uhol na to, aby tam chlapec ako Gregor mohol stráviť celú noc pozorovaním hviezd. Jeho mama a otec však mali iné predstavy, medzi ktoré patri-li domáce práce, úlohy, spánok v posteli, spoločná večera alebo „čas s rodinou“, teda s malými sestrami – dvojčičkami. Nič z toho však Gregora nebavilo.

Jediné, po čom túžil, bola fotka Saturnu. Keby si tak mohol aspoň raz odfotiť svoju obľúbenú planétu – velíkánskeho zmrznutého plynového obra s nádhernými ľadovými prachovými prstencami. Ale v tomto období roka, keď slnko zapadalo naozaj neskoro, sa Saturn objavil na nočnej oblohe až takmer o polnoci. Gregor však vtedy mal dávno po večierke a nebola šanca, že by ho rodičia nechali v domčeku na strome tak dlho.

Gregor zamyslene hojdal nohami na okraji domčeka, vzdychal a snažil sa vypočítať, koľko hodín a dní ešte musí



čakať, kým bude dosť starý na to, aby si mohol robiť, čo chce...

„Čau,“ prerušila jeho myšlienkový pochod útla postava v dlhých širokých maskáčových šortkách, mikine a bejzbalovej šiltovke, ktorá zrazu vyskočila na dlážku domčeka. „Čo tu tak sedíš?“

Gregorovi bolo hneď veselšie. „Anka?“

Anka bola jeho najlepšia kamarátka, odkedy sa pred niekoľkými rokmi spolu s mamou a otcom prisťahovala do mestečka Foxbridge. Bývala vo vedľajšom dome, ale nebol to jediný dôvod ich kamarátstva. Gregor ju mal skrátka rád: Anka, dcéra vedca, bola zábavná, šikovná, mala skvelé nápady a ničoho sa nebála. Nič pre ňu nebolo nemožné, žiadne dobrodružstvo nemohlo zostať ne-

povšimnuté, nijaká teória neoverená a žiadna domnienka nepreskúmaná.

„Čo robíš?“ opýtala sa.

„Nič,“ zamrmľal Gregor. „Len čakám.“

„A na čo?“

„Že sa niečo stane.“ Jeho hlas znel nešťastne.

„Aj ja,“ povedala Anka. „Myslíš, že na nás vesmír zabudol? Že už nikdy nezažijeme žiadne vesmírne dobrodružstvo?“

Gregor si vzdychol. „Myslíš, že ešte niekedy budeme lietať vo vesmíre?“

„Teraz asi nie,“ odvetila Anka. „Možno sme si užili dosť zábavy, a keďže už máme jedenásť rokov, musíme byť už navždy vážni.“

Gregor vstal a pocítil, ako sa pod ním drevené dosky rozkývali. Bol si *takmer* istý, že domček na strome je bezpečný a je veľmi nepravdepodobné, že by sa mohli zrútiť na tvrdú zem. Postavil ho spolu s otcom z materiálu, čo nazvláčali z miestnej skládky odpadu. A raz, keď sa práve zaoberali stavbou „obývatelnej“ časti, kde teraz sedeli s Ankou, sa otec preboril nohou cez prehnutú dosku. Našťastie cez ňu úplne neprepadol, ale Gregor musel vynaložiť všetky sily, aby ho vytiahol nahor, zatiaľ čo dole na zemi jeho sestry, dvojčičky Juno a Hera, pištali od smiechu.

Vďaka tejto malej nehode však Gregorovi rodičia usúdili, že domček na strome je príliš nebezpečný pre jeho malé sestry, ktoré tak dostali zákaz šplhať sa hore po

povrazovom rebríku. Gregor bol s rozhodnutím rodičov veľmi spokojný. Znamenalo to, že domček na strome je *jeho* kráľovstvo, chránené pred chaosom, ktorý vládol v celom dome. Dostal prísne pokyny vždy vytiahnuť rebrík tak, aby zabránil nedočkavým človečikom vyšplhať sa za milovaným bratom. Gregor veľmi dôsledne dbal na bezpečnosť a nikdy rebrík nespúšťal. Čo znamená...

„Hej!“ Zrazu si uvedomil, že Anka sa tam predsa nemala ako len tak objaviť. „Ako si sa dostala hore?“

Anka sa uškrnula. „Keď som bola malá, uštipol ma pavúk,“ zašepkala dramatickým hlasom. „Vďaka tomu mám nadprirodzené schopnosti, ktorým ešte len teraz začínam rozumieť.“

Gregor ukázal na povraz s uzlami, ktorý si práve všimol na najhrubšej vetve stromu. „To si bola ty?“

„Hej,“ priznala sa Anka už normálnym hlasom. „Chcela som len skúsiť, či to dokážem.“

„Spustil by som ti dole rebrík,“ povedal jej Gregor.

„Naposlady, keď som chcela, aby si mi



ho spustil,“ sťažovala sa, „si ma nútil hádať milión rôznych hesiel a ešte som sa potom musela s tebou podeliť o Kit Kat.“

„To nebol Kit Kat!“ pripomenul jej Gregor. „Bol to kúsok čokolády“ – prstami pritom nakreslil do vzduchu úvodzovky –, „čo si skúšala vyrobiť v laboratórnych podmienkach, zabalený do obalu od Kit Katu, aby si videla, či zistím rozdiel.“

„Keď môže myšiam narásť ucho na chrbte,“ namietla Anka, „prečo by som si ja nemohla vypestovať Kit Kat? Musí byť predsa možné vyrobiť samoreprodukčné čokoládové molekuly, ktoré sa budú jednoducho ďalej zdvojnásobovať.“

Anka bola nádejná experimentálna chemička. Často využívala kuchyňu ako svoje osobné laboratórium, čo jej mamu privádzalo do zúfalstva, napríklad keď chcela vybrať z chladničky jablkový džús a namiesto toho tam našla kryštalický proteínový produkt.

„Len aby si vedela,“ povedal Gregor. „Ten tvoj Kit Kat chutil ako dinosaurí necht.“

„Ani náhodou!“ protestovala Anka. „Moja doma vypestovaná čokoláda bola vynikajúca. Tak neviem, o čom hovoríš. A vôbec, kedy si stihol ochutnať dinosaurí necht?“

„Necht na palci,“ spresnil Gregor. „Vážne hnusné. Ako-by to bola bilión rokov stará skamenelina.“

„Haha,“ zasmiala sa Anka sarkasticky. „Netušila som, že je z teba *taký* gurumak.“

„Myslíš gurmán? Veď ani nevieš, čo to znamená,“ odsekol Gregor.

„Viem!“

„No tak povedz,“ Gregor si bol celkom istý, že má tentoraz pravdu.

„No, keď si v niečom naozaj dobrý, tak si guru,“ vysvetľovala Anka, „a keď sa pritom prechádzaš v maku, tak je z teba *gurumak*.“ Sotva dokončila vetu a vybuchla od smiechu – až pritom spadla zo sedacieho vaku.

„Ty si cvok,“ povedal Gregor a usmial sa.

„Čo má IQ 152.“ Anka sa zdvihla z dlážky. Pred týždňom bola na testoch IQ a chcela, aby si všetci pamätali jej výsledok. Zrazu zbadala na zemi rozložené Gregorove veci. „Čo s tým?“

„Dávam si to dokopy.“ Gregor ukázal na vybavenie, ktoré zachránil z rúk svojich malých sestier a vyniesol ho do domčeka na strome, aby bolo v bezpečí. Mal tam 60-milimetrový biely teleskop s čiernymi páskami na každej strane a fotoaparát, ktorý sa pokúšal primontovať na teleskop, aby mohol robiť fotky. Teleskop dostal od starkej, ale fotoaparát prekvapivo pochádzal zo smetiska. „Aby som mohol robiť fotky Saturnu, keď sa zotmie. Teda ak ma moji *nudní* rodičia nedonútia ísť dnu. Je to môj projekt na prázdniny.“

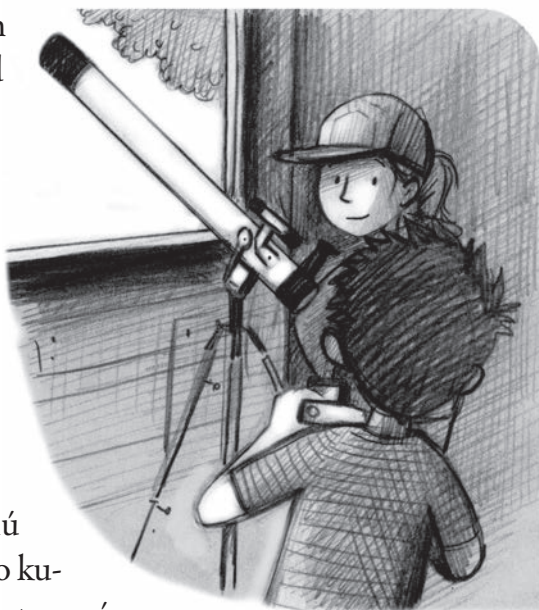
„Paráda!“ Anka prižmúрила oči a nazrela do hľadáčika teleskopu. „Fuj!“ vykrikla vzápätí. „Je na tom niečo lepkavé!“

„Čo?!“ zdesil sa Gregor. Pozrel sa bližšie. A naozaj, okolo hľadáčika bola akási lepkavá ružová hmota.

„Už toho mám dosť!“ vybuchol od zlosti. Začal schádzať po rebríku.

„Kam ideš?“ zliezala Anka za ním. „Veď to nie je nič hrozné! To sa dá očistiť!“

Ale Gregor sa už rútil do domu a tvár mal červenú od hnevu. Vrazil do kuchyne, kde sa jeho otec práve pokúšal nakrmiť dvojčičky.



„Jedna lyžička za ocka!“ povedal Here, ktorá otvorila ústa, ochutnala zelenú gebuzinu a vzápätí ju naňho vyplula. Hera potom začala pišťať od smiechu a trieskať lyžičkou o tácku na detskej stolíčke, takže všetky kúsočky jedla poskakovali okolo nej ako mexické fazuľky.

Juno, ktorá zvyčajne kopírovala svoje dvojča, sa k nej pridala, búchala lyžičkou, odúvala pritom pery a prskala.



Otec sa pozrel na Gregora s útrpno-radostným výrazom na tvári a zelený sliz mu pritom kvapkal z brady na doma vyrobenú košeľu.

Gregor sa zhlboka nadýchol, že zo seba vydá nahnevajúcu záplavu slov o deckách, ktoré babrú veci iných ľudí, ale Anka sa práve včas pretlačila pred neho.

„Ahoj!“ zavolala veselo na Gregorovho otca. „Ahojte, dievčatá!“

Dievčatá zabúchali lyžicami a dychtivo brblali pri novom rozptýlení od večere.

„Len som sa chcela opýtať, či by Gregor nemohol ísť k nám,“ zašvitorila Anka. Natiahla ruku, aby pošteklika Heru na lepkavej brade, načo sa dievčatko okamžite rozchichotalo.

„A čo môj teleskop?“ zamrmlal Gregor podráždene Anke za chrbtom.

„To sa vyrieši,“ odvetila potichu. „Ty máš ale šťastie, že máš malé sestričky,“ hrkútala pri pohľade na dvojčatá. „Aj ja by som chcela mať také roztomilé sestry. Som taký osamelý jedináčik...“ vystrúhala prehnane smutnú tvár.

„Hmm.“ Gregor by si nič neželal viac, ako žiť v Ankinej tichej, čudáckej a technológiami popretkáwanej domácnosti s otcom vedcom a mamou, ktorá sa čoraz viac zameriava na kariéru. Tam neboli žiadne malé deti, žiadny hluk, žiadna biozelenina a neporiadok – teda okrem prípadov, keď Anka robila jeden zo svojich „zaujímavých“ pokusov v kuchyni.

„No, ehm, môžeš ísť – ale nezabudni sa vrátiť načas, aby si stihol urobiť všetky povinnosti,“ povedal Gregorovi otec a snažil sa, aby to vyznelo tak, že má veci pod kontrolou.

„Super!“ zvolala Anka nadšene a tlačila Gregora von z dverí. Gregor vedel, že keď má Anka rozkazovačnú náladu, netreba jej odporovať. A tak šiel za ňou, čo zasa nebolo také ťažké, lebo vôbec nemal chuť trčať namosúrený doma, keď mohol ísť na návštevu k Anke.

„Ahojte!“ zahulákala Anka, keď vybehli z dverí. „Pekný deň!“

„Gregor, nezabudni, že musíš vyplniť graf odmien a dokončiť si týždenné úlohy!“ zavola Gregorovi otec za odchádzajúcou postavou svojho najstaršieho syna. „Ešte ti chýbajú tri pätiny kruhového grafu!“

No Gregor bol už preč, Anka ho uniesla na vzrušujúce územie susedného domu – domu, v ktorom bolo v Gregorových očiach všetko technologické, priekopnícke, vedecké, elektronické a úžasné.



**K**Ankinmu domu sa dostali cez dieru v plote medzi záhradami. Dieru urobil Freddy – prasiatko, ktoré bolo ďalším z darčkov od Gregorovej iniciatívnej starkej –, keď sa pokúšal predať zo záhrady Zeleninkovcov pri odvážnej ceste za slobodou. Jeho stopy v to popoludnie priviedli Gregora prvýkrát k Anke a k jej rodine – k otcovi, úžasnému vedcovi a supermozgu Erikovi, k mame, hudobníčke Zuzane a ich super počítaču Kozmovi, ktorý bol taký výkonný a inteligentný, že dokázal nakresliť dvere, cez ktoré ste sa mohli dostať na akékoľvek miesto vo vesmíre (ak ste, samozrejme, mali na sebe skafander). Od toho dňa sa Gregor stihol povozit' na kométe, chodiť po Marse a bojoval so zlým vedcom vo vzdialenom solárnom systéme. Treba povedať, že jeho život už nikdy nebol taký ako predtým.

„Hej!“ ozvala sa Anka, keď bežali. „Nemal by si byť na svoje sestry zlý.“

„Čo?“ Gregor už na dvojčky vôbec nemyslel. „O čom hovoríš? Ved' som vôbec nebol zlý!“

„Lebo som ťa zastavila,“ podotkla Anka. „Chcel si povedať niečo hnusné.“

„Bol som našťavaný!“ zvolal Gregor rozhorčene. „Nemajú sa čo dotýkať mojich vecí ani chodiť do domčeka na strome!“

„Máš šťastie, že máš aspoň nejakých súrodencov,“ povedala Anka zmierlivo. „Ja nemám nič.“

„Ale máš!“ vybuchol Gregor. „Veď máš toľko vecí! Máš Kozma, vedecké laboratórium, Xbox, smartfón, notebook, iPod, iPad... ani neviem, čo všetko, a ešte aj toho mechanického psa a kolobežku s motorom... no jednoducho... máš toho kopec.“

„To nie je to isté,“ odvetila Anka ticho, „ako mať ozajstného brata alebo sestru.“

„Keby si mala súrodenca,“ povedal Gregor pochybovačne, „alebo rovno dvoch, stavím sa, že by si ich už tak veľmi nechcela.“

Obaja preleteli cez dvere do kuchyne.

„Prvá!“ Anka sa šmykla po dlážke k obrovskej chladničke a natiahla sa k rúčke.

Ani chladnička nevyzerala ako obyčajná chladnička u nich doma – viac sa podobala na zariadenia z laboratória: obrovská oceľová škatuľa s veľkými zásuvkami a samostatnými priestormi na uloženie vecí. Bolo to, samozrejme, profesionálne zariadenie, ktoré bolo také vzdialené od normálnej chladničky ako vesmírna loď od papierového lietadielka. To bola jedna z vecí, ktoré Gregor u Anky doma zbožňoval: Ich dom bol plný nečakaných dômysel-

ných vecí a vedeckých zvláštností, ktoré Erik kúpil, získal alebo dostal v priebehu mnohých rokov vedeckej práce. Gregor sa závistlivo pozrel na chladničku, vyžarovala zvláštne modré svetlo. Najmodernejšia vec u nich do ma mala zrejme menší technologický výkon ako táto chladnička.

Gregor práve dumal nad touto deprimujúcou skutočnosťou, keď si uvedomil, že z obývačky počuť hlasy.

„Anka! Gregor!“ Ankin otec Erik vystrčil hlavu spoza kuchynských dverí. Naširoko sa usmieval, oči mu žiarili za hrubými sklami okuliarov, mal uvoľnenú kravatu a vyhrnuté rukávy na košeli. Keď vošiel, v rukách niesol dva krištáľové poháriky.

„Prišiel som si doliať,“ vysvetlil, natiahol sa po zaprášenú starú fľašu a s hlasným lupnutím z nej vytiahol korkovú zátku. Nalial si lepkavú hnedú tekutinu a obrátil sa, že sa vráti späť do obývačky.

„Podťe pozdraviť moju návštevu.“ Na tvári sa mu od úsmevu vytvorili jemné vrásky. „Myslím, že má niečo, čo by vás mohlo zaujímať.“





Gregor a Anka okamžite zabudli na svoj spor a šli za Erikom do obývačky, ktorá bola odhora až nadol zaprataná knihami. Bola to nádherná miestnosť plná zaujímavých predmetov, ako napríklad Erikov starý mosadzný teleskop. Špičková technológia, ktorá prevládala v celom dome, v nej nebola taká výrazná, bolo tu skôr útulne a príjemne a nie štýlovo hypermoderne. Na mäkkej pohovke, ktorú mal Erik už od svojich študentských rokov, sedela veľmi stará dáma.

„Anka, Gregor,“ povedal Erik a podával pritom starej dáme pohárik sherry.

„Toto je Beryl Wildová.“



Beryl si vďačne vzala pohárik a hneď aj z neho usrkávala.

„Ako sa máte?“ zamávala na nich veselo.

„Beryl je jednou z najvýznamnejších matematiciek našich čias,“ povedal Erik vážne.

Beryl sa rozosmiala. „Ale prosím ťa!“

„Je to pravda!“ trval Erik na svojom. „Bez jej matematického talentu by zomrelo o niekoľko miliónov ľudí viac.“

„Akých ľudí?“ opýtal sa Gregor.

Anka vytiahla svoj smartfón a pokúšala sa vyhľadať na Wikipédii heslo Beryl Wildová.

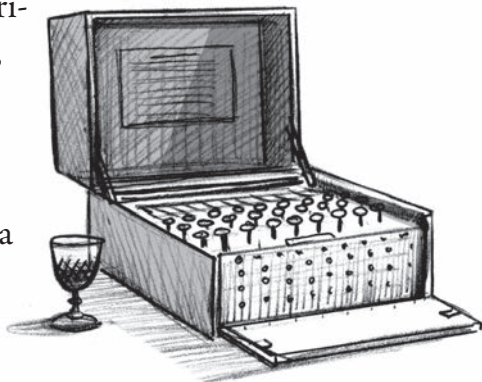
„Ako presne sa píše vaše meno?“ opýtala sa.

„Nenájdeš ma,“ odvetila Beryl, keď zistila, o čo sa Anka snaží, a bledomodré oči jej pritom zaiskrili. „Moja osoba spadá pod zákon o štátnom tajomstve. Hoci už odvtedy prešlo toľko rokov. Nikde o mne nenájdeš ani jedinú zmienku.“

Erik ukázal na predmet na konferenčnom stolíku pred pohovkou.

„Toto,“ oznámil dramaticky a pritom ukazoval na akýsi zastaraný písací stroj, „je šifrovací stroj Enigma – jeden z tých, ktoré sa používali počas druhej svetovej vojny na šifrovanie správ. To teda znamená, že sa ním dali posilať

správy, ktoré boli pre nepovolaných príjemcov nezrozumiteľné. Ale Beryl patrila medzi matematikov, ktorým sa podarilo rozlúštiť kód Enigmy. Vďaka tomu sa vojna skončila oveľa skôr a na oboch stranách tak prišlo o život oveľa menej ľudí.“



„Fíha!“ zvolala Anka a zdvihla oči od telefónu. „To ste akože dokázali čítať tajné správy bez toho, aby zistili, že viete, čo plánujú? Ako keby si niekto teraz mohol prečítať všetky moje maily? Aj keď ja, samozrejme,“ dodala, „s nikým nevediem vojnu. Teda okrem Karolíny Horenosej, ktorá sa mi pred všetkými smiala, keď som zle napísala slovo na tabuli.“

„Presne tak,“ prikývla Beryl. „Dokázali sme zachytiť ich správy a rozlúštiť obsah, a tak sme vedeli, čo chystajú. Vďaka tomu sme mali veľkú výhodu.“

„Paráda!“ zhodnotila Anka. „Uznávam vás, Beryl!“ Znova začala ťukať do telefónu.

„To je *naozajstná* Enigma?“ Gregor uprene hľadel na šifrovací stroj. Nemohol uveriť, že u Anky doma sa objavil ďalší úžasný prístroj. Už tisíci raz si v duchu povzdychol, prečo sa radšej nenarodil v tomto dome.

„Je,“ prisvedčila Beryl a usmiala sa naňho. „A chcem ju dať Erikovi. Ako darček.“

## ČÍSELNÉ SÚSTAVY

### **Desiatková**

Základom našej bežnej číselnej sústavy – decimálnej – je číslo 10. Počítame od 1 do 9 a potom prejdeme na nový stĺpec pre desiatky.

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

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

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

A tak ďalej.

### **Dvojková**

V prvých počítačových systémoch sa používala dvojková číselná sústava, ktorá sa označuje aj ako *binárna*. Dvojková sústava je založená na čísle 2, takže jediné číslice, ktoré sa používajú, sú 0 a 1.

$$10 = 1 \times 2 \text{ plus } 0 \times 1, \text{ t. j. číslo } 2 \text{ v desiatkovej sústave}$$

$$11 = 1 \times 2 \text{ plus } 1 \times 1, \text{ t. j. číslo } 3$$

$$111 = 1 \times 4 (2^2) \text{ plus } 1 \times 2 (2^1) \text{ plus } 1 \times 1 (2^0), \text{ t. j. číslo } 7$$

Výber medzi 0 a 1 sa dal prepojiť prepínačmi na počítačových obvodoch, kde 0 = „vyp“ a 1 = „zap“, a kód zapísaný v dvojkovej sústave tak okruhy pri výpočtoch podľa potreby zapína a vypína.

### **Šestnástková**

V súčasnosti sú počítače oveľa zložitejšie a kódy sa často zapisujú pomocou *šestnástkovej* číselnej sústavy na základe čísla 16. V nej sa používajú čísla od 0 do 9, ale okrem toho sa používa aj písmeno A ako desiatka, B ako jedenásťka a tak ďalej, až po F ako pätnásťka.

C tak v desiatkovej sústave znamená 12

10 je šestnástkový spôsob zápisu čísla 16

11 = sedemnášť

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

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

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

$$100 = 256$$

## LÚŠTENIE KÓDOV

Lúštenie kódov zvyčajne znamená dekódovanie správ bez prístupu k tajnému kľúču, ktorý použila osoba, čo napísala danú správu. Táto činnosť sa odborne nazýva *kryptoanalýza* a osobitný spôsob kódovania sa označuje aj ako *šifrovanie*.

### Kým prišli počítače

Do príchodu digitálnych počítačov sa pri kódovaní používali písmená, prípadne čísla, ktoré zastupovali písmená. Každé písmeno v správe sa môže napríklad nahradiť iným písmenom. V jednoduchom kóde by sa namiesto A používalo písmeno E, B by nahradilo F a tak by to platilo pre celú abecedu. Prípadne by sa abeceda nejako poprehadzovala.

Na vyriešenie takejto šifry je dobré spočítať, ako často sa každé písmeno objaví v zašifrovanom texte (to sa nazýva *frekvenčná analýza*) a potom hádať jednotlivé zámeny. Vo veľkom počte slov sa napríklad objavuje písmeno „a“ a ak je takým písmenom v kódovanej správe písmeno „z“, potom to môže znamenať, že „z“ = „a“. To môže stačiť na zistenie zvyšných zámen, keďže pôvodná správa musí dávať zmysel.

Komplikovanejšie šifry môžu používať rozličné kódovanie abecedy pre každé písmeno abecedy – a na výber je naozaj veľký počet možných kódovaní: 46 písmen v abecede (26 v jednoduchšej abecede bez diakritických znamienok a zložených písmen), 46 možných písmen pre prvé písmeno, 45 pre druhé, 44 pre tretie a tak ďalej.

### Moderné lúštenie kódov

Moderné metódy nepracujú s písmenami, ale s bitmi (1 a 0) v pamäti počítača. Kódovanie a dekódovanie používa tajný kľúč, ktorým je dlhá sekvencia bitov (jednotiek a núl). Kľúč s dĺžkou 256 bitov sa dnes považuje za dostatočne odolný na to, aby zabránil dekódovačom používajúcim superpočítače odhaliť kľúč pomocou hrubej sily (t. j. odskúšaním každého možného kľúča).

LÚŠTENIE KÓDOV  
NYÜVHÔLH MREQY  
(+ 4 písmená)

GREGOR  
IŠGIPŠ  
(+ 3 písmená)

ANKA  
ŽMJŽ  
(- 1 písmeno)



Erik zalapal po dychu. Očividne nemal ani tušenia, čo zamýšľa. „Ale to nemôžete!“ zvolal.

„Ale áno, môžem!“ oponovala Beryl. „Je to dar pre vašu katedru matematiky na univerzite. A vy ste ten správny človek – keď vezmem do úvahy vašu prácu na kvantových počítačoch, neviem si preň predstaviť lepši domov.“

„Čo sú kvantové počítače?“ opýtal sa rýchlo Gregor. Bola to preňho novinka, navyše náramne vzrušujúca. Erik bol už dosť dlhý čas veľmi tajnostkársky – Gregor nebol schopný zo skvelého vedca dostať viac, ako len veľmi neurčitú odpoveď na otázku, na čom práve teraz pracuje. Zdalo sa však, že dnes večer je Erik zhovorčivejší, ako býval zvyčajne.

„Je to ďalšia veľká zmena,“ povedal Gregorovi. „V počítačovej oblasti sme zažili digitálnu revolúciu a teraz sme na pokraji kvantovej revolúcie. Keby sme dokázali vyrobiť kvantový počítač – a zároveň ho ovládať, čo sa momentálne zdá veľmi komplikované –, mohli by sme robiť veci, ktoré sú s dnešnou generáciou počítačovej technológie nepredstaviteľné.“

„Ako čo?“ opýtal sa Gregor.

„S kvantovým počítačom by sme dokázali rozlúštiť každý kód – na Zemi nejestvuje taký bezpečnostný systém, ktorý by ho mohol zastaviť!“ povedal Erik rozjarene. „Mohli by sme s jeho pomocou urobiť úžasné veci v oblasti spracovania informácií, medicíny, fyziky, techniky či matematiky. Je to ďalší veľký krok.“

„Ale čo to má spoločné s Enigmou?“ nechápal Gregor.

## ENIGMA

### **Vojnové tajomstvá**

V čase druhej svetovej vojny (v rokoch 1939 až 1945) využívali bojujúce strany stroje ako *Enigma* (v Nemecku) a *Typex* (v Spojenom kráľovstve) na kódovanie dôležitých správ.

Pracovník, ktorý obsluhoval stroj Enigma, napísal správu na klávesoch na prednej časti zariadenia, ktoré potom vytvorilo zakódovaný text, pričom každé zakódované písmeno ukázalo pomocou jeho osvetlenia malou elektrickou žiarovkou.

Zakódovaná správa sa ručne zaznamenala, previedla sa do morzeovky a napokon sa odoslala prostredníctvom rádiovej komunikácie.

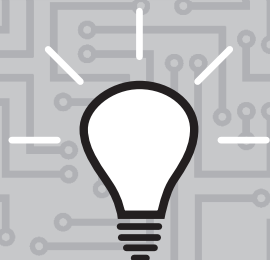


### **Tri rotory**

Šifrovací stroj Enigma mal tri rotory – *kolieska* – so zložitým prepojením. Rotory sa dali vyberať a vkladať v rozličnom poradí a následne sa dali otáčať tak, že každý z rotorov sa mohol nachádzať v ktorejkoľvek z 26 rôznych polôh.

To znamená, že existovalo šesť možných spôsobov nastavenia troch rotorov ( $3 \times 2 \times 1$ ) a potom  $26 \times 26 \times 26$  pozícií každého písmena. Aby to bolo ešte komplikovanejšie, do prepájacieho panela na čelnej strane zariadenia sa dalo zapojiť až desať krátkych káblov – pričom každý z mnohých spôsobov zapojenia vytváral úplne nový súbor  $26 \times 26 \times 26$  šifier, ktoré sa mohli v správe použiť. Na strane príjemcu bol ďalší šifrovací stroj Enigma, ktorý bol nastavený presne takým istým spôsobom a na ktorom sa potom zadával zakódovaný text. Pôvodný text bolo možné následne získať zaznamenávaním postupne rozšvecovaných písmen. Každý pracovník, ktorý obsluhoval Enigmou, dostal každý deň informáciu, na aké miesto je potrebné založiť jednotlivé rotory, v akej pozícii sa majú nachádzať a ako treba zapojiť káble na prepájacom paneli.

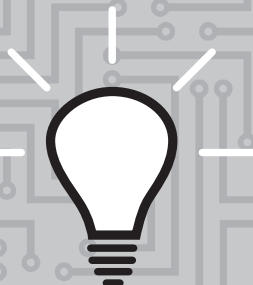
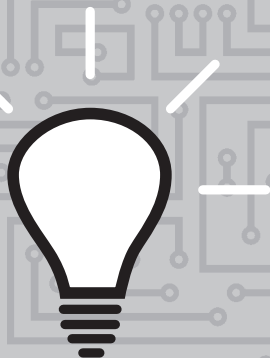




### **Rozlúštenie Enigmy**

Kódovací systém sa spoliehal na spoločné tajomstvo, v tomto prípade to boli denné pokyny na nastavenie a používanie zariadenia – a problémom bolo zaistiť, ako ho bezpečne môžu používať viacerí ľudia. Chyba niektorého z nich by mohla prezradiť dôležité informácie a vytlačené pokyny sa dali ukradnúť alebo zachytiť.

Vďaka kombinácii niekoľkých nemeckých chýb, vyššej matematiky a vynaliezavosti dokázali dekodovatelia – najprv v Poľsku a neskôr v anglickom Bletchley Parku – odhaliť nastavenia prístrojov Enigma a boli schopní lúštiť nemecké správy. Kľúčovou súčasťou metódy bolo špecifické zariadenie, ktoré navrhol geniálny matematik Alan Turing, nazývané Bomba. Ďalším dôležitým zariadením, ktoré vytvorili v Bletchley Parku, bol Colossus – prvý elektronický programovateľný digitálny počítač –, ktorý sa používal na dešifrovanie kódu. Ten nevytvárala Enigma, ale iný nemecký šifrovací stroj s názvom *Lorenz*.



# UNIVERZÁLNY TURINGOV STROJ

## **Fiktívne zariadenie**

V roku 1936 sa ako počítač označoval človek, ktorý vykonával výpočty. Turingov stroj, ktorý vytvoril geniálny matematik Alan Turing, mal byť jednoduchým fiktívnym zariadením schopným reprodukovať všetko, čo môže ľudský počítač potrebovať pri počítaní. Ide teda skôr o matematický a nie reálny stroj, zariadenie, ktoré slúži na porozumenie toho, čo je to výpočet a čo možno výpočtom dosiahnuť. Nemohlo však reálne existovať, keďže sa napríklad predpokladá, že má nekonečnú pamäť aj nekonečný čas na vykonávanie operácií, pričom ani jedno nie je možné.

## **Reťazec núl...**

Fungovanie stroja sa najprv definuje konečným zoznamom kódovaných pokynov. Predstavte si veľmi dlhú pásku, na ktorej je napísaný dlhý reťazec núl (po celej dĺžke pásky). Páska siaha na každej strane donekonečna (predpokladajme, že je nekonečne dlhá) a predstavuje pamäť počítača. Medzi týmito nulami je roztrúsené konečné množstvo jednotiek, ktoré predstavujú údaje zadané do stroja. Na tejto páske je položené spracovateľské zariadenie (procesor); to dokáže čítať len jeden symbol, ktorý sa pod ním práve nachádza a ktorý môže nechať bezo zmeny alebo ho nahradiť 0 alebo 1.

Okrem toho obsahuje aj hodiny, ktoré ustavične tikajú a pri každom tiknutí procesor prečíta symbol, ktorý práve vidí. Potom vykoná jednu z dvoch vecí na základe toho, čo práve prečítal, a jeho aktuálneho stavu. Môže:

- zmeniť symbol pod sebou a označiť ho ako 0 alebo 1, potom sa posunúť na páske o jedno miesto doľava alebo doprava, prípadne sa zmeniť do iného stavu a potom čakať na ďalšie tiknutie,
- alebo vykoná rovnaké kroky, ale potom sa zastaví (vypne).

To, čo *naozaj* urobí, závisí od pravidiel (programu), ktoré mu zadáme, a od toho, čo prečíta na páske. Predpokladajme napríklad, že stroj začne v stave 0 s dlhým reťazcom núl na páske a že niekde napravo sa niektoré z týchto núl zmenili na 1 – tieto jednotky tvoria vzor; tým je binárne číslo, ktoré zadávame stroju ako jeho vstup.

Dobрым pravidlom na začiatok je: *ak je v stave 0 a prečíta 0, má prepnúť na stav 0, napísať 0 a posunúť sa vpravo.*





To znamená, že keď stroj vidí pôvodne 0 (keď je v stave 0), zostane v stave 0, nemení 0 na páske a posunie sa o krok doprava. Ak páska jeden krok vpravo takisto uvádza 0, prebehne to isté – stroj zostane v stave 0, nechá pásku bezo zmeny a posunie sa o ďalší krok vpravo.

To sa stane pri každom tiknutí hodín, kým stroj napokon nenarazí na prvú z 1, ktoré sú uvedené na páske. Teraz potrebuje pravidlo, ktoré mu povie, čo má robiť, keď prečíta 1 v stave 0. Najjednoduchšie pravidlo by bolo: *zostať v stave 0, napísať 1, posunúť sa o ďalší krok doprava a zastať*. Na ľavej strane stroja sa teraz objaví 1, čo je výsledok výpočtu.

Tento veľmi jednoduchý výpočet by sme mohli opísať ako „vytlačiť 1, ak je vstup platný“, pričom platný znamená, že „obsahuje aspoň jednu 1“. Ak by napravo od miesta, na ktorom stroj začína, neboli žiadne 1, tak by jednoducho pokračoval v krokoch smerom doprava a hľadal 1 donekonečna – nezastal by, ale bezvýsledne by pokračoval v práci. To sa môže stať na skutočnom počítači – program sa môže dostať do nekonečnej „slučky“ alebo sa „zacykliť“, kým sa systém počítača nezrúti. Táto možnosť je, žiaľ, základnou vlastnosťou Turingovho stroja aj skutočných počítačov. Môžeme však tomu jednoducho zabrániť tak, že budeme trvať na tom, že „platné“ vstupy musia obsahovať aspoň jednu 1, aby sa prvé pravidlo nemohlo používať donekonečna.

### **Každý možný výpočet**

V prípade dostatku času a možnosti napísať na pásku toľko 1, koľko je nutné, by sa každá mechanická operácia s celými číslami, ktoré si dokážeme myslieť, mohla vykonať tak, že by sa do Turingovho stroja zadali čísla na pravej strane stroja, spustili by sa hodiny a čakalo by sa na zastavenie stroja. Potom by sa na ľavej strane stroja prečítal výsledok. To zahŕňa všetky aritmetické výpočty, ktoré kedy človek dokázal vypočítať na papieri. Alan Turing uviedol, že to, čo jeho stroj dokáže vypočítať, by sa malo považovať za definíciu toho, čo sa vôbec dá vypočítať. Prekvapivo takmer 80 rokov po sformulovaní jeho teórií sa to stále všeobecne považuje za dobrú definíciu, pretože každý známy koncept digitálneho počítača dokáže vypočítať len to, čo dokázal vypočítať Turingov stroj.

Turing matematicky dokázal aj to, že ani Turingov stroj nedokáže vyriešiť každý problém. Inými slovami, počítač nedokáže vyriešiť každý matematický problém – počítače ešte nedokážu nahradiť matematikov.

„Enigma,“ odvetila Beryl, „je predchodcom všetkých možných ohromujúcich technológií, ktoré sa objavili neskôr. A, samozrejme, Enigma naozaj existovala a fungovala. Pritom kvantový počítač v tejto chvíli ešte tak ďaleko nie je.“

„Presne – ha-ha-ha!“ zasmial sa Erik. „Väčšinu času teraz venujem detekcii kvantových chýb...“

„Erik,“ prerušila ho Beryl, „je zrejme jediný človek na svete, ktorý by dokázal ovládať kvantový počítač – ak by teda nejaký existoval.“

Erik sa tváril spokojne. „Detekcia kvantových chýb v podstate znamená uistenie, že keď sa nám podarí spustiť kvantový počítač, budeme schopní mať ho viac-menej pod kontrolou. Čo však v súčasnosti nevyzerá veľmi pravdepodobné! Takýto problém s Enigmou nemali.“

„Mohli by sme vyskúšať Enigmu? Mohli by sme si s Ankou posielat kódované správy?“ opýtal sa Gregor.

„Enigma nevie *posielat* správy,“ odvetila Beryl a dopila sherry. „Používa sa na kódovanie a dekodovanie, ale na prenos potrebujete iný spôsob. Takéto zakódované správy sa zvyčajne posielali cez rádio pomocou morzeovky. Dnes už máme technológie, ktoré dokážu oboje – každú sekundu kódujú miliardy správ a rozosielaajú ich po svete prostredníctvom káblov alebo rádiových vĺn a tieto správy potom zasa iné počítače dekodujú. Každý e-mail, každá požiadavka na webovej stránke a každý počítačový príkaz je kódovaná správa, a hoci by niektoré kódy mali byť zrozumiteľné všetkým – lebo inak by bol internet v peknej kaši –, keď

si online kúpite ponožky, určite by ste chceli, aby bolo zakódované aspoň číslo vašej platobnej karty, aby vám nikto nemohol ukradnúť peniaze. Zoberte si počítače po celom svete, ktoré riadia fungovanie dôležitých vecí – a stačí spomenúť len tri – elektrina, doprava a obrana. Všetky musia používať kódovanie, aby tak zabránili nesprávnym ľuďom narobiť veľké problémy. Keby ste dokázali prelomiť takéto kódovanie, mali by ste svet v hrsti.“

„Také nápady im radšej nepodsúvajte,“ povedal Erik s hranou prísnosťou. „Nemám chuť písať žiadosť o ich vydanie, keď sa rozhodnú prehrabať do nejakého supertajného vládneho programu.“

„To by bola zábava!“ zvolala Beryl. „Dúfam, že niečo také urobia!“

Gregor sa pozrel na Anku. Beryl musí mať určite veľa zaujímavých historiek, pomyslel si.

„Zrejme máte na ľudí dobrý vplyv, však?“ poznamenal Erik, ale nevyzeral ani trochu nahnevane. „Tak poďme, vy dvaja, zmiznite, kým vás Beryl nenaverbuje do nejakého detského oddelenia tajných služieb.“



„Ale, oci!“ pošťazovala sa Anka, ktorej záujem bol teraz už dosť veľký na to, aby odložila telefón. „Ja chcem vstúpiť do tajných služieb! To je moje úplne najväčšie želanie v živote! Môžeme ešte zostať?“