LITERATURA

Simon Singh: Kniha kódů a šifer. Utajování od starověkého Egypta po kvantovou kryptografii

Druhá kniha britského autora zřejmě indického původu předčí jeho první knihu Velká Fermatova věta. Autor je vzděláním fyzik, který pracoval pro BBC, a věnuje se popularizaci vědy. Kniha líčí tajemnou a utajovanou historii kryptografii, tedy vědy o šifrování dokumentů a boj kryptologů, kteří se snaží prolomit šifry. Autor prokázal značné schopnosti literární i popularizační a také zúročil dlouhou přípravu, kterou věnoval napsání knihy. Líčí osudy vědců, kteří se věnovali šifrování i dešifrování a vývoj šifrování od jednoduché záměny množiny znaků, kdy každému znaku je jednoznačně přiřazen právě jeden znak stejné abecedy, tedy tzv. monoalfabetické šifry po kvantovou kryptografii.

Kniha vyšla v roce 2017 v 2. vydání v nakladatelství Dokořán a ARGO, Praha. Na její úrovni se v českém překladu podíleli oba překladatelé –Petr Koubský, Dita Eckhardtová a odborný lektor překladu, přední český kryptolog Vlastimil Klíma. Kniha je krásná po literární a obsahové i formální stránce a designu a čte se jedním dechem. Mohu ji doporučit každému, kdo se zajímá nejen o šifrování, ale o historii vědy nebo společnosti obecně. Autor zařadil také kapitolu o luštění starověkých písem, tedy o rozluštění egyptských hieroglyfů, které rozluštili Thomas Young a Jean Francois Champollion, kteří použili tzv. Rosettskou desku, která obsahovala zápis v řečtině, démotickém písmu a hieroglyfech. Mnohem složitější bylo rozluštění tzv. minojského lineárního B písma. Při něm použili vědci jen dedukci, neboť neměli žádné vodítko ani nevěděli, v jakém jazyku jsou destičky napsány. Nejzajímavější byla kapitola o druhé světové válce, jejíž kryptologické objevy byly třicet let utajovány. Tato historie je známa z dokumentárních televizních seriálů nebo z filmu Kód Navajo. Chybí mi kapitola o sovětské kryptografii, která je zřejmě ještě utajována.

Jako matematik bych přivítal něco víc o matematických základech asymetrického šifrování. Vzhledem k tomu, že je kniha určena širokému okruhu čtenářů, nebylo to asi možné. Předností knihy je rozsáhlý seznam literatury a webových stránek. Autor zařadil také soutěž pro čtenáře v luštění šifer, která byla v originálu ohodnocena cenou 10 000 liber. V Česku vyšla také výborná kniha Simona Garfinkela PGP – Báječné soukromí, která obsahuje historii asymetrického šifrování a popis programu Phila Zimmermanna PGP. Také tuto knihu i program, který sám používám, mohu čtenářům doporučit.

Karel Vašíček