Kapitola 1

Základní pojmy

Už od starověku se lidé snaží předávat zprávy tak, aby je mohl číst pouze adresát a nikdo jiný. Je-li zpráva napsána ručně a doručována otrokem (jak tomu bylo ve strém Řecku nebo Římě) nebo poštou dnes, tak vždy existuje nebezpečí, že se dostane do ruky někomu, komu není určena. Otrok může být zajat, pošťák se může zmýlit a doručit zprávu na nesprávnou adresu. Je-li zpráva napsána srozumitelně, přirozeným jazykem bez jakékoliv snahy skrýt její obsah, tak jí může porozumět každý, komu se dostane do ruky, pokud zná jazyk, kterým je napsána.

V novější době můžeme zprávy předávat telegrafem, radiovými vlnami, telefonem, faxem nebo e-mailem, ale nebezpečí, že budou odposlechnuty, je stále přítomná. Ve skutečnosti se od té doby nesmírně zvýšila. Tak například radiové vysílání může slyšet každý, kdo je v dosahu vysílače a má přijímač naladěný na správnou frekvenci. Zpráva e-mailem může být doručena na spoustu nezamýšlených adres v důsledku překlepu nebo viru číhajícího v počítači.

Jakkoliv pesimisticky to může vypadat, je dobrým pravidlem předpokládat, že *každá* zpráva, která má být důvěrná, se může dostat do rukou někomu, komu není určena. Je proto projevem potřebné opatrnosti učinit kroky, které zajistí, že nezamýšlený příjemce bude mít přinejmenším velké problémy jí porozumět, nebo ještě lépe, ji vůbec nebude schopen přečíst. Rozsah škody, kterou může nezamýšlené odhalení zprávy způsobit, do velké míry závisí na čase, který uplynul mezi odposlechnutím zprávy a jejím rozluštěním. V některých případech stačí, aby mezi odposlechnutím a rozluštěním zprávy uplynul jeden den nebo dokonce jenom pár hodin, aby k žádné škodě nedošlo. Například rozhodnutí akcionáře prodat nebo koupit okamžitě velký balík akcií, nebo rozkaz armádního velitele zaútočit za rozbřesku ná-

sledujícího dne. V jiných případech má informace dlouhodobou hodnotu a musí být proto utajena co nejdéle. Například zprávy týkající se plánování rozsáhlých vojenských operací.

Úsilí, které musí vynaložit soupeř, oponent nebo nepřítel k tomu, aby rozluštil zachycenou zprávu, má proto velký význam. Jesliže neautorizovaný příjemnce zprávy nedokáže zprávu rozluštit za použití nejlepších známých metod a nejvýkonnějších dostupných počítačů za dobu kratší, než po kterou je utajení obsahu zprávy důležité, tak si odesílatel může být relativně jistý. Nemůže si ale být *zcela* jistý, protože rozluštění nějakých dříve odeslaných zpráv může protivníkovi pomoci urychlit luštění následujících zpráv. Je také možné, že protivník objevil nějakou metodu, kterou odesílatel nezná, a je proto schopen luštit zprávy rychleji, než si odesílatel dokáže představit. To se například přihodilo německé armádě se šifrovacím zařízením Enigma v průběhu druhé světové války.

Ceasarova šifra

Říká se, že staří Řekové vymysleli zvláštní způsob, jak utajit zprávy před protivníkem. Zprávu napsali na oholenou hlavu otroka a pak počkali, než mu hlava znovu zaroste. Pak jej vyslali k adresátovi. Ten otrokovi hlavu zase oholil a zprávu si přečetl. To byla očividně velmi nespolehlivá a pomalá metoda. Každý, kdo ji znal a zadržel příslušného otroka, mohl zprávu snadno přečíst. Stačilo otrokovi hlavu oholit. Navíc odeslání zprávy trvalo celé týdny a další týdny bylo třeba čekat na odpověď.

Místo v historii kryptografie si zajistil až Julius Ceasar. Ten napsal zprávu a každé písmeno zprávy nahradil písmenem, které je v abecedě o tři místa dále. Pokud by používal mezinárodní latinskou abecedu, nahradil by každé písmeno `A` písmenem `D`, písmeno `B` písmenem `E`, a tak dále, písmeno `W` písmenem `Z`, potom písmeno `X` písmenem `A`, písmeno `Y` písmenem `B` a písmeno `Z` písmenem `C`. Každé písmeno mezinárodní latinské abecedy tak nahradil písmenem, které je v následující tabulce pod ním.

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

Kdyby Julius Ceasar používal naši latinskou abecedu (kterou pochopitelně neznal) a chtěl někomu utajeně sdělit, že

```
KOSTKY JSOU VRZENY,
```

poslal by

```
NRVWNB MVRX YUCHQB.
```

Ceasarova metoda není příliš důmyslná. Zejména proto, že na první pohled odhaluje, že zpráva se skládá ze tří slov, první a poslední jsou tvořené šesti písmeny zatímco druhé má čtyři písmena. Slabosti takového naivního systému není jednoduché odstranit, i když rozšíření abecedy z 26 symbolů na 29 nebo více tak, aby zahrnovala také interpunkční znaménka a mezeru, by učinilo rozpoznání délky jednotlivých slov *nepatrně* obtížnějším. Přesto je Ceasarova šifra příkladem *šifrovacího systému* a je speciálním případem *jednoduché záměny*, šifry, kterou se budeme za chvíli zabývat.

Několik základních definic

Opakovaně budeme používat slova jako *bigram*, *kryptografie*, *zašifrovat*, a proto je nyní definujeme.

Monogram je jedno písmeno v jakékoliv abecedě, kterou budeme používat. *Bigram* je jakákoliv dvojice *sousedních* písmen v nějakém textu. Tak například `DO` je bigram v českém textu, `AT` je bigram v anglickém textu. *Trigram* je trojice po sobě následujících písmen. *Polygram* je tvořený nespecifikovaným počtem po sobě jdoucích písmen v textu. Polygram nemusí být slovem v nějakém jazyce, ale pokud se pokoušíme rozšifrovat nějakou zprávu, o které můžeme rozumně předpokládat, že je v angličtině, pak je nalezení *heptagramu* `MEETING` mnohem slibnější, než nalezení heptagramu `QYRDBCFK`.

Symbolem rozumíme jakékoliv písmeno, číslici, interpunkční znaménko atd., které se mohou v textu vyskytnout. *Řetězec* je jakákoliv posloupnost po sobě jdoucích symbolů. *Délka* řetězce je počet symbolů, které řetězec obsahuje. Tak například `A3£%$` je řetězec délky 5.

Šifrovací systém nebo také *kryptografický systém* je jakýkoliv systém, který lze použít ke změně textu nějaké zprávy s cílem učinit ji nesrozumitelnou komukoliv jinému s výjimkou adresáta, kterému je určena.

Pokud nějaký šifrovací systém použijeme na nějakou zprávu, tak říkáme, že zprávu *šifrujeme* nebo že jsme ji *zašifrovali*.

Původní text zprávy, ještě před tím, než byl zašifrován, se nazývá *otevřený text*; poté, co byl zašifrován, se nazývá *šifrový text* nebo *šifrová zpráva*.

Opačný proces k šifrování, tj. rekonstrukce původního otevřeného textu zprávy z jeho šifrové verze, se nazývá *dešifrování* nebo *luštění*. Tato dvě slova neznamenají zcela totéž. Zamýšlený příjemce zprávy tuto zprávu dešifruje, zatímco nezamýšlený příjemce, který se snaží pochopit její obsah, ji luští, případně řeší.

Kryptografie je věda o tom, jak navrhovat a používat šifrovací systémy včetně zkoumání jejich silných stránek a slabin a jejich odolnosti vůči různým metodám útoků. *Kryptografové* jsou ti, kteří se návrhem, používáním

a zkoumáním šifrovacích systémů zabývají.

Kryptoanalýza je studium metod luštění šifrovacích systémů. Ten, kdo se zabývá kryptoanalýzou, je *kryptoanalytik*, populární anglický výraz je *codebreaker*.

Kryptografie a kryptoanalýza jsou dvě součásti jedné vědecké discipliny, kterou nazýváme *kryptologie*. Společnost *kryptologů* tvoří jak kryptografové tak kryptoanalytici.

Kryptografové a kryptoanalytici jsou soupeři, každý z nich se snaží přelstít toho druhého. Představuje si sám sebe v postavení toho druhého a klade si otázky jako "Kdybych byl na jeho místě, co bych asi udělal, abych mě porazil?". Obě strany, které se pravděpodobně nikdy nesetkají, jsou zapojené do fascinujícího intelektuálního souboje a v sázce může být opravdu hodně.

Tři fáze luštění: identifikace, prolomení a nastavení

Když kryptoanalytik poprvé vidí šifrovou zprávu, jeho první otázkou je odhalit, jaký šifrovací systém byl použit. Může to být nějaký už známý šifrovací systém nebo zcela nový. Tomu se říká problém *identifikace*. K tomu vezme v úvahu veškeré dostupné současné informace. Například jaký typ šifrovacího systému odesílatel, je-li znám, dosud používal, nebo jaké nové šifrovací systémy se v nedávné době objevily. Potom začne zkoumat úvod zprávy. Ten může obsahovat informace, které mají zamýšlenému příjemci zprávy pomoci v jejím dešifrování, ale mohou být také užitečné kryptoanalytikovi. Potom analyzuje celou zprávu. Je-li zpráva příliš krátká, tak může být nemožné pokročit dále a kryptoanalytik musí čekat na další zprávy. Je-li zachycená zpráva dostatečně dlouhá nebo pokud má kryptoanalytik k dispozici několik zpráv, tak může použít řadu matematických testů, které mu s jistotou odhalí, jestli byla použita například kódová kniha nebo nějaký jednoduchý šifrovací systém případně něco dokonalejšího.

Pokud se kryptoanalytikovi podařilo identifikovat použitý šifrovací systém, může odhadnout, kolik šifrových zpráv bude potřebovat, aby měl přijatelnou naději, že jej *prolomí*, tj. že přijde na to, jakým způsobem systém zprávy šifruje. Jde-li o jednoduchý systém, u kterého nedochází k podstatným změnám mezi jednotlivými zprávami, jako je například kódová kniha, jednoduchá záměna nebo transpozice, tak může být schopen zprávy rozluštit bez velkých problémů. Daleko pravděpodobnější ale je, že některé části šifrovacího systému se mění zprávu od zprávy a kryptoanalytik potřebuje napřed určit, jaké části systému se nemění. Tak například přístroj pro německý šifrovací systém Enigma používaný ve druhé světové válce obsahoval několik kruhů. Uvnitř těchto kruhů bylo propojení pomocí drátů. Propojení uvnitř kruhů se neměnilo, ale pořadí kruhů se měnilo každý den. Propojení

uvnitř jednotlivých kruhů tak tvořilo pevnou (neměnnou) část systému, zatímco jejich pořadí bylo proměnlivé. Prolomení je nejobtížnější fází luštění šifrových zpráv. Může trvat týdny a měsíce a vyžadovat použití pokročilých matematických metod, využití chyb obsluhy systému nebo informací získaných špionáží.

Pokud se už podařilo určit všechny pevné součásti šifrovacího systému, je třeba ještě určit, jak se mění proměnlivé části. Například počáteční nastavení kroužků v přístroji Enigma, které se měnilo s každou zprávou. Tomu se říká problém *nastavení*. Pokud se podaří vyřešit i tento problém, je možné zprávy rozluštit.

Prolomení se tak týká celého šifrovacího systému, zatímco *nastavení* se vztahuje k luštění jednotlivých zpráv.

Kódy a šifry

Budeme rozlišovat mezi *kódy* a *šiframi*. V *kódu* jsou běžné fráze tvořené jedním nebo více písmeny, čísly nebo slovy, typicky nahrazované čtveřicemi nebo pěticemi písmen nebo čísel. Říká se jim *kódové skupiny* a jsou přebírány z *kódové knihy*. V případě nejčastěji používaných výrazů nebo písmen může kódová kniha obsahovat několik *kódových skupin* s cílem umožnit odesílateli výběr. Záměrem je učinit identifikaci nejužívanějších frází obtížnější. Tak například ve čtyřmístném kódu může být pro slovo "`pondělí`" několik možností: `2475` nebo `7032` nebo `6845`.

Kódy jsou speciálním případem *šifrovacích systémů*, ale ne všechny *šifrovací systémy* jsou *kódy*. My budeme používat termín *šifra* pro metodu šifrování, která není založena na *kódové knize*, ale vytváří šifrovou zprávu z otevřeného textu pomocí nějakého pravidla – *algoritmu*. Rozdíl mezi *kódy* a *šiframi* je v některých případech nezřetelný. Tak například Ceasarovu šifru můžeme považovat za kódovou knihu s jednou stránkou, na které je vedle každého písmena napsáno písmeno, které je za ním v abecedě na třetím místě. V naprosté většině případů je ale rozdíl jasný. Tak například Enigma je *šifrovací* přístroj, v žádném případě to není *kód*.

Až do nástupu počítačů v kryptografii dominovaly dvě základní metody a mnohé šifrovací systémy byly založené na jedné nebo obou z nich. První idea spočívá v zamíchání písmen abecedy stejně jako se míchá balíček karet s cílem vytvořit náhodné pořadí, permutaci, těchto písmen. Druhá idea spočívá v nahrazení písmen v otevřeném textu zprávy čísly podle nějakého pravidla, např. `A=0, B=1, C=2, ... , Z=25`. K nim potom pořadě přičítáme nějaká jiná čísla, kterými rovněž mohou být písmena nahrazená čísly, říká se jim *klíč*. Pokud je součet větší než 25, odečteme od něho 26, abychom dostali opět nějaké přirozené číslo mezi 0 a 25. Tomu se říká *modulární arit-*

metika s modulem 26. Výsledná čísla potom zpětně nahradíme písmeny. Pokud jsou přičítaná čísla klíče vytvořena nějakým dostatečně nepředvídatelným způsobem, pak je velmi obtížné, pokud ne zcela nemožné, šifrovou zprávu bez znalosti klíče rozluštit.

Jakkoliv je Ceasarova šifra jednoduchá, může být považována za ilustraci obou myšlenek. V prvním případě naše "míchání" abecedy spočívá v přesunutí posledních tří písmen `X,Y,Z` abecedy na její počátek. Ve druhém případě je klíčem prostě stále opakované číslo 3. Je to ten nejjednodušší možný klíč.

Překlad zprávy do jiného jazyka lze považovat za šifrování pomocí kódové knihy – slovníku. To ale je význam slova *kód* rozšířený do krajnosti. Použití málo známého jazyka k předávání zpráv krátkodobého významu může být ale v některých případech vhodné. Tak například během druhé světové války používala americká armáda v Pacifiku k předávání telefonických zpráv menšího významu vojáky z indiánského kmene Navajů. Jejich využití bylo založené na rozumném předpokladu, že i kdyby nepřátelská japonská armáda telefonické rozhovory odposlechla, tak je velmi nepravděpodobné, že by měla k dispozici někoho, kdo by jim byl schopen rozumět.

Jiným způsobem šifrování je používání nějakého osobního těsnopisu. Tato metoda byla některými lidmi využívána už od středověku k psaní osobních denníků. Je-li k dispozici dostatek záznamů, není obtížné takový kód rozluštit. Pravidelné výskyty některých symbolů, jako třeba názvy dnů v týdnu, mohou poskytnout dostatečný klíč k rozluštění některých polygramů. Daleko hlubším příkladem je rozluštění starodávných Mykénských textů založených na symbolech nahrazujících řeckou abecedu Michaelem Ventrisem v roce 1952. Mnohem známější je rozluštění hieroglyfů francouzským badatelem J.F. Champollionem, ten měl ale narozdíl od Ventrise k dispozici "paralelní text" ve známém jazyce. Na rozluštění čekají ještě další starodávné texty.

Nástup počítačů a možnost vytváření složitých elektrických obvodů na silikonových čipech zcela proměnily jak kryptografii tak kryptoanalýzu. V důsledku toho jsou některé z nedávných šifrovacích systémů založené na pokročilých matematických metodách, které vyžadují výkonné výpočetní a elektronické prostředky, a byly tak prakticky nepoužitelné v předpočítačové době.

Posuzování spolehlivosti šifrovacích systémů

Pokud někdo navrhuje nový šifrovací systém, tak je důležité posoudit jeho sílu – odolnost vůči všem známým útokům za předpokladu, že kryptoanalytik zná typ tohoto šifrovacího systému, ale nezná všechny jeho detaily.

Odolnost šifrovacího systému může být posuzována ve třech různých situacích:

1. kryptoanalytik má k dispozici pouze šifrové texty,
2. kryptoanalytik má k dispozici jak šifrové texty tak také jim odpovídající otevřené texty,
3. kryptoanalytik má k dispozici šifrové texty k otevřeným textům, které si sám zvolil.

První situace je ta "obvyklá". Šifrovací systém, který lze v této sitaci rozluštit za rozumnou dobu, by neměl být používán. Druhá situace může nastat, pokud je identická zpráva zašifrována jak pomocí nového systému, tak také pomocí "starého" systému, který už kryptoanalytik umí luštit. Takové situace, které jsou významným porušením pravidel bezpečnosti předávání zpráv, nezřídka nastávají. Třetí situace může nastat pokud kryptograf chce posoudit sílu navrženého šifrovacího systému. Vyzve kolegy, aby jeho systém rozluštili, a dovolí jim nadiktovat si zprávu, která má být zašifrována. Toto je standardní metoda posuzování nových šifrovacích systémů. Pro kryptoanalytika je velmi zajímavý problém jak formulovat texty tak, aby mu po zašifrování poskytly co nejvíce informací o detailech systému. Podoba těchto zpráv závisí na tom, jak šifrování probíhá. Druhá a třetí situace může také nastat, pokud má kryptoanalytik k dispozici špiona v protivné kryptografické organizaci. To se například stalo ve třicátých létech minulého století, kdy polští kryptoanalytici získali otevřené texty a jejich šifrové verze vytvořené německou Enigmou. Šifrovací systém, který nelze rozluštit ani za třetí situace, je opravdu silný. Po takových kryptografové touží a kryptoanalytici se jich obávají.

Kódy, které odhalují a opravují chyby

Zcela jiná skupina kódů je navržena s cílem zajistit *přesnost* přenášené informace, nikoliv skrýt její *obsah*. O takových kódech říkáme, že *odhalují chyby*, případně že *opravují chyby*. Tyto kódy jsou předmětem intenzivního matematického výzkumu. Jsou používány od nejranějších počátků počítačů, aby je ochránily před chybami v operační paměti nebo v datech uložených na magnetické pásce. První kódy, jako jsou třeba Hammingovy kódy, dokážou správně opravit jednu chybu v posloupnosti sedmi bitů. Novější verze používané například při přenášení informací z Marsu získaných sondou Mariner dokážou správně opravit až sedm chyb v každém vysílaném 32-bitovém slově. Chrání tak přenášenou informaci před značným poškozením, ke kterému může dojít během dlouhé cesty z Marsu na Zemi.

Příkladem kódu jiného druhu, který dokáže jednu chybu odhalit ale ne opravit, je mezinárodní číselný systém knih ISBN (International Standard Book Number). Každé číslo ISBN $a_1a_2a_3\cdots a_{10}$ je tvořené buď posloupností deseti cifer nebo posloupností devíti cifer následovaných písmenem X (které je interpretováno jako číslo 10), a dává možnost překontrolovat, zdali číslo neobsahuje jednu chybu. Kontrolu provedeme tak, spočítáme *kontrolní součet*

$$1a_1 + 2a_2 + \cdots + 10a_{10} = \sum_{i=1}^{10} ia_i.$$

Cifry jsou většinou rozdělené do čtyř skupin oddělených pro pohodlí pomlčkou nebo mezerou. První skupina označuje jazykovou oblast, druhá nakladatelství, třetí je sériové číslo knihy v nakladatelství a poslední skupina je *kontrolní cifra*.

Kontrolní součet musí být dělitelný číslem 11. Pokud není, tak je v čísle ISBN chyba. Tak například tento text vychází z knihy, která má ve vázané verzi jako ISBN číslo 0 521 81054 X. Kontrolní suma se pak rovná

$$1\cdot 0+2\cdot 5+3\cdot 2+4\cdot 1+5\cdot 8+6\cdot 1+7\cdot 0+8\cdot 5+9\cdot 4+10\cdot 10 = 242 = 22\cdot 11.$$

Naproti tomu 0 987 65432 1 má kontrolní součet

$$1\cdot 0+2\cdot 9+3\cdot 8+4\cdot 7+5\cdot 6+6\cdot 5+7\cdot 4+8\cdot 3+9\cdot 2+10\cdot 1 = 19\cdot 11+1,$$

a musí proto obsahovat aspoň jednu chybu.

Kód ISBN dokáže *odhalit* jednu chybu, neumí ji ale *opravit*. Pokud jsou v čísle ISBN aspoň dvě chyby, může kontrolní součet dokonce naznačit, že jde o správné číslo, i když tomu tak není.

Oblast kódů odhalujících a opravujících chyby je založena na dosti pokročilé matematice a v této úvodní přednášce se jí nebudeme zabývat.

Jiné metody skrývání zpráv

Existují jiné metody skrývání smyslu nebo obsahu zpráv, které nejsou založené na šifrách nebo kódech. První dvě nejsou z našeho pohledu relevantní, zaslouží si ale zmínku. Jsou to

1. použití "neviditelných" inkoustů,
2. využití *mikroteček*, drobounkých fotografií zprávy na mikrofilmu přilepených na zprávu na předem domluveném místě,
3. "vložení" zprávy dovnitř jinak nevinně vyhlížejícího textu, *slova* nebo *písmena* zprávy jsou rozptýlena podle nějakého pravidla v textu, který sám o sobě není utajený.

První dvě metody jsou s různým úspěchem využívány mnohými špiony. Třetí metoda může být rovněž využívána vězni nebo válečnými zajatci v dopisech domů k předávání informací o umístění táborů a podmínkách v nich. Touto metodou se zabývá obor nazývaný *steganografie*.

Příklady v této a následujících přednáškách budou založené téměř výhradně na mezinárodní abecedě tvořené 26 písmeny, žádná diakritika nebude používána. V některých případech budeme používat rozšířenou abecedu, která obsahuje také mezeru a interpunkční znaménka jako je tečka, čárka, dvojtečka, atd.

Teoreticky není obtížné modifikovat příklady tak, aby obsahovaly také více písmen používaných v jiných jazycích. Pokud je ale k šifrování zpráv používáno nějaké šifrovací zařízení, může požadavek zvětšit počet písmen abecedy vést k nutnosti změnit konstrukci zařízení.

Modulární aritmetika

V kryptologii je často třeba sčítat posloupnost (proud) čísel s jinou posloupností (proudem) čísel nebo odečítat jednu číselnou posloupnost od jiné. Zpravidla nejde o obvyklé sčítání nebo odčítání celých čísel, ale o *modulární aritmetiku*. V modulární aritmetice sčítáme, odčítáme a násobíme čísla vzhledem k nějakému předem zvolenému číslu, kterému říkáme *modul*. Typické příklady modulů jsou 26, 10 nebo 2. Ať používáme jakýkoliv modul, je každé číslo ve výpočtu nahrazeno nezáporným zbytkem při jeho dělení modulem. V modulární aritmetice s modulem 26 tak počítáme pouze s čísly 0,1,...,25. Platí potom

$$17 + 19 = 10 \bmod 26,$$

protože $17 + 19 = 36$ a dělíme-li 36 modulem 26, dostaneme zbytek 10. Podobně

$$17 - 19 = 24 \bmod 26 \quad \text{a} \quad 7 \cdot 8 = 4 \bmod 26.$$

Dvě posloupnosti čísel stejné délky sčítáme (odčítáme) tak, že sečteme (odečteme) dvojice čísel na stejným místech posloupnosti.

Příklad 1.1 *Sečtěte a odečtěte posloupnosti* 15 11 23 06 11 *a* 17 04 14 19 23 *modulo* 26.

Řešení. Pro součet platí

	15	11	23	06	11
+	17	04	14	19	23
	32	15	37	25	34
mod 26:	6	15	11	25	9

a pro rozdíl podobně

$$\begin{array}{rccccc} & 15 & 11 & 23 & 06 & 11 \\ - & 17 & 04 & 14 & 19 & 23 \\ \hline & -2 & 07 & 09 & -13 & -12 \\ \mathrm{mod}\,26: & 24 & 07 & 09 & 13 & 14 \end{array} .$$

□

Při počítání $\mathrm{mod}\,10$ používáme pouze čísla $0, 1, 2, \ldots, 9$ a při počítání $\mathrm{mod}\,2$ počítáme pouze s čísly $0, 1$. Modulární aritmetika $\mathrm{mod}\,2$, neboli *binární aritmetika*, má tu vlastnost, že sčítání $\mathrm{mod}\,2$ se rovná odčítání $\mathrm{mod}\,2$:

$$\begin{array}{rcccc} & 0 & 0 & 1 & 1 \\ + & 0 & 1 & 0 & 1 \\ \hline & 0 & 1 & 1 & 2 \\ \mathrm{mod}\,2: & 0 & 1 & 1 & 0 \end{array}$$

a

$$\begin{array}{rcccc} & 0 & 0 & 1 & 1 \\ - & 0 & 1 & 0 & 1 \\ \hline & 0 & -1 & 1 & 0 \\ \mathrm{mod}\,2: & 0 & 1 & 1 & 0 \end{array} .$$

Modulární sčítání a odčítání písmen

Potřebujeme-li sčítat nebo odčítat posloupnosti písmen, používáme modulární aritmetiku s modulem 26. K tomu nahradíme každé písmeno dvouciferným číslem počínaje `A=00` a konče `Z=25` podle následující tabulky:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Poté sečteme (odečteme) obě posloupnosti čísel $\mathrm{mod}\,26$ a nakonec výsledná čísla zpětně nahradíme písmeny podle stejné tabulky.

Příklad 1.2 *Sečtěte a odečtěte posloupnosti* `POSTEL` *a* `KOLENO`.

Řešení. Pro součet platí

POSTEL	=	15	14	18	19	04	11		
+KOLENO	=	10	14	11	04	13	14		
		25	02	03	23	17	25	=	ZCDXRZ

a rozdíl se rovná

POSTEL	=	15	14	18	19	04	11		
−KOLENO	=	10	14	11	04	13	14		
		05	00	07	15	17	23	=	FAHPRX.

□