1. Úvodní postřehy

V první zprávě se dočteme, že čísla na okrajích mají čistě pomocný charakter. Po chvilce počítání je zřejmé, že označují celkový počet znaků na předchozích řádcích. Když z velkého textu čteme každý první znak ze dvou, získáme druhou zprávu; ta ohledně způsobu luštění neříká nic zajímavého. Když z nevyškrtaných písmen čteme každý první znak ze tří, získáme třetí zprávu; ta říká cosi o obsahu tajenky, ale zároveň upozorňuje, že je to pouze kontrolní informace. Nyní se nabízí z nevyškrtaných písmen číst každé první ze čtyř, ale ejhle, místo očekávaného textu `CTVRTAZPRAVA...` dostáváme jen `CVTZRV...`, tedy každé druhé písmeno z toho, co bychom čekali, chybí. Všimneme si ovšem, že očekávaná písmena v textu jsou, a to vždy na čtvrté pozici ze čtyř, a když tedy přečteme každé první a čtvrté písmeno ze čtyř, získáme smysluplnou čtvrtou zprávu. Ta říká mimo jiné, že periody jsou zvoleny nanejvýš intuitivně; tedy bychom čekali, že perioda n-té zprávy je n. Zbylý text nyní zní `ORIPSBAOSE...` Pokud v něm nyní chceme číst `PATA`, musíme vybrat z první pětice právě čtvrté písmeno a z druhé pětice právě druhé písmeno, což nesedí s tím, že perioda má být 5. Náš dosavadní pohled na čtení zpráv je tedy nejspíš špatný!

Pokud chceme dočíst čtvrtou zprávu dostatečně daleko, máme k dispozici pracný a intelektuálně nenáročný postup: pokračujeme ve vyškrtávání druhé a třetí zprávy i tam, kde jsou už jen hovna a sračky, a pro čtvrtou zprávu vždy ze zbytku dvě písmena čteme a dvě nečteme. Můžeme si ale uvědomit, že vzdálenosti mezi písmeny čtvrté zprávy v rámci celého (nevyškrtaného) textu jsou vždy střídavě 8 a 4, takže můžeme číst čtvrtou zprávu snadno i tam, kde nemáme vyškrtanou druhou ani třetí. Po chvíli hledání páté zprávy vidíme, že vzdálenosti mezi jejími znaky jsou vždy střídavě 20 a 40. Nyní už bychom si měli všimnout, že tyto vzdálenosti pro n-tou zprávu jsou vždy násobky n, a navíc vždy čteme všechna písmena, která nejsou součástí dřívější zprávy. Správný pohled na čtení zpráv tedy není ten, že bychom písmena vyškrtávali a pak se zajímali o zbytek; naopak se vždy zajímáme o celý text a n-tou zprávu čteme tak, že vybereme každý n-tý znak, přičemž nečteme ty, které jsou součástí dřívější zprávy.

Jak ale zjistit, kde která zpráva začíná? Čtvrtá zpráva říká, že offsety nejsou zvoleny tak intuitivně, ale stále jsou zvoleny systematicky, a to tak, aby daly vzniknout krásné struktuře této šifry. V tuto chvíli se tedy nejspíš nezvládneme dovtípit, podle jakého vzorce jsou offsety zvoleny.

Ale je tu mnohem důležitější otázka: Kde číst tajenku? Po vyškrtání 2.–5. zprávy zní text `ORISBOSEEMAJ...` a je jasné, že přinejmenším písmena `R` a `I` není jak vyškrtnout. Zdá se tedy, že tajenka bude sestávat z toho, co není obsaženo v žádné zprávě. Ale vyškrtávat všechny ty zprávy je tak strašnej vopruz! Nicméně čtvrtá zpráva říká, že offsety jsou zvoleny tak, aby daly vzniknout nějaké struktuře — nejspíš tedy ani tajenka nebude jen tak náhodně rozházená, ale její pozice budou mít nějakou pravidelnost a pro úspěšné vyluštění této šifry je nezbytné přijít na to, jakou.

Možných přístupů je nyní více; v zásadě se dají rozdělit na (a) fištrónský a (b) exaktní.

2.a. Fištrónské řešení

Ve zbylém textu se snažíme hledat další zprávy. Šestou zprávu se nějak nedaří najít. (Pokud jsme přečetli pátou zprávu až po její 61. písmeno (na pozici 1822), tak již víme, že šestá zpráva v textu není.) Začátek sedmé i osmé zprávy ale lze identifikovat poměrně snadno a zbylý text pak zní `ORIBEJTH...` Nyní potřebujeme netriviální skill pro interpretaci zkratkovité tajenky (jak říká druhá zpráva) anebo nápovědu — ta mimo jiné říká, že první tři písmena tajenky jsou začátek desetipísmenného přídavného jména; je to tedy originální, orientální, ... nebo snad orientační? Domyslíme si, že `J` a `T` patří dalším zprávám (konkrétně jedenácté a třinácté, ale to už není podstatné) a máme to: orientační běh! Co je podstatné (a k čemu nabádá i nápověda), je podívat se na vzdálenosti mezi pozicemi tajenky. Vyjde 4, 8, 16, 32, 64. A vida, vzdálenost se vždy zdvojnásobuje. Není tedy potřeba nic vyškrtávat, stačí vždy spočítat další pozici a vyhledat ji v textu. Dostáváme tak `ORIBEHTRI`, a jelikož všechno souhlasí s informací ze třetí zprávy (sedmé je T, poslední I), není důvod se nevydat do nedalekého Areálu pevných kontrol pro orientační běh Rosnička na kontrolu číslo tři. Ale tam nic nenajdeme. Že bychom tedy neměli tajenku správně? V průběhu luštění nás určitě napadlo, že když je každá zpráva nekonečná, bylo by pěkné, kdyby i tajenka byla nekonečná. Navíc třetí zpráva říká, že sedmý *znak* je T a poslední *písmeno* je I. Je tedy možné, že tajenka je skutečně nekonečná, ale dále sestává ze znaků, které nejsou písmena. Podíváme se tedy na další pozici tajenky (2050), a tam je tečka! Z toho asi moc moudří nejsme, takže nezbývá než se podívat na další pozici (4098), a tam je (velmi malá, ale stále dobře čitelná) devítka! Pokud z toho stále nejsme moudří, musíme se podívat ještě na další pozici (8194), a tam je (miniaturní, ale s dobrým zrakem/lupou/foťákem/mobilem stále čitelná) další devítka. Nyní už bychom se měli dovtípit, že tajenka je skutečně nekonečná a zní `ORIBEHTRI.999999...`, a tedy další stanoviště je na kontrole číslo čtyři.

2.b. Exaktní řešení

Exaktní přístup spočívá v tom, že (1) zjistíme vzorec pro offsety a (2) spočítáme pozice tajenky.

2.b.1. Zjištění offsetů

Jelikož ze čtvrté zprávy tušíme, že vzorec pro offsety asi nevykoukáme, nezbývá než se o tom něco dočíst v některé zprávě. A jsou hned dvě možnosti:

Tou první — intelektuálně snazší, zato mnohem pracnější — je, že dočteme pátou zprávu opravdu hodně daleko. Jestliže už aspoň chápeme, že její pozice jsou 22 a 42 s periodou 60, je to zvládnutelné a navíc dobře paralelizovatelné. Pokud z ní přečteme prvních 150 písmen (pozice 4482), dozvíme se, že první pozice pro šestou zprávu splývá s šestým znakem druhé zprávy, tj. šestá zpráva by začínala na pozici 11 (a jako záchrana pro týmy, které ještě nepochopily, že n-tá zpráva má periodu n, pokračuje pátá zpráva výčtem všech potenciálních pozic šesté zprávy). Offsety pro jednotlivé zprávy (počínaje druhou) jsou tedy $1, 2, 4, ?, 11, \ldots$ Navíc víme, že offset páté zprávy dává zbytek 2 modulo 5. Taky se zdá, že offsety jsou rostoucí; jedinou možností je tedy 7. A nyní už bychom si měli všimnout, že vzdálenost mezi offsety pro danou dvojici sousedních zpráv je vždy o jedna větší než u předchozí dvojice. (Snadno zkontrolujeme, že to pro každou další n-tou zprávu sedí modulo n.)

Tou druhou — intelektuálně náročnější, ale zdaleka ne tak pracnou — je chytit se toho, co říká čtvrtá zpráva, a najít šestnáctou zprávu. Už po vyškrtání 2.–5. zprávy je jasné, že nemůže začínat `Skem` na pozici 30 (začínala by `SOAZRANOS...`) ani na pozici 54 (začínala by `SMPAVMEBHZE...`), ale začíná na pozici 138 (`SESTNACTARZPRAVANNEOOBSAHUJUNE...`). Samozřejmě se tam pletou znaky z dřívějších lichých zpráv; pokud jsme zkušení skrebliči, tak nám to nevadí. (V opačném případě si můžeme vypsat všechny pozice $138 + 16k$ pro $k \geq 0$ (`SEASRETNIAATCTEA...`) a uvědomit si, že každá dřívější lichá n-tá zpráva v nich pokryje každý n-tý znak (jelikož n a 16 jsou nesoudělná čísla).) Po přečtění prvních 66 písmen (pozice 2794) se dozvídáme, že offsety jsou trojúhelníkové. (Pokud tento pojem neznáme, lze snadno vygooglit, že trojúhelníková čísla jsou ta, která jsou tvaru $1 + 2 + 3 + \ldots + n$, tj. $0, 1, 3, 6, 10, \ldots$) Pokud indexujeme pozice od nuly, tak nám to přesně sedí (jemným hintem na to, že může být pro tuto šifru přirozenější indexovat od nuly, je fakt, že čísla na okrajích jsou od nuly); v opačném případě jsou pro nás offsety 2.–4. zprávy 1, 2, 4, z čehož odtušíme, že jsme prostě jen v indexování posunutí o jedničku. (Pro případ, že bychom se nedovtípili, co jsou trojúhelníková čísla, pokračuje šestnáctá zpráva výčtem offsetů jednotlivých zpráv.) Opět lze snadno zkontrolovat, že to pro každou n-tou zprávu sedí modulo n.

2.b.2. Čtení tajenky

Teď, když už víme, kde jsou pozice každé ze zpráv, jsou i pozice tajenky pro nás jednoznačně určeny. A opět máme dvě možnosti, jak je zjistit:

2.b.2.a. Informatické řešení

Napíšeme si jednoduchý programek, který vyškrtá všechny pozice zpráv a vypíše ty zbylé: $6, 10, 18, 34, 66, \ldots$

2.b.2.b. Matematické řešení

Už víme, že n-tá zpráva začíná na pozici $(1+2+\ldots+(n-2))+1 = (n-2)(n-1)/2+1 = (n^2-3n+2)/2+1 = n(n-3)/2+2$. Otázka tedy je, která přirozená čísla se nedají vyjádřit jako $n(n-3)/2+2+kn$ pro $k \geq 0$, $n \geq 2$. Nejprve se zamyslíme nad tím, jak vycházejí pozice n-té zprávy modulo n. Abychom se zbavili nepěkného dělení dvěma v našem vzorci, oddiskutujeme paritu čísla n:

Pro $n = 2k$ je $n(n-3)/2 + 2 = 2k(2k-3)/2 + 2 = k(2k-3) + 2 = 2k(k-2) + k + 2 = n(k-2) + k + 2$, což je kongruentní s $k + 2$ modulo n.

Pro $n = 2k + 1$ je $n(n-3)/2 + 2 = n((2k+1)-3)/2 + 2 = n(k-1) + 2$, což dává zbytek 2 modulo n.

Vidíme tedy, že by se nám nad úlohou uvažovalo lépe, kdybychom si indexování pozic posunuli o dvojku, tj. indexovali je od -1 (jakkoli podivně to zní). Pak jsou pozice lichých n-tých zpráv na násobcích čísla n a pozice sudých n-tých zpráv na lichých násobcích čísla $n/2$. Zejména tedy pokud n má lichého dělitele l, pak každá pozice n-té zprávy je i násobkem čísla l.

Uvažme nyní pozici $p = 2^a$. Jelikož 2^a není násobek žádného lichého $l > 1$, může být pokryta n-tou zprávou jedině pro $n = 2^b$. A jelikož p musí být lichý násobek čísla $n/2$, jediná možnost je $b = a + 1$, tedy $n = 2^{a+1}$. Tato zpráva však začíná až na pozici $n(n-3)/2 = 2p(2p-3)/2 = p(2p-3) > p$ pro $p > 2$. Jediné mocniny dvojky, které můžou být pokryté nějakou zprávou, jsou tedy 1 a 2 (a ty skutečně pokryté jsou); všechny ostatní jsou nutně součástí tajenky.

Nyní naopak ukážeme, že všechny pozice p, které nejsou mocninou dvojky, jsou pokryté nějakou zprávou. Pro první dvě pozice (-1 a 0) je to pravda; pro $p \geq 3$ pišme $p = l \cdot k$, kde $l > 1$ je (libovolný) lichý dělitel čísla p. Ukážeme, že pozice p je pokryta l-tou nebo $2k$-tou zprávou. Modulo sedí, takže p by mohla být nepokrytá jedině proto, že obě zprávy začínají později. To by znamenalo, že $l(l-3)/2 > p$, tedy $(l-3)/2 > k$, tedy $l - 3 > 2k$; a zároveň $2k(2k-3)/2 > p$, tedy $2k - 3 > l$, tedy $2k > l + 3$, což dohromady dává $l - 3 > l + 3$, a to je spor.

Došli jsme tedy k závěru, že (v původním indexování od jedničky) jsou pozice tajenky právě čísla $2^a + 2$ pro $a \geq 2$.

2.b.2.b.1. Jen tak pro zajímavost...

...se ještě můžeme zamyslet nad tím, že zprávy jsou skutečně nekonečné a které zprávy se v textu vlastně vyskytují. Zřejmě pokud na pozici p je znak n-té zprávy, pak n-té zprávě patří (přinejmenším) také pozice $p+n!$, $p + 2 \cdot n!$, $p + 3 \cdot n!, \ldots$ Každá zpráva je tedy buď nekonečná, nebo zcela nepřítomná.

A nyní k tomu, které zprávy se v textu nachází. Uvažme nejprve číslo n, které má lichého dělitele l, $1 < l < n$. Už jsme si rozmysleli, že všechny pozice n-té zprávy jsou násobky čísla l. Ovšem vzhledem k tomu, že offsety zpráv jsou rostoucí, začíná l-tá zpráva dříve než n-tá, a tak všechny pozice n-té zprávy jsou pokryté už (přinejmenším) l-tou zprávou. Proto se n-tá zpráva v textu nevyskytuje. (Nenechme se zmást tím, že např. pro $n = 6$ tento argument tvrdí, že šestá zpráva v textu není, protože je zabitá třetí zprávou; zatímco pátá zpráva tvrdí, že šestá zpráva v textu není, protože je zabitá druhou zprávou. Pravda je obojí.) Zjistili jsme tedy, že pořadí zprávy, která se v textu vyskytuje, je nutně mocninou dvojky nebo prvočíslem.

Uvažme tedy nyní číslo $n = 2^a$, kde $a \geq 1$, a pozici $p = 2^{a-1}$. Jak jsme si již rozmysleli výše, pozice p je pokryta pouze n-tou zprávou, takže n-tá zpráva se v textu vyskytuje.

A konečně zbývá případ, že n je liché prvočíslo. Nechť a je takové, že $2^a < n < 2^{a+1}$, a uvažme pozici $p = 2^a \cdot n$. Tato pozice je násobkem čísla n, takže je pokryta n-tou zprávou. Kterými dalšími zprávami je pokryta? Jistě ne žádnou lichoprvočíselnou, jelikož p není dělitelné žádným lichým prvočíslem kromě n. A pokud je pozice p pokryta m-tou zprávou pro $m = 2^b$, pak musí být $b = a + 1$ (aby seděl zbytek modulo m), tedy zejména $m > n$, takže pozice p skutečně patří n-té zprávě.

Dokázali jsme tedy, že v textu se vyskytují právě zprávy, jejichž pořadí je mocninou dvojky nebo prvočíslem (výčet těchto čísel je pro zajímavost zahrnut v osmé zprávě).

3. Pár slov na závěr

3.1. Co (ne)považujeme za řešení

Tuto šifru považujeme za vyřešenou až ve chvíli, kdy tým dokáže (ať už fištrónem, informaticky, či matematicky) spočítat pozice tajenky. Zejména tedy nepovažujeme za řešení šifry urputně vyškrtávat všechny zprávy. Také proto byla tajenka záludně zvolena tak, aby její začátek naváděl na jinou kontrolu a aby si týmy musely uvědomit, že tajenka je nekonečná, a přečíst si i její další znaky. Na druhou stranu jsme do třetí zprávy dali dost informací na to, aby se urputně škrtající týmy mohly poměrně rychle dovtípit, že se jedná o číslo tři, a neuškrtaly se až do úplného vyčerpání...

Ultrafištrónským řešením, vyžadujícím nesmírnou všímavost, by bylo v textu rychle postřehnout tečku a devítky, uvědomit si, že jejich pozice (2050, 4098, 8194) jsou velmi blízko mocninám dvojky (nebo že vzdálenosti mezi nimi jsou přesně mocniny dvojky), a z toho si domyslet všechny pozice tajenky.

3.2. O vzniku této šifry

Na úplném začátku byl nápad udělat nekonečný text, z něhož by se nějak pravidelně vyškrtávaly jednotlivé nekonečné zprávy, a zbytek by pak tvořil nekonečnou tajenku. Prvotní idea skutečně byla se po vyškrtání vždy zajímat už jen o zbytek textu, ovšem při tomto pohledu na věc žádný systematický vyškrtávací vzorec nevedl k pravidelným pozicím tajenky, a celá šifra by pak byla řešitelná jen urputným vyškrtáváním nebo informatickým přístupem, což by nebylo pěkné.

Bylo tedy nutné změnit pohled na vyškrtávání a uvažovat vždy celý text. Také by bylo hezké, kdyby se v textu nacházely všechny zprávy; to ale — jak si lehce rozmyslíme — také není možné. Modulo 12 totiž druhá zpráva obsadí 6 pozic, třetí další 2, čtvrtá další 2, šestá další jednu a dvanáctá tu poslední, takže text by obsahoval jen 2.–12. zprávu a navíc by tajenka byla konečná.

Nezbývalo tak než se smířit s tím, že některé zprávy v textu nebudou. Po vyčerpávajícím hledání nějakého aspoň trochu intuitivního systému, jak volit offsety, aby měla vzniklá tajenka pravidelnou strukturu, se nakonec našla stávající varianta s trojúhelníkovými offsety. Uznáváme, že ta volba offsetů je tak trochu „spadlá z nebe“, a kdyby je šlo zvolit nějak pěkněji, tak bychom to rádi udělali, ale matematická realita je holt neoblomná. :-)