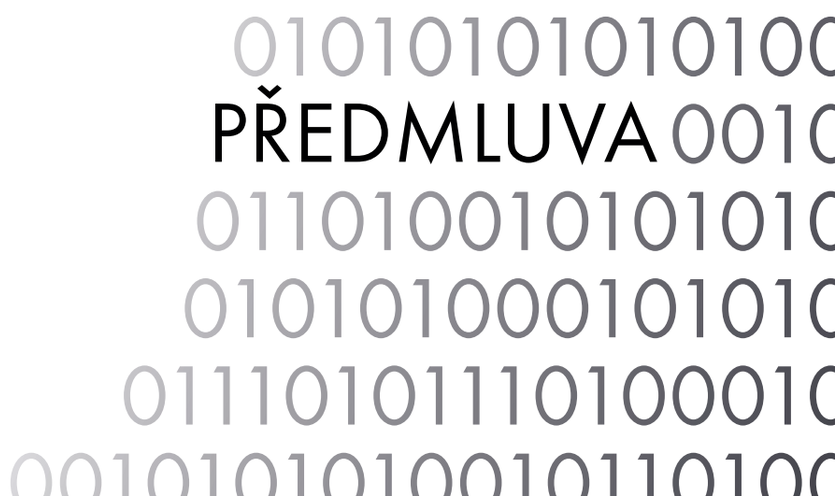


10101010101111100PŘEDMLUVA
1001101001010101000010
00010110110
0011010
00111010
1010
1

Kryptografie se zabývá konstrukcí matematických metod zajišťování bezpečnosti zpráv, a tak se významným způsobem podílí na bezpečném fungování komunikačních a informačních systémů. Praxe ukazuje se, že k vývoji a k zavádění kryptografických ochran jsou zapotřebí vysoce kvalifikovaní specialisté. K přípravě i k dalšímu samostatnému vzdělávání takovýchto specialistů je určena kniha, kterou právě držíte v rukou.

Kniha je koncipována jako přehledová. Čtenář se v ní seznámí s nutným objemem teorie, která je potřebná k porozumění dané problematiky. Dále se seznámí s obsahem standardů pro jednotlivé aplikace kryptografie a s popisem prakticky nasazených kryptografických systémů. Ke zvládnutí knihy čtenáři postačí znalost středoškolské matematiky a zájem o kryptografii. Při psaní knihy byl kladen důraz na srozumitelnost při zachování odbornosti.

Protože obdobná monografie v českém jazyce doposud neexistuje, autor se v knize zároveň pokusil o návrh jednotné a systematické terminologie. K orientaci v anglicky psané odborné literatuře a k posouzení správnosti navrženého názvosloví jsou základní pojmy v závorce opatřeny anglickým ekvivalentem. Při výběru českého názvu byl upřednostněn obsah pojmu před doslovným překladem anglického označení (např. „product cipher“ a „kaskádová šifra“). V případě převzetí anglického slova byla preferována vyslovovaná podoba před psanou (např. „hash“ a „heš“).

Autor knihy pracoval po řadu let jako specialista pro vojenské kryptografické a komunikační systémy. V současné době vyučuje na VUT v Brně, přičemž se specializuje na problematiku kryptografie a na problematiku bezpečnosti informací obecně. I přes autorovu erudici se v knize může vyskytnout chyba, či opomenutí. Autor bude čtenářům vděčen za upozornění na případné nedostatky či za náměty ke zkvalitnění knihy. Ke komunikaci s autorem lze využít e-mailovou adresu **aplikovana.kryptografie@email.cz**.

V této kapitole se seznámíme se základními pojmy kryptografie, s kryptografickými systémy, s teorií utajení a autentizace a také se základními matematickými pojmy a operacemi, které se v kryptografii používají.

1.1 ZÁKLADNÍ POJMY

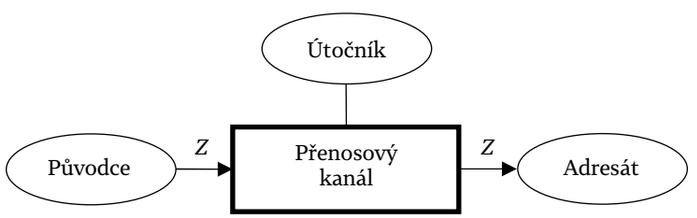
S aplikovanou kryptografií se setkáváme zejména v komunikačních a v informačních systémech. Komunikační systémy (např. telefonní sítě) zajišťují přenos informací mezi osobami nebo zařízeními, která jsou umístěna v různých lokalitách (přenos zpráv prostorem). Účelem informačních systémů je zajistit přenos informací jak prostorem, tak i časem (formou uchovávání informací) a zajistit zpracování informací (např. jejich vyhledáváním nebo propojováním). Fungování a rozvoj naší civilizace jsou na komunikačních a informačních systémech ve velké míře závislé, a proto je zapotřebí zajistit jejich bezchybné a spolehlivé fungování. Na dosažení tohoto cíle se podílí i aplikovaná kryptografie.

Informace se v čase a prostoru přenáší pomocí nosičů informací. Nosičem informace budeme v dalším rozumět materiál nebo proces, který může nabývat více stavů (např. orientace magnetického pole materiálu nebo velikost elektrického proudu). Zprávu potom můžeme definovat jako posloupnost stavů nosiče informace, ve které je určitým kódem zakódována informace. Posloupnost stavů nosiče informace může být posloupností v čase nebo v prostoru. Časová posloupnost se nazývá signál (např. časový průběh změn proudu) a prostorová posloupnost stavů nosiče se nazývá záznam (např. sled různě zmagnetovaných oblastí na pevném disku počítače).

Počet stavů nosiče informace může být buď konečný nebo nekonečný. V současné době je zcela dominantní případ s konečným počtem stavů, kdy

jednotlivé stavy nosiče informace můžeme reprezentovat znakem z nějaké konečné abecedy nebo celým číslem. Protože v kryptografii není fyzikální forma zprávy podstatná, budeme dále zprávu chápat jako posloupnost celých čísel, v níž je všeobecně známým kódem zakódována určitá informace. Obecně lze kryptografickými technikami chránit také zprávy, které jsou reprezentovány posloupnostmi o nekonečném počtu stavů (např. analogové signály), avšak tyto techniky mají v současné době pouze okrajový význam a v éře digitalizace se ani nejeví perspektivními. Příkladem těchto technik jsou kryptografické skramblery, které se používaly k šifrování telefonních hovorů.

K zajištění správného chodu komunikačních a informačních systémů je zapotřebí chránit nejen prvky, z nichž tyto systémy sestávají (např. ústředny, servery apod.), ale je zapotřebí také chránit informace, které tyto systémy přenášejí, uchovávají a zpracovávají. Protože informace fyzicky existují jen v podobě zpráv, pak jsme fakticky postaveni před problém zajistit ochranu zpráv v komunikačních a v informačních systémech. Problém ochrany zpráv lze ilustrovat na obr. 1.1, kde je uvedeno obecné schéma přenosu zpráv. Zdroj zpráv budeme označovat jako původce a zamýšleného příjemce zpráv budeme označovat jako adresáta. Oba zmíněné subjekty budeme souhrnně označovat jako oprávněné osoby, i když se také může jednat o zařízení nebo o procesy běžící v těchto zařízeních. Zprávy *Z* jsou od původce přenášeny k adresátovi prostřednictvím přenosového kanálu. Přenosovým kanálem budeme rozumět technický systém, který umožňuje buď přenos zpráv prostorem (tzv. komunikační kanál), nebo přenos zpráv časem (tzv. paměťový kanál). Příkladem komunikačního kanálu je telefonní kanál a příkladem paměťového kanálu je nějaké paměťové úložiště (např. pevný disk počítače).



Obr. 1.1: Obecné schéma přenosu zpráv.

K přenosovému kanálu má obecně přístup další subjekt, který budeme nazývat útočník. Útočník je neoprávněná osoba, která může přenosy zpráv buď odposlouchávat (tzv. pasivní útočník), nebo je může modifikovat (tzv. aktivní útočník). Odposlechem zpráv útočník může získat důvěrné informace (např. výrobní tajemství), a ty pak využít ve svůj prospěch. Modifikací komunikace nebo předávaných zpráv (např. platební příkaz bance) může útočník dosáhnout takového chování adresáta, které povede ke ztrátě aktiv oprávněných osob nebo povede ku prospěchu útočníka.

Pro většinu komunikačních a informačních systémů je hrozba odposlechu nebo modifikace zpráv neakceptovatelná. Z tohoto důvodu se pomocí různých typů ochran zajišťuje důvěrnost a autentičnost přenášených zpráv. Důvěrnost zprávy budeme chápat jako stav, kdy zpráva je známa pouze oprávněným osobám. Autentičnost zprávy budeme definovat jako stav, kdy informace o původu zprávy jsou pravdivé. Zpravidla se jedná o informace, kdo je původcem zprávy, popřípadě kdy a kde zpráva vznikla.

K zajištění důvěrnosti a autentičnosti zpráv se v praxi používají různé typy ochran. Při ochraně zpráv se primárně snažíme, aby útočník o existenci zpráv vůbec nevěděl. K tomu se používají techniky skrytí zpráv. Pokud fakt samotné existence zpráv nelze skrýt, pak usilujeme o to, aby se útočník nemohl ke zprávám dostat. K tomu se používají techniky řízení přístupu. V řadě případů však techniky řízení přístupu nejsou použitelné (např. zprávy jsou přenášeny přes veřejně přístupný komunikační kanál). V takovýchto případech se používají techniky založené na transformaci zpráv. Nyní si výše uvedené typy ochran popíšeme podrobněji.

Ochrana skrytím zpráv spočívá v tom, že útočník neví, kde se zprávy nacházejí, popřípadě neví, že zprávy vůbec existují. Proto útočník nemůže tyto zprávy odposlouchávat, ani modifikovat. Příkladem uvedeného typu ochran jsou techniky skrývání informací do obrázků, komunikační systémy s přímým rozprostřením spektra, psaní zpráv neviditelnými inkousty atd. Problematikou skrývání zpráv se zabývá věda nazývaná steganografie.

Ochrana řízením přístupu („Access Control“) spočívá v tom, že přístup ke zprávám je umožněn jen oprávněným osobám. Útočník tak nemá možnost chráněné zprávy číst nebo modifikovat. Typickým příkladem uvedeného typu ochran je regulace přístupu osob do místností, kde jsou chráněné zprávy uloženy, dále regulace přístupu osob k síťovým službám, jejichž prostřednictvím lze chráněné zprávy číst, eliminace parazitních kanálů, personální opatření atd.

Posledním z výše uvedených typů ochran jsou ochrany založené na transformaci zpráv. Protože čísla mohou reprezentovat také slova, upravíme si výše uvedenou definici zprávy Z pro tuto chvíli do takové podoby, že zpráva bude posloupností čísel nebo slov, v níž jsou veřejně známým kódem zakódovány informace. K zajištění důvěrnosti je původní posloupnost Z čísel nebo slov transformována na jinou posloupnost C čísel nebo slov (tzv. kryptogram), ke které má obecně přístup kdokoliv, tj. i útočník. Principem ochrany je skutečnost, že ke zjištění zakódované informace je nutná zpětná transformace posloupnosti C na posloupnost Z. K provedení zpětné transformace je však zapotřebí nějaká utajovaná informace K (např. klíč nebo kód), kterou má obecně k dispozici pouze adresát. Jen tato osoba dokáže posloupnost C transformovat na původní posloupnost Z, a z ní důvěrné informace přečíst. V případě, že jde o zajištění autentičnosti zprávy, zpráva Z je svým původcem rozšířena o autentizační číselnou posloupnost P. Tato posloupnost závisí na původní zprávě a na nějaké utajované informaci K, kterou obecně zná pouze původce, a tudíž správnou autentizační posloupnost P dokáže vygenerovat pouze tato osoba. Adresát správnost autentizační posloupnosti kontroluje, čímž si ověřuje autentičnost doručených zpráv. Příkladem ochran založených na transformaci zpráv jsou kódové knihy, šifrování nebo digitální podpis.

Transformace zpráv mohou být buď překladové, nebo matematické. V případě překladové transformace je zpráva chápána jako posloupnost slov nebo vět nějakého obecně známého jazyka. Při překladové transformaci je zpráva přeložena do jazyka, který je znám pouze původci a adresátovi. Útočník potom není schopen transformované zprávě porozumět nebo ji cílevědomě modifikovat. Příkladem popsaného typu transformace jsou kódové knihy ([1], s. 16) nebo použití prakticky neznámého jazyka indiánského kmene Navahů pro vojenskou komunikaci v bojích USA proti Japonsku za 2. světové války ([2], s. 185 – 193). Významnou nevýhodou překladové transformace je skutečnost, že vyžaduje objemné překladové slovníky.

V případě matematické transformace je zpráva chápána jako posloupnost čísel a s těmito čísly jsou prováděny určité matematické transformace. K praktickému provedení těchto a případně inverzních transformací je nutná znalost nějakého tajného parametru, tzv. klíče. Uvedený parametr mívá délku pouze stovek až tisíců bitů, a tak na rozdíl od kódových knih neklade vysoké nároky na kapacitu paměťových úložišť. Navíc jej lze i snadno operativně měnit, tj. pro každou zprávu může být použita jiná transformace definovaná jiným klíčem. Útočník, který klíč nezná, není schopen transformované zprávě porozumět nebo ji cílevědomě modifikovat. Ochrany, které jsou založeny na matematických transformacích zpráv, budeme dále nazývat matematické ochrany. Právě matematické ochrany jsou tématem této knihy.

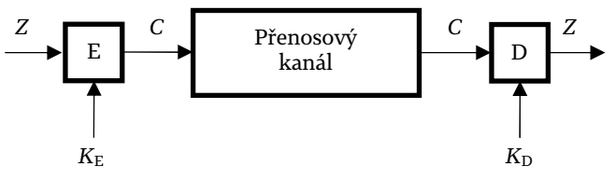
Věda, která se zabývá konstrukcí matematických ochran, se nazývá kryptografie a věda, která se zabývá překonáváním těchto ochran, se označuje jako kryptoanalýza. Kryptografii potom můžeme definovat jako vědu, která se zabývá konstrukcí matematických metod zajišťování důvěrnosti a autentičnosti zpráv. Kryptoanalýzu lze analogicky definovat jako vědu o překonávání matematických metod zajišťování důvěrnosti a autentičnosti zpráv. Kryptografie i kryptoanalýza společně tvoří vědu nazývanou kryptologie.

1.2 KRYPTOGRAFICKÉ SYSTÉMY

V úvodu této kapitoly si nejprve zavedeme pojmy algoritmus a kryptografický protokol. Algoritmem budeme rozumět výpočetní postup pro řešení určité úlohy (například výpočetní postup k transformaci zprávy do podoby kryptogramu) a kryptografickým protokolem (nebo zkráceně protokolem) budeme rozumět algoritmus, na jehož provádění se podílí více stran (např. původce i adresát). Kryptografickým systémem (zkráceně kryptosystém) potom budeme rozumět systém algoritmů určený k zajištění důvěrnosti a autentičnosti zpráv.

Na obr. 1.2 je vyobrazen kryptografický systém, který slouží k zajištění důvěrnosti přenášených zpráv. Tento typ kryptosystému se často nazývá šifra nebo jej také budeme označovat jako utajovací kryptosystém. Pro fungování utajovacího kryptosystému je zapotřebí dvou parametrů. Na straně původce je to číslo K_E, které se nazývá šifrovací klíč, a na straně adresáta se jedná o číslo K_D, které se nazývá dešifrovací klíč. Jádrem systému jsou dvě speciální matematické funkce (transformace), které se nazývají šifrování a dešifrování. Obě tyto funkce se prakticky vykonávají podle příslušných algoritmů. Funkce šifrování E je prostá funkce, která je určena šifrovacím klíčem K_E. Tato funkce každé zprávě Z přiřadí posloupnost celých čísel, která se nazývá kryptogram C. Formálně lze šifrování vyjádřit následovně:

$$C = E(Z, K_E).$$



Obr. 1.2: Kryptografický systém pro zajištění důvěrnosti přenášených zpráv.

Funkce šifrování je konstruována tak, aby útočník s předpokládanou úrovní možností nebyl schopen z daného kryptogramu bez znalosti dešifrovacího klíče odvodit zprávu dříve, než je stanovená doba rezistence kryptogramu. Takovýto požadavek budeme nazývat praktickou nemožností. Doba rezistence kryptogramu je individuální a závisí na potřebách dané aplikace. Například k ochraně důvěrnosti řídících příkazů zasílaných bezpilotnímu bombardéru postačí doba rezistence kryptogramu řádově hodiny. Po této době (zpravidla po vybombardování cíle) je každému jasné, jaké příkazy byly bombardéru v průběhu jeho letu předány. Na druhou stranu například zašifrovaný seznam špiónů musí mít dobu rezistence desítky let.

Na straně adresáta se v kryptografickém systému provede dešifrování D, což je inverzní funkce k šifrování. Dešifrování můžeme formálně vyjádřit následovně:

$$\mathrm{D}(C, K_D) = Z,$$

přičemž požadujeme, aby k praktickému zjištění hodnoty závisle proměnné (tj. Z) byla zapotřebí znalost tajného dešifrovacího klíče K_D.

Dvojice šifrovací a dešifrovací klíč nemohou být libovolné. Mezi oběma uvedenými parametry musí samozřejmě existovat určitá závislost, kterou můžeme formálně vyjádřit funkcí:

$$K_D = f(K_E).$$

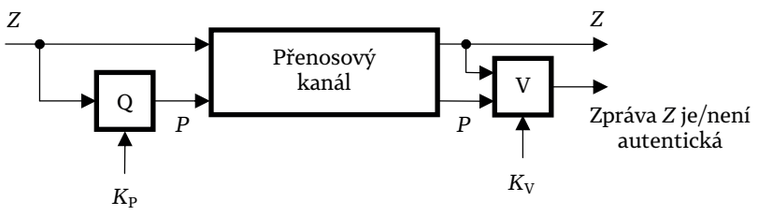
Pokud je prakticky možné hodnotu dešifrovacího klíče K_D zjistit z hodnoty šifrovacího klíče K_E, pak oba klíče musí být tajné (tzv. tajné klíče). V uvedeném případě mají oba klíče z hlediska jejich utajení stejné, tj. symetrické postavení, a proto se tyto kryptosystémy nazývají symetrické utajovací kryptosystémy nebo také utajovací kryptosystémy s tajným klíčem. Do této třídy kryptosystémů náleží například šifra AES, IDEA, DES, RC4 apod.

Pokud však je prakticky nemožné zjistit klíč K_D z hodnoty klíče K_E, pak šifrovací klíč může být veřejně známý (tzv. veřejný klíč) a utajovat je zapotřebí pouze dešifrovací klíč (tzv. soukromý klíč). V popsaném případě mají oba klíče z hlediska jejich utajení nestejné, tj. asymetrické postavení, a proto se tyto kryptosystémy nazývají asymetrické utajovací kryptosystémy nebo také utajovací kryptosystémy s veřejným klíčem. Příkladem této třídy kryptosystémů je šifra RSA nebo El Gamalova šifra.

V této souvislosti je zapotřebí upozornit na častou chybu, kdy utajovací kryptosystém s různými klíči (tj. $K_D \neq K_E$) je vydáván za asymetrický kryptosystém. Různost klíčů je pro asymetrický kryptosystém sice nutnou podmínkou, avšak nikoliv podmínkou postačující. Například tzv. maticová šifra využívá jako šifrovací klíč matici $\boldsymbol{K}$ a dešifrovacím klíčem je inverzní matice $\boldsymbol{K}^{-1}$. Zpráva má podobu vektoru $\boldsymbol{Z}$ a vektor kryptogramu C se určuje podle vztahu $\boldsymbol{C} = \boldsymbol{K} \times \boldsymbol{Z}$. Dešifrování se provádí tak, že se vypočítá $\boldsymbol{K}^{-1} \times \boldsymbol{C} = \boldsymbol{Z}$. Na uvedeném příkladě vidíme, že oba klíče jsou různé. Protože však výpočet dešifrovacího klíče $\boldsymbol{K}^{-1}$ z šifrovacího klíče $\boldsymbol{K}$ je i pro rozsáhlé matice velmi rychlý, útočník by ze znalosti veřejně známého $\boldsymbol{K}$ snadno zjistil soukromý dešifrovací klíč $\boldsymbol{K}^{-1}$. Pro asymetrický kryptosystém je tedy podmínkou praktická neodvoditelnost dešifrovacího klíče z klíče šifrovacího, a nikoliv jen různost těchto klíčů.

Autentičnost zprávy jsme definovali jako stav, kdy informace o původu přijaté zprávy jsou pravdivé. Informace o původu zprávy obvykle popisují původce zprávy, čas vzniku zprávy a místo vzniku zprávy, avšak provozovatel kryptosystému může informace o původu zpráv definovat podle vlastních konkrétních potřeb. S autentičností zpráv úzce souvisejí pojmy nepopiratelnost a integrita. První z uvedených pojmů rozebereme později a nyní se budeme věnovat pojmu integrita zprávy. Integritou zprávy se obvykle rozumí stav, že zpráva nebyla během svého přenosu pozměněna, tj. adresát přijal zprávu, jež je totožná se zprávou, kterou původce vyslal. Je-li zpráva během přenosu pozměněna, pak je takzvaně porušena integrita zprávy. Pokud však došlo při přenosu zprávy k neúmyslné nebo úmyslné změně třeba i jediného bitu, pak za původce zprávy již nelze uvádět odesílatele zprávy. Jednoduše proto, že odesílatel takovouto zprávu neodeslal. Vidíme tedy, že integrita zprávy je pouhým neoddělitelným aspektem autentičnosti zprávy. V dalším textu se proto nebudeme problematikou zabezpečení integrity zpráv samostatně zabývat.

Většina informací o původu bývá obvykle zapsána přímo ve zprávě (např. identifikační údaje původce, čas vzniku zprávy apod.). Ke zprávě pak její původce připojuje dodatečná data, která adresátovi zprávy umožní ověřit pravdivost informací o původu zprávy. Na obr. 1.3 je uvedeno schéma nejčastěji používaného kryptosystému pro zajištění autentičnosti. Tento typ kryptosystému budeme také označovat jako autentizační kryptosystém. Jeho princip je analogický se zajišťováním autentičnosti listinných dokumentů pomocí pečetí, a proto zde zavedeme podobnou terminologii. K fungování zmíněného kryptosystému je opět zapotřebí dvou parametrů. Na straně původce je to číslo K_P, které nazveme pečetící klíč, a na straně adresáta se jedná o číslo K_V, který nazveme ověřovací klíč. Jádrem systému jsou dvě speciální matematické funkce, které pojmenujeme pečetění a ověřování. Funkce pečetění Q je funkce, která je určena pečetícím klíčem K_P. Tato funkce každé zprávě Z přiřadí nějaké číslo P, které nazveme pečeť zprávy. V praxi se pečetě zpráv nazývají různě – například MAC („Message Authentication Code“), MIC („Message Integrity Check“), HMAC („Hashed MAC“), digitální podpis („Digital Signature“) apod.



Obr. 1.3: Kryptografický systém pro zajištění autentičnosti přenášených zpráv.

Pečetění můžeme formálně vyjádřit následovně:

$$P = \mathrm{Q}(Z, K_P),$$

přičemž požadujeme, aby k praktickému zjištění hodnoty závisle proměnné (tj. P) byla zapotřebí znalost tajného pečetícího klíče K_P. Funkce pečetění je konstruována tak, aby útočník s předpokládanou úrovní možností nebyl schopen bez znalosti pečetícího klíče odvodit k libovolné zprávě správnou pečeť dříve, nežli je stanovená doba rezistence pečeti.

Původce zprávy odešle adresátovi jak zprávu Z, tak i její pečeť P. Na straně adresáta (někdy označovaného jako ověřovatele) se v kryptografickém systému provede ověření V, což je funkce, jejímž vstupem je zpráva Z, pečeť P a ověřovací klíč K_V. Hodnota funkce V nabývá dvou hodnot – zpráva je autentická (tj. informace o původu zprávy jsou pravdivé) a zpráva není autentická. Formálně můžeme funkci ověření zapsat následovně:

$$V(Z, P, K_V) = \begin{cases} \text{zpráva } Z \text{ je autentická} \\ \text{zpráva } Z \text{ není autentická} \end{cases}$$

Dvojice pečetící a ověřovací klíč opět nemohou být libovolné. Mezi oběma uvedenými parametry musí samozřejmě existovat určitá závislost, kterou můžeme formálně vyjádřit funkcí:

$$K_P = f(K_V).$$

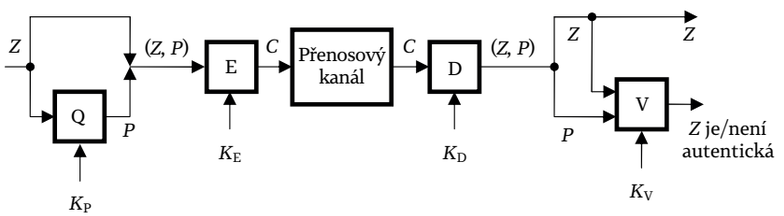
Pokud je prakticky možné pečetící klíč K_P zjistit z hodnoty ověřovacího klíče K_V, pak oba klíče musí být tajné (tzv. tajné klíče). V tomto případě mají oba klíče z hlediska utajení stejné, tj. symetrické postavení, a proto se tyto kryptosystémy nazývají symetrické autentizační kryptosystémy nebo také autentizační kryptosystémy s tajným klíčem. K nejznámějším reprezentantům uvedené třídy kryptosystémů náleží technika HMAC. Pokud je však prakticky nemožné klíč K_P zjistit z hodnoty klíče K_V, pak šifrovací klíč může být veřejně známý (tzv. veřejný klíč) a utajovat je zapotřebí pouze pečetící klíč (tzv. soukromý klíč). V popsaném případě mají oba klíče z hlediska jejich utajení nestejné, tj. asymetrické postavení, a proto se tyto kryptosystémy nazývají asymetrické autentizační kryptosystémy nebo také autentizační kryptosystémy s veřejným klíčem. Nejznámějšími reprezentanty těchto autentizačních kryptosystémů jsou systémy digitálního podpisu.

Asymetrické autentizační kryptosystémy umožňují prakticky realizovat tzv. nepopiratelnost („non-repudiation“). U symetrického autentizačního kryptosystému může pečeť zprávy vytvořit nejen její původce (dále subjekt A), ale také ověřovatel zpráv (dále subjekt B). Subjekt B zná ověřovací klíč a z něho může odvodit pečetící klíč. Subjekt B potom může vytvořit nějakou zprávu, do informací o jejím původu uvede jako původce subjekt A, opatří ji správnou pečetí a zprávu s touto pečetí zašle sám sobě. Může potom tvrdit,

že danou zprávu mu zaslal subjekt A, přičemž mu obecně vzato nikdo nemůže dokázat opak. V případě asymetrického autentizačního kryptosystému toto možné není, protože subjekt B není prakticky schopen odvodit hodnotu pečetícího klíče subjektu A. Na druhou stranu subjekt A nemůže v tomto případě u jakékoliv zprávy se správnou pečetí popřít, že tuto zprávu pečetil on – nikdo jiný totiž správný pečetící klíč nezná.

Lze tedy shrnout, že u symetrických autentizačních kryptosystémů může informaci o původci zprávy ověřit jen její adresát. Adresát přijme zapečetěnou zprávu (Z, P), ověřovací funkcí ověří správnost pečeti, a protože ví, že si tuto zprávu neposlal sám, má záruku, že zpráva pochází od majitele pečetícího klíče K_P. U asymetrických autentizačních kryptosystémů však může informaci o původci zprávy ověřit pomocí veřejného klíče K_V kdokoliv, a navíc původce zprávy nemůže autorství zprávy popřít. V obou případech však jde o ověření autentičnosti, tj. pravdivosti informací o původu zprávy. Nepopiratelnost autorství zprávy tak lze chápat jen jako speciální vlastnost, kterou nabízejí asymetrické autentizační kryptosystémy.

Asymetrické autentizační kryptosystémy, jejichž primárním účelem je zajistit nepopiratelnost informace o původci zprávy, se nazývají systémy digitálního podpisu. K nejznámějším systémům tohoto typu náleží kryptosystém DSA nebo RSA-PSS. Jak již bylo řečeno, systémy digitálního podpisu můžeme považovat za speciální případ asymetrického autentizačního kryptosystému. Funkce pečetění se nazývá podepisování a soukromý pečetící klíč se nazývá podepisovací klíč.



Obr. 1.4: Utajovací a autentizační kryptosystém.

Utajovací a autentizační kryptosystémy obecně zajišťují buď důvěrnost, nebo autentičnost zpráv. Pokud je zapotřebí zajistit oba bezpečnostní aspekty současně, pak se praxi postupuje obvykle tak, že na straně původce je zpráva Z nejprve opatřena pečetí P a dvojice (Z, P) je poté zašifrována (viz obr. 1.4). Na straně příjemce je přijatý kryptogram nejprve dešifrován a následně je ověřena autentičnost zprávy pomocí její pečeti. Tím je zajištěna současně důvěrnost i autentičnost zpráv.

Existují však i systémy, kdy se nejprve zašifruje zpráva a vzniklý kryptogram se opatří pečetí. K adresátovi se tedy přenáší dvojice (C, P). Adresát nejprve ověří pečeť kryptogramu a poté kryptogram dešifruje. Výhodou tohoto řešení je skutečnost, že pokud se zjistí, že kryptogram není autentický, jeho další zpracování se neprovádí, tj. ušetříme čas a kapacity, které by si dešifrování kryptogramu vyžádalo. Nevýhodou však je skutečnost, že původce neví, co přesně pečetí, protože zpráva je zašifrována, tj. je v nečitelné podobě. To je v případě podepisování nepřípustné.

Na závěr této podkapitoly je vhodné ještě zmínit, že autentizační kryptosystémy lze využít také k ověřování identity osob. Je to důsledek skutečnosti, že ověřením informace o původu přijaté zprávy se automaticky ověřuje identita původce dané zprávy. Autentizací zpráv tak lze řídit přístup osob do fyzických prostorů (např. do místností nebo budov) nebo do kybernetických prostorů (např. k datům na internetu nebo v počítači). Popsané systémy se nazývají přístupové systémy. Osoby jsou v tomto případě vybaveny specializovanými autentizačními předměty (obvykle se jedná o mikropočítačové karty), které komunikují s řídicí jednotkou přístupového systému. Řídicí jednotka ověřuje autentičnost zpráv přijatých od autentizačního předmětu a v pozitivním případě dané osobě umožní přístup k chráněným aktivům. Uvedený typ autentizace osob náleží do kategorie autentizace předmětem.

1.3 TEORIE UTAJENÍ A AUTENTIZACE ZPRÁV

Kryptografie vznikla prakticky současně se vznikem písma. Když se lidé naučili pomocí písma zaznamenávat informace, současně vznikla i potřeba, aby tyto záznamy byly schopny přečíst pouze oprávněné osoby. Vznikaly tak různé kryptografické utajovací kryptosystémy. Spolu s nimi však vznikla i kryptoanalýza, která se zabývala překonáváním těchto kryptosystémů, tj. zabývala se luštěním kryptogramů bez znalosti dešifrovacího klíče. Kryptoanalýza se vyvíjela současně s kryptografií a obě se navzájem stimulovaly. Nové kryptografické techniky zapříčinily vznik nových kryptoanalytických metod a naopak.

Vzhledem k úspěchům kryptoanalýzy, kdy prakticky každý navržený kryptosystém byl nakonec překonán, se v minulosti řada kryptologů začala domnívat, že nepřekonatelný kryptosystém ani neexistuje. Tento názor například v roce 1843 formuloval amatérský kryptolog a spisovatel E. A. Poe, který ve své povídce [3] (s. 105) ústy hlavního hrdiny příběhu vyslovuje otázku, zda je lidský důmysl vůbec schopen sestrojit takovou šifru, kterou by lidský důmysl opět nebyl schopen vyřešit. Definitivní odpověď na tuto otázku přišla až v roce 1949 a jejím autorem byl americký matematik C. E. Shannon.

Pan Shannon ve své práci [4] uvádí, že utajovací kryptosystém může poskytnout tři stupně důvěrnosti:

- maximální důvěrnost („perfect secrecy“),
- redukovanou důvěrnost („ideal secrecy“),
- minimální důvěrnost („practical secrecy“).

Uvedené stupně důvěrnosti zpráv jsou definovány pomocí pojmů z teorie informace. My si je vysvětlíme jednodušeji a názorněji pomocí analýzy šifrovací a dešifrovací funkce.

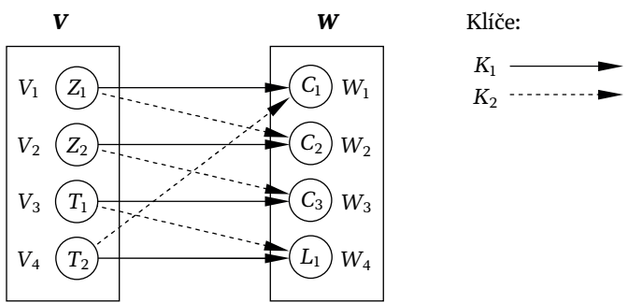
Šifrování E jsme definovali jako prostou funkci, která je určena šifrovacím klíčem K_E. Tato funkce každé zprávě Z přiřadí číslo C, které se nazývá kryptogram. Formálně jsme funkci šifrování vyjádřili následovně:

$$C = E(Z, K_E).$$

Nyní si definici funkce šifrování rozšíříme a zpřesníme. Jak již bylo uvedeno, šifrovací klíč K_E je považován za parametr, a tak pro konkrétní hodnotu klíče lze šifrování považovat za funkci jedné proměnné, kdy je vstupní hodnotě Z přiřazena hodnota výstupu C. Množinou vstupů $\boldsymbol{V}$ šifrovací funkce E jsou čísla V (tzv. vzory), s nimiž může daný kryptografický systém pracovat. Pokud je ve vzoru $V \in \boldsymbol{V}$ zakódována informace, pak se jedná o zprávu Z. Vzor, v němž není zakódována žádná informace, nazveme prázdným vzorem T. Množinu výstupů $\boldsymbol{W}$ funkce E tvoří hodnoty W (tzv. obrazy) všech vzorů. Obraz $W \in \boldsymbol{W}$, který je alespoň pro jednu hodnotu klíče K_E přiřazen nějaké zprávě, nazýváme kryptogram C. Ostatní obrazy nazveme prázdným obrazem L.

Předpokládáme, že počet prvků množin $\boldsymbol{V}$ i $\boldsymbol{W}$ je roven číslu m a připomínáme, že funkce šifrování je prostá funkce. Máme-li množinu šifrovacích klíčů $\boldsymbol{K}$, potom pro každý klíč $K_E \in \boldsymbol{K}$ platí, že pro každou dvojici vzorů $V_1 \neq V_2$ lze psát $E(V_1, K_E) \neq E(V_2, K_E)$. Každý klíč tedy přiřazuje každému vzoru z m možných jeden unikátní obraz z m možných. Pokud tvoříme konkrétní šifrovací transformaci, zvolíme si první vzor a tomu přiřadíme jeden z m obrazů. Druhému vzoru pak přiřadíme jeden z $(m - 1)$ zbývajících obrazů atd. Potom pro maximální počet přiřazení, tj. pro maximální počet klíčů K_{Max}, platí $K_{Max} = m!$ V prakticky používaných systémech bývá počet možných klíčů podstatně menší.

Výše uvedené definice ilustruje obrázek 1.5. Množinu vstupů $\boldsymbol{V}$ funkce šifrování tvoří čtyři vzory V_1 až V_4. Informaci nesou vzory V_1 a V_2 (jsou označeny jako zprávy Z_1 a Z_2) a zbývající dva vzory nemají v daném jazyce nebo kódu význam. Ty jsou označeny jako prázdné vzory T_1 a T_2. V kryptosystému jsou definovány dva klíče. Funkce šifrování je pro první klíč K_1 definována plnými čarami s šipkami a pro druhý klíč K_2 je definována přerušovanými čarami s šipkami. Množina obrazů $\boldsymbol{W}$ je definována rovněž čtyřmi prvky, protože šifrovací funkce musí pro každý daný klíč kvůli jednoznačnosti dešifrování přiřadit každému možnému vzoru unikátní obraz. V našem příkladě v množině obrazů existují tři kryptogramy C_1 až C_3 a jeden prázdný obraz L_1.



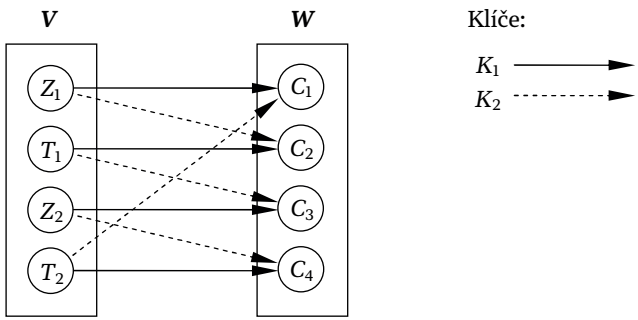
Obr. 1.5: Příklad funkce šifrování.

Nyní definujme valenci *Val* obrazu W_i jako počet zpráv, které vzniknou dešifrováním W_i všemi možnými klíči. Na našem obrázku například $Val(W_1) = 1$, protože dešifrováním obrazu W_1 pomocí klíče K_1 vznikne V_1 a dešifrováním pomocí klíče K_2 vznikne V_4. Protože zprávou je jen V_1, valence W_1 je rovna jedné. Platí, že valence kryptogramu je alespoň 1 a nanejvýše Min{N, K}, kde N je celkový počet zpráv a K je celkový počet klíčů. Obraz s valencí rovnou nule je prázdný obraz.

Dále definujme veličinu M jako minimální valenci ze všech kryptogramů. V našem příkladě je valence všech kryptogramů rovna hodnotě 1, 2, a 1 a tak

Předpokládejme například, že původce chce odeslat zprávu Z_1 a s adresátem má domluven klíč K_2. Vyslán je tedy kryptogram $E(Z_1, K_2) = C_2$. Útočník v přenosovém kanále tento kryptogram odposlechne, vyzkouší oba možné klíče a získá $D(C_2, K_1) = Z_2$ a $D(C_2, K_2) = Z_1$. Dospěje tak k závěru, že mohla být přenesena buď zpráva Z_1, nebo zpráva Z_2. V žádném případě však nebyla přenášena zpráva Z_3 ani zpráva Z_4. Redukovaná důvěrnost je v praxi možná, pokud je délka zpráv srovnatelná s délkou klíčů nebo pokud zprávy mají velmi nízkou redundanci, tj. pravděpodobnost výskytu prázdného vzoru je nízká. Oba popsané případy bývají ojedinělé, a tak se s kryptosystémy poskytujícími redukovanou důvěrnost prakticky nepotkáváme.

V případě minimální důvěrnosti zpráv je minimální valence rovna jedné, což znamená, že dešifrováním kteréhokoliv kryptogramu pomocí všech klíčů útočník získá jedinou možnou zprávu, a tím kryptogram zároveň vyluští. Příklad kryptosystému s minimální důvěrností zpráv ilustruje obr. 1.8.



Obr. 1.8: Příklad kryptosystému s minimální důvěrností zpráv.

Předpokládejme, že původce chce odeslat zprávu Z_1 a s adresátem má domluven klíč K_2. Vyslán je tedy kryptogram $E(Z_1, K_2) = C_2$. Útočník v přenosovém kanále tento kryptogram odposlechne, vyzkouší oba možné klíče a získá $D(C_2, K_1) = T_1$ a $D(C_2, K_2) = Z_1$. Prázdný vzor T_1 může vyloučit, a tak dospěje k závěru, že mohla být přenesena pouze zpráva Z_1. Tím je kryptogram vyluštěn.

Dále uvidíme, že kryptosystémy s minimální důvěrností zpráv jsou v praxi i přes uvedenou slabinu používány nejčastěji. Je to dáno tím, že počet všech možných klíčů je tak velký, že v rámci požadované doby rezistence kryptogramu je technicky nemožné útok hrubou silou provést. Například pro symetrické