## Ukázka z kapitoly *5. Důležitá data a mezníky v dějinách kryptologie*

### 1499

Významným představitelem evropské kryptografie byl Němec Johannes Trithemius (někdy psán jako Tritheim) (1462-1516). Byl opatem benediktinského kláštera ve Spanheimu a od roku 1506 v klášteře Sv. Jakuba ve Würzburgu. Napsal řadu významných knih o historii, životopisný slovník slavných Němců, biografii o slavných benediktinech. Dopisoval si s řadou učenců své doby. Je však znám také tím, že se zasloužil o rozkvět vysoké magie v době renesance. Známé jsou jeho spisy *Antipalus maleficiorum* (Varování před černokněžnictvím, 1508) a *Steganographia* (1499). Ač byl označován za mága a kouzelníka, zachoval si kritický úsudek a sám před podvodníky a šarlatány varuje. Šarlatánem nazval např. i proslulého doktora Johannesa Fausta (1480 nebo1485 –1530?). Jeho okultní spisy jsou ovlivněny jeho obrovským zájmem a vírou ve skryté a tajemné síly. Např. roztřídil čarodějnice do 4 přesně definovaných kategorií, zabýval se tříděním andělů atd. Mezi tyto spisy lze zařadit knihu *Steganographia* (Tajné písmo), která se však částečně věnuje i kryptografii. V prvních dvou svazcích popsal elementární substituce (samohláska / souhláska) a utajení textu, kdy se čtou jen určitá písmena na určitých místech a ostatní písmena nedávají žádný smysl. Například lze pro získání otevřeného textu číst pouze druhá písmena z každého druhého slova. Věta : „Takže p**o**dle popisu u**k**áži jak t**o** fungovalo“ - je skrytý zápis slova OKO v popsaném systému.

Pro Trithemia sloužily tyto systémy především ke krytí a zamaskování magických operací, které jsou popsány ve třetí knize, která není věnována kryptografii. Pokud do kryptografie nebudeme počítat tu část, kde Trithemius popisuje, jak na dálku přenášet skrytě a bezpečně text.

Podle něj k tomu stačilo pouze říct zprávu modle nebo obrazu planetárního anděla v okamžik stanovený na základě složitých astrologických výpočtů, zahalit modlu, říci příslušnou formuli a zpráva došla na místo určení bez jakýchkoliv slov nebo šifrovaného textu nebo použití posla.

Jeho pověst a popularita, pokud jde o znalosti tajemných sil, natolik vzrostla, že jeho dílo *Steganographia* se šířilo v rukopisu po stovky let, mnoho lidí si je opisovalo a hledalo v knize tajemství, která tato kniha měla obsahovat. Jeden z opisů knihy vlastnil např. Giordano Bruno. Právě toto dílo způsobilo, že se v následujících letech kryptologie spojovala v obecném povědomí většiny lidí s alchymií a okultními vědami.

## 1508

V roce 1508 se pustil Johannes Trithemius (1452-1516) do psaní šestidílné knihy výhradně zaměřené na kryptologii. Tuto knihu nazval *Polygraphia*, a to vzhledem k rozmanitosti možných metod psaní, které se v knize vyskytují. Knihu (rukopis) věnoval 24. dubna 1508 císaři Maxmiliánovi I. Dva roky po jeho smrti byla kniha roku 1518 vytištěna, a stala se tak vůbec první tištěnou knihou pojednávající o kryptologii. Její celý název je *Šest knih o polygrafii od Johanna Trithemia, opata z Würzburgu, dříve ze Spanheimu věnované císaři Maxmiliánovi*. Kniha má 540 stran, je tištěna černým a červeným písmem.

V knize je představen jím navržený šifrový systém nazývaný Ave Maria. Šifra spočívá v tom, že jednotlivým písmenům jsou přiřazena celá slova. Seznam slov volí autor tak, aby dávala smysluplný text – jakousi nevinnou modlitbu. Tak třeba slovo abbot (opat) se zašifruje jako DEUS CLEMENTISSIMUS REGNES AEVUM INFINIVET, kde DEUS = A, CLEMENTISSIMUS = B, REGNES = B atd.

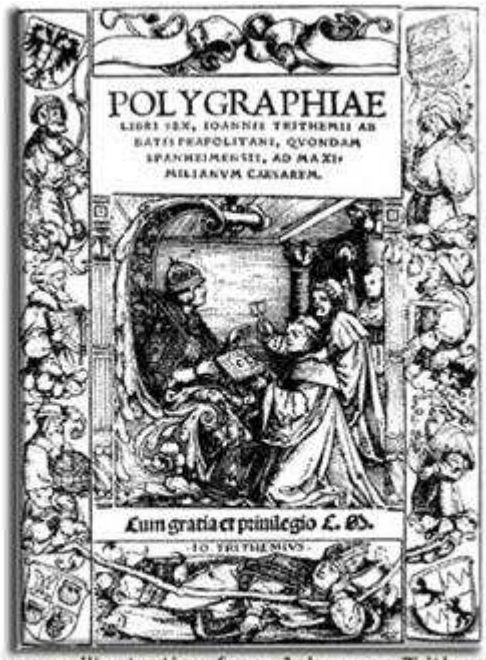
Ve druhé knize je připraveno 284 takovýchto abeced.

Obdobně v knize tři a čtyři jsou připraveny další abecedy, které však již tak nevinně nevypadají. V knize tři jsou použita běžná slova a v knize čtyři dokonce slova umělá.

V pátém díle, který je z kryptologického hlediska nejvýznamnější, je uvedena šifrovací tabulka, tzv. "tabula recta", která je základem pro polyalfabetické šifry.

abcdefghijklmnopqrstuvwxyz
bcdefghijklmnopqrstuvwxyza
cdefghijklmnopqrstuvwxyzab
defghijklmnopqrstuvwxyzabc
efghijklmnopqrstuvwxyzabcd
...
zabcdefghijklmnopqrstuvwxy

Trithemius používal této tabulky k polyalfabetickému šifrování velmi prostě a jednoduše. První písmeno otevřeného textu zašifroval pomocí první abecedy, druhé písmeno pomocí druhé abecedy atd. Slovo OKO by se



The title page illustration from Johannes Trithemius' 1518 "Polygraphiae libri sex" shows the author wearing his Benedictine habit and kneeling to present his book to the Holy Roman Emperor Maximilian.

zašifrovalo touto metodou jako OLQ (otevřené písmeno vyhledejte v prvním řádku a šifrový ekvivalent najdete pod ním v abecedě, která odpovídá pořadí písmene ve zprávě).
Bezpečnostním zlepšením proti polyalfabetickému systému Albertiho je, že se abeceda mění po každém písmenu.
Trithemius měl obrovský vliv na kryptologii. Bylo to jednak proto, že se těšil mimořádné pověsti a věhlasu a jednak proto, že jeho kniha o kryptologii, která byla první tištěnou knihou o tomto tématu, se stala pro zájemce relativně snadno dostupná.

## 1552-1557

Girolamo Cardano (1501-1576), milánský fyzik, astronom a matematik trpěl až chorobnou touhou získat popularitu. Za svého života napsal neuvěřitelné množství knih (131 vyšlo a dalších 111 zůstalo v rukopise). O kryptologii nenapsal samostatnou knihu, ale své poznatky uložil do dvou spisů věnovaných popularizaci vědy. První se nazýval *De Subtiliate* (1550) a druhý *De Rerum Varietate Libri XVII* (1557). Obě knihy si veřejnost oblíbila pro jejich jasný popis, využití zajímavých až anekdotických příběhů a bohaté ilustrace. Obsahovaly nejmodernější učení fyziky tehdejší doby a byly napsány velmi pokrokovým způsobem. Obě knihy byly překládány a vydávány po celé tehdejší Evropě.
Pokud jde o vývoj kryptologie, přidal Cardano další významnou myšlenku pro zvýšení bezpečnosti polyalfabetické šifry. Pochopil, že změna klíče, který se využívá k určení abecedy pro zašifrování dalšího znaku zprávy, má významný vliv na bezpečnost. Je jasné, že změna hesla před každou zprávou je z hlediska bezpečnosti výhodnější než používat jeden klíč na šifrování všech zpráv. Kompromitace (prozrazení) hesla v prvním případě vede k rozluštění jen jedné zprávy, ve druhém případě ke kompromitaci celé korespondence. Jak však zajistit, aby mohl být klíč pro výběr abecedy pokaždé jiný? Cardano navrhuje použití autoklíče. Bohužel tuto novou nádhernou myšlenku formuluje nedokonale. Jím popsaný způsob dovoluje určitou nejednoznačnost šifrování, navrhuje opětovné použití klíče vždy na začátku otevřeného slova a nestanoví předání začátečního hesla autoklíče – tj. příjemce i luštitel jsou ve stejném postavení. Proto se jím uvedený systém nepoužíval. Kdyby jej byl dotáhl k dokonalosti, získal by mezi kryptology nesmrtelnou slávu, po které tolik toužil.
Věhlas mu však přinesla jiná zde publikovaná metoda, která se zabývá utajením textu, tedy steganografická metoda. Metoda nese na jeho počest jeho jméno. Metoda byla velmi jednoduchá a i proto se stala velmi oblíbenou. V obdélníkové nebo čtvercové mřížce se vystřihla určitá pole, vzniklá šablona se položila na papír a do děr se zapsalo tajné sdělení.

Šablona se zvedla a doplnil se zbytek písmen tak, aby text vypadal jako obyčejná nezávadná zpráva. Šlo tedy o jednoduché skrytí otevřeného textu do těla jiné zprávy, která vypadala jako zcela nezávadná. Cardano navrhoval, aby zpráva byla takto opsána za sebou dokonce 3x, aby se odstranily jakékoli případné problémy při dešifrování. Dešifrování bylo velmi prosté, příjemce přiložil mřížku a text v okénkách jednoduše přečetl.

Cardano proslul také svými důkazy o nemožnosti rozluštit jednoduchou substituci metodou, která byla později popsána jako útok hrubou silou (*Bruttal Force Attack*). Tato metoda je založena na vyzkoušení všech možných klíčů na šifrovaný text. Ukázal, že všech možností jak vytvořit klíč z abecedy čítající N znaků, je N! (N! se čte N faktoriál a je to symbol pro součin všech čísel od 1 do N). Pokud abeceda obsahuje 26 znaků, pak je klíčový prostor tak obrovské číslo, že šifru nelze v průběhu luštitelova života tímto způsobem prolomit. Vzhledem k tomu, že k vyluštění monoalfabetické šifry stačí kryptologovi zpravidla jen několik minut, je toto současně poučným příkladem, že kvalita šifry nezávisí jen na počtu všech možných klíčů. Nicméně i dnes se stává, že firmy zabývající se implementací některého šifrového algoritmu (zvláště méně známého) argumentují obdobně a na počtu klíčů a zdánlivé složitosti dokazují zákazníkovi, že systém je zcela bezpečný a že jej nelze v reálném čase prolomit.