Karel Burda

Kryptografie okolo nás

Edice CZ.NIC

KRYPTOGRAFIE OKOLO NÁS
Karel Burda

Vydavatel:
CZ.NIC, z. s. p. o.
Milešovská 5, 130 00 Praha 3
Edice CZ.NIC
www.nic.cz

1. vydání, Praha 2019
Kniha vyšla jako 24. publikace v Edici CZ.NIC.
ISBN 978-80-88168-49-2

CZ.NIC | SPRÁVCE DOMÉNY CZ

ISBN 978-80-88168-49-2

— Karel Burda

Kryptografie okolo nás

— Edice CZ.NIC

Předmluva vydavatele

Předmluva vydavatele

Vážení čtenáři,

tím, jak se náš běžný život čím dál více přesouvá do online světa internetu, nabývá kryptografie na důležitosti. Do elektronického světa je nutné promítnout řešení problémů v reálném světě již alespoň částečně vyřešených, jako je zajištění soukromí při komunikaci, prokazování totožnosti komunikujících stran nebo autenticity vyměňovaných zpráv. Toto všechno a mnohem více pomáhá vyřešit právě kryptografie.

Vzhledem k tomu, že internet vznikal převážně na akademické půdě, nevnímali jeho průkopníci výše uvedené problémy jako klíčové, a tak spousta protokolů stojících v samotných základech internetu získávala důležité bezpečností prvky se značným zpožděním. Ještě větší urychlení v tomto směru přineslo odhalení praktik tajných služeb v posledních letech. Přestože použití kryptografie jako nástroje není možné z principu morálně posoudit, nelze ignorovat, že bývá nezřídka zneužívána k páchání trestné činnosti. Nechtěně se tak stává bitevním polem, na kterém se utkávají internetoví architekti a vývojáři aplikací na jedné straně a bezpečnostní složky nebo celé vlády na straně druhé. Bez ohledu na to, jak tato bitva dopadne, je určitě užitečné získat přehled o tom, kde všude se můžeme ve světě internetu s kryptografií setkat. A takový přehled vám zaručeně poskytne právě tato kniha.

Autor Karel Burda, vysokoškolský pedagog na VUT v Brně, touto knihou volně navazuje na své předchozí publikace a popisuje v ní celou řadu internetových technologií a protokolů, které kryptografii využívají. Osobně se s mnoha z nich setkávám při své práci denně. Jako příklad bych jmenoval DNSSEC (rozšíření protokolu DNS o kryptografické zajištění autenticity DNS odpovědí), v jehož rozšíření a tedy počtu zabezpečených domén jsme v ČR světovými lídry, nebo podporu nejmodernějšího autentizačního protokolu OpenID Connect službou mojeID, kterou u nás využívá přes 600 000 lidí.

Ať už knihu přečtete od začátku do konce, nebo pouze nalistuje část obsahující protokol, který vás nejvíce zajímá, jsem přesvědčen, že získané informace vám umožní pohybovat se po internetu s mnohem větší důvěrou a jistotou.

Jaromír Talíř, CZ.NIC
Praha, 1. listopadu 2019

Obsah

Úvod

Úvod

První kryptografické techniky (tzv. šifry) vznikly prakticky vzápětí po vzniku písma, neboť jejich účelem bylo utajit obsah písemných zpráv před nepovolanými čtenáři. Historicky nejstarším známým důkazem o praktickém využití kryptografie je hliněná destička ze starověké Mezopotámie z období asi 1.500 let před naším letopočtem, na níž je uveden šifrovaný popis technologie výroby glazurované keramiky. Zpočátku se v šifrách používaly jednoduché záměny znaků ve zprávě (tzv. substituce), nebo se ve zprávě měnilo pořadí znaků (tzv. transpozice). Postupně se však ukázalo, že z bezpečnostních důvodů je zapotřebí šifrovací postupy kombinovat a komplikovat. Šifry se tak stávaly stále složitějšími a k jejich použití, analýze a návrhu se proto začala používat matematika. V minulém století se také zjistilo, že matematické metody lze použít nejen k utajování obsahu zpráv, ale rovněž k prokazování původu doručených zpráv. Z původně jednoduchých šifrovacích technik se tak nakonec vyprofilovala kryptografie jako věda, která se zabývá konstrukcí a aplikací matematických metod pro utajování obsahu a prokazování původu přenášených zpráv.

Kryptografie primárně vznikla k ochraně zpráv během jejich přenosu, a tak až donedávna byly její doménou přenosové systémy. Praxe však ukázala, že pomocí kryptograficky chráněných zpráv lze velmi efektivně zajistit vysokou úroveň bezpečnosti mnoha dalších systémů, jako například systémů řízení přístupu, systémů elektronických plateb apod. S aplikacemi kryptografie proto přicházíme do styku každodenně, avšak všeobecné povědomí o tom, jak fungují, je nízká. Je to dáno zejména tím, že uvedené aplikace jsou poměrně složité.

Vzhledem ke složitosti a rozsáhlosti kryptografických aplikací budeme v této knize abstrahovat od různorodosti účelově stejných funkcí. To znamená, že celý soubor kryptografických funkcí, které jsou z hlediska svého účelu stejné, budeme reprezentovat jedinou obecnou funkcí. Nebudeme tak například rozlišovat, zda se šifrování provádí proudovou či blokovou šifrou, jakými algoritmy a případně v jakých režimech. Tímto přístupem si zjednodušíme situaci natolik, že nám pak k popisu naprosté většiny kryptografických aplikací postačí sedm elementárních kryptografických funkcí a jeden generátor. Konkrétně se jedná o:

- šifrovací (ENC) a k ní komplementární dešifrovací (DEC) funkci,
- pečetící (PCT) a k ní komplementární verifikační (VER) funkci,
- hešovací funkci (HSF),
- Diffie-Hellmanovu funkci (DHF),
- odvozovací funkci (ODF),
- generátor nepředvídatelných čísel (GEN).

Uvedený přístup umožní čtenáři rychle a efektivně porozumět principu fungování celé řady velmi různorodých kryptografických aplikací. Zaplatí za to určitými zjednodušeními, ale úplnější a detailnější informace se případný zájemce může dozvědět z odkazované literatury.

Struktura knihy je následující. Po tomto úvodu následuje kapitola Základy kryptografie, kde se čtenář podrobněji seznámí s výše uvedenými elementárními kryptografickými funkcemi. Zbytek knihy je věnován popisu kryptografických aplikací, s nimiž se potkáváme v běžném životě. Jsou rozděleny celkem do tří kapitol. V kapitole Přenosové systémy jsou vysvětleny kryptograficky zabezpečené protokoly, jejichž primárním účelem je zajistit bezpečný přenos zpráv. Příkladem jsou protokol TLS, který používáme kupříkladu v internetovém bankovnictví, nebo protokoly komplexu WPA, kterými se zabezpečují rádiové přenosy ve Wi-Fi sítích. V kapitole Přístupové systémy jsou popisovány protokoly k prokázání identity osob (např. Kerberos) a k řízení přístupu osob buď k síťovým službám (např. RADIUS), nebo do fyzických prostor (elektronická kontrola vstupu). Poslední kapitola s názvem Platební systémy je věnována platebním protokolům, jejichž účelem je elektronický převod peněz mezi účty uživatelů (např. protokoly pro platební karty či kryptoměna Bitcoin).

1 Základy kryptografie

1 Základy kryptografie

Jak již bylo uvedeno kryptografie je věda, která zkoumá matematické metody utajování obsahu i prokazování původu přenášených zpráv. Zprávou přitom budeme rozumět číselnou posloupnost, v níž je veřejně známým kódem zakódována informace. V praxi se zpravidla jedná o texty, obrázky a případně příkazy v podobě posloupností dvojkových číslic (tzv. bitů).

Autor zprávy (tzv. původce) svoji zprávu předává vhodným přenosovým systémem (typicky přes počítačovou síť) zamýšlenému příjemci (tzv. adresátovi). Z kryptografického hlediska mají běžně používané přenosové systémy charakter tzv. veřejného přenosového kanálu, což znamená, že ke kanálu mají kromě původce a adresáta přístup i jiné (tzv. neoprávněné) osoby. Některé z těchto osob usilují o čtení, resp. pozměňování přenášených zpráv, a tak je nazveme útočníky. Kryptografické techniky umožňují původci a adresátovi zajistit ochranu přenášených zpráv před uvedenými hrozbami. V případě utajování obsahu zpráv nejsou útočníci schopni zjistit, jaké zprávy jsou v přenosovém kanálu předávány (tzv. důvěrnost zpráv). A v případě prokazování původu zpráv si je adresát schopen ověřit, zda přijatá zpráva skutečně pochází od udávaného původce, tj. zda tato zpráva nebyla během přenosu případným útočníkem nějakým způsobem pozměněna, či dokonce nebyla celá podvržena (tzv. autentičnost zpráv).

Zabezpečená komunikace mezi původcem a adresátem je definována kryptografickým protokolem. Základ kryptografického protokolu tvoří datové jednotky, což jsou bloky bitů, které si mezi sebou původce s adresátem vyměňují. Každý typ datové jednotky má svoji určenou strukturu a svůj význam. Kromě různých typů datových jednotek je součástí protokolu i sada pravidel, jimiž se výměna datových jednotek mezi původcem a adresátem (v protokolu se nazývají strany) řídí. Kromě dvoustranných protokolů existují i vícestranné protokoly, což jsou protokoly, kde se výměna datových jednotek uskutečňuje mezi více subjekty. Reprezentantem vícestranného protokolu jsou například platební protokoly, na nichž se kromě plátce a příjemce zúčastňuje také banka plátce a banka příjemce.

Než přejdeme k základním kryptografickým funkcím, tak si zde ještě vysvětlíme operaci, která se nazývá zřetězení. Vstupem operace zřetězení jsou dva bitové bloky x a y, přičemž výstupem je blok z, který vznikne připojením bloku y na konec bloku x. Formálně budeme uvedenou operaci značit

$$z = x \| y.$$

Pokud máme například dva bloky $x = 00$ a $y = 101$, tak $z = x \| y = 00 \| 101 = 00101$.

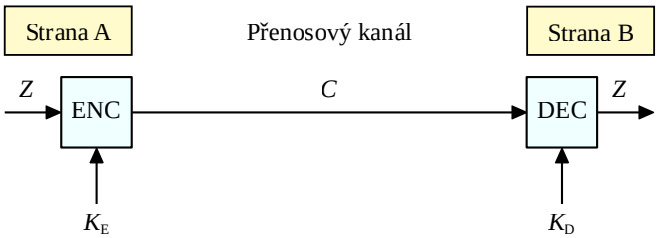
Na závěr této podkapitoly si ještě domluvíme typografické konvence, které v této knize použijeme. Jednotlivá písmena v základním řezu budou reprezentovat strany (např. strana A) a řetězce písmen v základním řezu budou vyjadřovat funkce (např. šifrování ENC). Písmena či jejich řetězce v kurzívě pak budou označovat proměnné (např. zpráva *Z* nebo blok ukončení zprávy *UZ*).

1.1 Utajovací kryptosystémy

Účelem utajovacích kryptosystémů je zajistit důvěrnost zpráv, což v praxi znamená utajení obsahu těchto zpráv před neoprávněnými osobami. Již jsme si uvedli, že zpráva (např. text či obraz) je číselná posloupnost, ve které jsou veřejně známým kódem zakódovány informace. K utajení obsahu zpráv (tedy k utajení zakódovaných informací) se zprávy Z převádějí na tzv. kryptogramy. Kryptogram C je číselná posloupnost, která je tzv. pseudonáhodná. To znamená, že kryptogram se jeví jako náhodná posloupnost čísel, avšak ve skutečnosti náhodnou posloupností není. Kryptogram je oproti zprávě veřejný, tj. je přístupný i neoprávněným osobám. Jeho pseudonáhodný charakter však způsobuje, že případní útočníci nejsou schopni jej převést zpět do podoby původní zprávy. Pouze oprávněná osoba, která zná tajný číselný parametr, je schopna provést konverzi kryptogramu na původní zprávu a z ní pak zakódované informace zjistit.

Strukturu utajovacího kryptosystému (nebo-li šifry) ilustruje obr. 1.1. Strana A (odesílatel) přivede svoji zprávu Z na vstup tzv. šifrovací funkce, kterou v dalším budeme označovat zkratkou ENC (z anglického „encrypting“). Tato funkce přiřazuje každé vstupní číselné posloupnosti Z právě jednu pseudonáhodnou posloupnost C. Z bezpečnostních důvodů musí v každém kryptosystému existovat velké množství použitelných šifrovacích funkcí (tzv. rodina funkcí) a konkrétní použitou funkci (tj. konkrétní přiřazení) pak definuje parametr K_E, který se nazývá šifrovací klíč. Přiřazení kryptogramu C vstupní zprávě Z pro danou hodnotu klíče K_E se nazývá šifrování a formálně je budeme vyjadřovat vztahem

$$C = \mathrm{ENC}(Z, K_E).$$



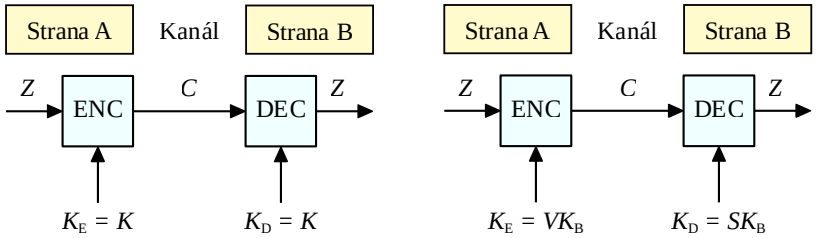
Obrázek 1.1: Struktura utajovacího kryptosystému

Odesílatel odešle kryptogram C veřejným kanálem k adresátovi B. Během tohoto přenosu se ke kryptogramu mohou dostat i neoprávněné osoby, avšak pouze oprávněný adresát B zná hodnotu tajného parametru K_D, který se nazývá dešifrovací klíč. Pomocí tohoto parametru nastaví tzv. dešifrovací funkci DEC („decrypting“) tak, aby byla inverzní k šifrovací funkci ENC. Na výstupu dešifrovací funkce se proto objeví původní zpráva Z. Formálně budeme proces dešifrování zapisovat vztahem

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

Funkce ENC a DEC jsou obvykle veřejně známy (často jsou dokonce standardizovány). Požaduje se po nich, aby bez znalosti dešifrovacího klíče K_D nebylo prakticky možné ke kryptogramům C zjistit jim odpovídající zprávy Z. Další požadavek vyplývá ze skutečnosti, že dešifrovací klíč často slouží k dešifrování více kryptogramů. Proto se po funkcích ENC a DEC ještě požaduje, aby ze znalosti různých dvojic zpráva a odpovídající kryptogram nebylo prakticky možné odvodit hodnotu používaného dešifrovacího klíče K_D.

Utajovací kryptosystémy se dělí na symetrické a asymetrické (viz obr. 1.2).



Obrázek 1.2: Symetrický (vlevo) a asymetrický (vpravo) utajovací kryptosystém

U symetrických kryptosystémů platí, že zjistit hodnotu dešifrovacího klíče ze znalosti hodnoty klíče šifrovacího je prakticky možné. Z tohoto důvodu se musí utajovat hodnoty obou klíčů, přičemž obvykle platí, že tyto klíče jsou stejné, tj. $K_D = K_E = K$, kde K se nazývá tajný klíč. Symetrické kryptosystémy jsou rychlé, a tak se využívají k šifrování velkých objemů dat. Nevýhodou symetrických kryptosystémů je skutečnost, že bezpečné doručení klíče K komunikující protistraně je vzhledem k tajnému charakteru klíče komplikované.

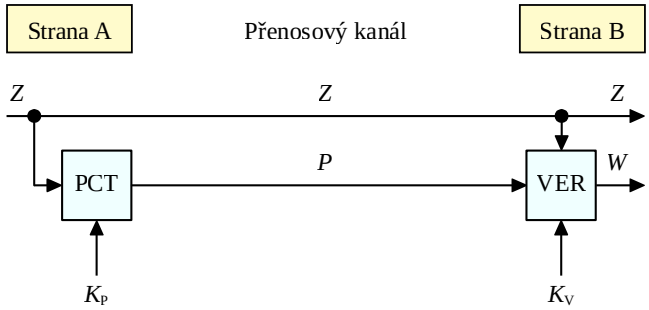
U asymetrických kryptosystémů naopak platí, že určení hodnoty dešifrovacího klíče ze znalosti hodnoty klíče šifrovacího je prakticky nemožné. Z tohoto důvodu je pak nutné utajovat pouze hodnotu dešifrovacího klíče. Adresát B si nejprve stanoveným postupem vytvoří dvojici šifrovací a dešifrovací klíč. Tato dvojice se odvozuje z velkých náhodných čísel, a tak pravděpodobnost, že dva uživatelé vytvoří stejnou dvojici klíčů, je prakticky rovná nule. Dešifrovací klíč je tajný a je znám pouze jeho tvůrci B (tzv. soukromý klíč SK_B strany B). Hodnotu šifrovacího klíče tvůrce daného kryptosystému zveřejní (tzv. veřejný klíč VK_B strany B). Platí tak, že $K_D = SK_B$ a $K_E = VK_B$. Adresátovi B potom může zasílat kryptogramy kdokoliv, bez nutnosti si s ním šifrovací klíč předem sjednat. Nevýhodou je, že asymetrické kryptosystémy jsou pomalé, a tak se používají k šifrování dat o malých objemech. Typicky se jedná o klíče pro symetrické kryptosystémy a o hesla.

1.2 Autentizační kryptosystémy

Účelem autentizačních kryptosystémů je garantovat adresátům původ doručených zpráv (tzv. autentičnost zpráv) [1]. Zpravidla se jedná o autorství zprávy, případně lze garantovat i další atributy původu zprávy, jako je čas nebo místo jejího vzniku. Princip autentizačních kryptosystémů je takový, že odesílatel spolu se zprávou Z odesílá i krátkou číselnou posloupnost P, která umožní adresátovi původ zprávy ověřit.

Strukturu autentizačního kryptosystému ilustruje obr. 1.3. Odesílatel A přivede svoji zprávu Z na vstup tzv. pečetící funkce, kterou budeme označovat zkratkou PCT. Zmíněná funkce přiřazuje každé vstupní číselné posloupnosti Z jednu z mnoha možných výstupních posloupností P. Posloupnost P nazveme pečeť. Konkrétní přiřazení pečetí jednotlivým zprávám se nastavuje pomocí tajného parametru K_P, jenž nazveme pečetící klíč. Proces přiřazení pečeti P vstupní zprávě Z budeme nazývat pečetění a formálně jej budeme vyjadřovat vztahem

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



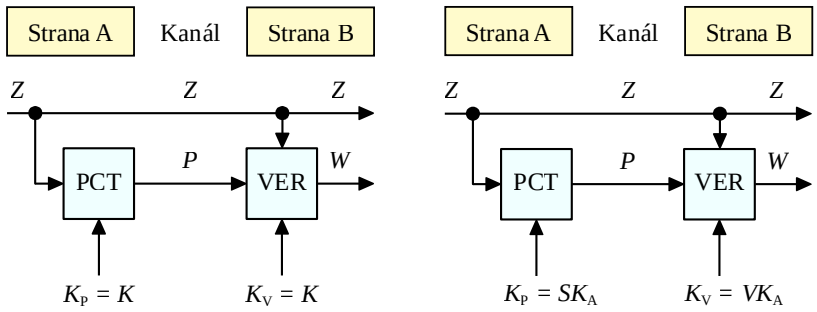
Obrázek 1.3: Struktura autentizačního kryptosystému

Dvojici (Z, P) nazveme zapečetěná zpráva. Odesílatel zapečetěnou zprávu odešle veřejným kanálem k adresátovi zprávy, přičemž během tohoto přenosu ji mohou neoprávněné osoby nahradit falešnou dvojicí (Z', P'). Adresát B zná správnou hodnotu parametru K_V (tzv. verifikační klíč), který definuje verifikační funkci VER. Přijatá zpráva Z spolu s její pečetí P jsou přivedeny na oba vstupy této funkce, v důsledku čehož výstupní hodnota W, kterou nazveme autentizační indikátor, má hodnotu buď 0, nebo 1. Verifikační funkce je konstruována tak, že pokud je pro danou zprávu pečeť správná, tak autentizační indikátor $W = 1$. V takovémto případě adresát zprávu Z akceptuje jako autentickou. V opačném případě, tj. když $W = 0$, adresát přijatou zprávu vyhodnotí jako podvodnou. Verifikaci budeme formálně zapisovat vztahem

$$W = \mathrm{VER}(Z, P, K_V).$$

Funkce PCT a VER jsou obvykle veřejně známy. Požaduje se po nich, aby bez znalosti pečetícího klíče K_P nebylo prakticky možné ke zprávám Z určit správné pečeti P. Pečetící klíč je zpravidla používán vícenásobně, tj. jeden pečetící klíč slouží k pečetění mnoha různých zpráv. Proto se také požaduje, aby ze znalosti různých dvojic zpráva a odpovídající pečeť nebylo prakticky možné odvodit hodnotu používaného pečetícího klíče K_P.

Stejně jako utajovací, tak i autentizační kryptosystémy se dělí na symetrické a asymetrické (viz obr. 1.4). U symetrických kryptosystémů platí, že zjistit hodnotu pečetícího klíče ze znalosti hodnoty klíče verifikačního je prakticky možné. Proto se musí utajovat hodnoty obou klíčů, přičemž obvykle platí, že tyto klíče jsou stejné, tj. $K_P = K_V = K$, kde K se nazývá tajný klíč. Pečeti symetrických autentizačních kryptosystémů se v anglicky psané literatuře označují mnoha různými zkratkami (MAC = „Message Authentication Code“, MIC = „Message Integrity Check“ nebo ICV = „Integrity Check Value“). Výhodou symetrických kryptosystémů je, že jsou rychlé, a proto se využívají při pečetění velkých množství zpráv. Jejich nevýhodou je opět fakt, že bezpečné doručení klíče K komunikující protistraně je vzhledem k tajnému charakteru klíče komplikované.



Obrázek 1.4: Symetrický (vlevo) a asymetrický (vpravo) autentizační kryptosystém

U asymetrických kryptosystémů naopak platí, že určení hodnoty pečetícího klíče ze znalosti hodnoty klíče verifikačního je prakticky nemožné. Z tohoto důvodu je tak nutné utajovat pouze hodnotu pečetícího klíče. Původce A si stanoveným postupem vytvoří dvojici pečetící a verifikační klíč. Uvedená dvojice se odvozuje z velkých náhodných čísel, a tak pravděpodobnost, že dva uživatelé vytvoří stejnou dvojici klíčů, je prakticky rovná nule. Pečetící klíč je tajný a je znám pouze jeho tvůrci (tzv. soukromý klíč SK_A strany A). Hodnotu verifikačního klíče tvůrce daného kryptosystému zveřejní (tzv. veřejný klíč VK_A strany A). Platí tedy, že $K_P = SK_A$ a $K_V = VK_A$. Autentičnost zpráv od strany A potom může ověřovat kdokoliv, bez nutnosti si s ním předem sjednat verifikační klíč.

Další velmi významnou předností autentizačních asymetrických kryptosystémů oproti symetrickým je skutečnost, že soukromý klíč SK_A zná pouze původce zprávy. A protože SK_A nelze ze

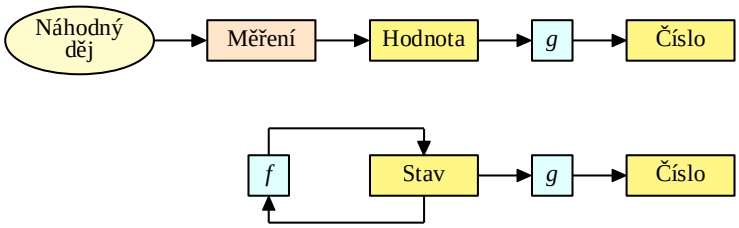
znalosti veřejného VK_A určit, tak správné pečeti dokáže vytvářet pouze strana A. Tato vlastnost způsobuje, že pečeti asymetrického autentizačního kryptosystému vykazují vlastnosti klasického ručního podpisu, kdy podpis dokáže vytvořit pouze jediná osoba a zároveň pravost tohoto podpisu může ověřit kdokoliv. Z tohoto důvodu se pečeti P u asymetrických kryptosystémů nazývají digitálními podpisy („Digital Signature“), soukromý klíč SK_A se nazývá podpisový klíč a funkce PCT se nazývá podpisová funkce. Nevýhodou podpisových kryptosystémů oproti autentizačním symetrickým kryptosystémům je, že jsou pomalé.

1.3 Generátory nepředvídatelných čísel

Generátory nepředvídatelných čísel jsou zařízení určená ke generování posloupností čísel, které se neoprávněným osobám jeví jako náhodné posloupnosti. To konkrétně znamená, že číselné hodnoty v generované posloupnosti mají stejnou pravděpodobnost výskytu a jednotlivá čísla posloupnosti se jeví, že jsou navzájem nezávislá. V kryptografii je tento typ generátorů používán zejména ke generování klíčů a ke generování unikátů (tj. čísel, jimiž se individualizuje vykonání a tedy i výstup kryptografické funkce). Jsou rovněž i základní komponentou tzv. proudových šifer. Vygenerování nepředvídatelného čísla N budeme formálně vyjadřovat

$$N = \mathrm{GEN}.$$

Generátory nepředvídatelných čísel klasifikujeme na náhodné a pseudonáhodné (viz obr. 1.5). Náhodné generátory (obr. nahoře) generují svá čísla na základě nějakého náhodného fyzikálního děje (např. tepelný šum). Měřením se zjišťuje aktuální hodnota náhodné veličiny a výsledky měření se vhodnou konverzní funkcí g převádějí na čísla pro výstup generátoru. Výstup těchto generátorů je tak skutečně náhodný („true random number generator“). Oproti tomu pseudonáhodné generátory („pseudorandom number generator“) generují svá čísla pomocí vhodného stavového automatu (obr. dole). Stavový automat je hardwarová (např. posuvný registr), nebo datová struktura (např. číslo), která může nabývat více stavů (např. obsah registru, nebo velikost čísla). Stavový automat se nejprve nastaví podle tajné náhodné hodnoty (tzv. semeno) do výchozího stavu. Pomocí přechodové funkce f se aktuálnímu stavu pokaždé přiřadí nový následující stav,



Obrázek 1.5: Generátor náhodných (nahoře) a pseudonáhodných (dole) čísel

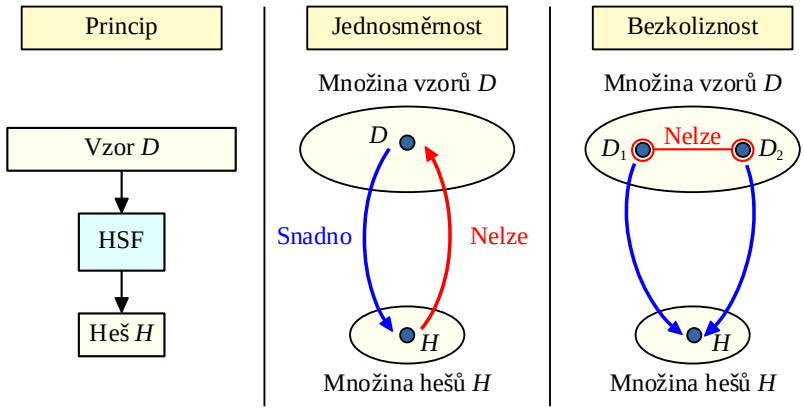
a tak automat postupně prochází všemi určenými stavy. Speciální konverzní funkce g přitom každému aktuálnímu stavu automatu přiřazuje číslo, které je výstupem generátoru. Chování pseudonáhodného generátoru je tedy zcela deterministické, tj. oprávněné osoby, které znají funkce f, g a semeno, dokáží vygenerovat tutéž posloupnost čísel. Požaduje se však, aby neoprávněná osoba došla statistickým testováním vygenerované posloupnosti k závěru, že daná posloupnost je náhodná.

1.4 Hešovací funkce

Hešovací funkce HSF je kryptografická funkce (viz obr. 1.6 vlevo), která číselnému argumentu D (nebo-li vzoru) o prakticky libovolné délce (jednotky bitů až triliony triliónů bitů) přiřazuje tzv. heš H, což je číselná hodnota o pevně stanovené délce (typicky o délce 256 až 512 bitů). Formálně budeme tuto funkci zapisovat

$$H = \mathrm{HSF}(D).$$

Od hešovací funkce se vyžadují dvě specifické vlastnosti, které se nazývají jednosměrnost a bezkoliznost. Jednosměrnost (obr. uprostřed) znamená, že určení hodnoty heše H je pro zadaný vzor D výpočetně snadné, avšak určení hodnoty vzoru D ze znalosti jeho heše H je prakticky nemožné. Bezkolizností (obr. vpravo) se rozumí, že je prakticky nemožné nalézt nějakou dvojici různých vzorů D_1 a D_2 takovou, aby jejich heše byly stejné. V této souvislosti je zapotřebí si uvědomit, že počet číselných posloupností libovolné délky (tj. počet vzorů) je vždy větší než počet posloupností jediné možné délky (tj. hešů). Z toho pak plyne, že mnoho vzorů musí mít stejný heš (tzv. kolize). Požaduje se však, aby nalezení kolize bylo prakticky nemožné.



Obrázek 1.6: Hešovací funkce a její vlastnosti

Jak v dalším uvidíme, tak jednosměrnost a bezkoliznost předurčuje hešovací funkce pro širokou škálu aplikací. Kromě vlastního samostatného nasazení jsou i důležitou komponentou zejména autentizačních kryptosystémů.

1.5 Diffie-Hellmanova funkce

Základním stavebním kamenem hojně využívaného Diffie-Hellmanova (zkráceně DH) protokolu je funkce, kterou nazveme Diffie-Hellmanova funkce (DHF). Uvedenou funkci (přesněji zobrazení) lze definovat pomocí různých typů konečných grup, avšak my se ve výkladu omezíme na číselné grupy s operací násobení. Tato operace nám dovoluje definovat mocnění, kdy například $V \cdot V \cdot V = V^3$, přičemž výchozí V i výsledné V^3 jsou čísla dané grupy. Abychom nemuseli vysvětlovat modulární aritmetiku, tak použijeme notaci bez operace modulo, čímž bude vysvětlení vlastností funkce DHF principiálně srozumitelné i čtenářům, kteří tuto operaci neznají. Podle avizované notace je pro argument V a tajný parametr a výstupní hodnotou Diffie-Hellmanovy funkce hodnota

$$A = \mathrm{DHF}(V, a) = V^a.$$

Uvedenou funkci lze interpretovat (viz [2]) jako specifickou symetrickou šifru, kde vstupní zprávou je číslo V, tajným klíčem je hodnota a a výstupem je kryptogram A. Diffie-Hellmanova funkce, jako každá šifra, se vyznačuje tou vlastností, že neoprávněná osoba není schopna ze znalosti vstupní hodnoty V a výstupního kryptogramu A zjistit hodnotu tajného klíče a. Oproti běžným šifrám má však Diffie-Hellmanova funkce jednu velmi zajímavou vlastnost. K její ilustraci si zvolme další tajný klíč b a jemu příslušející kryptogram

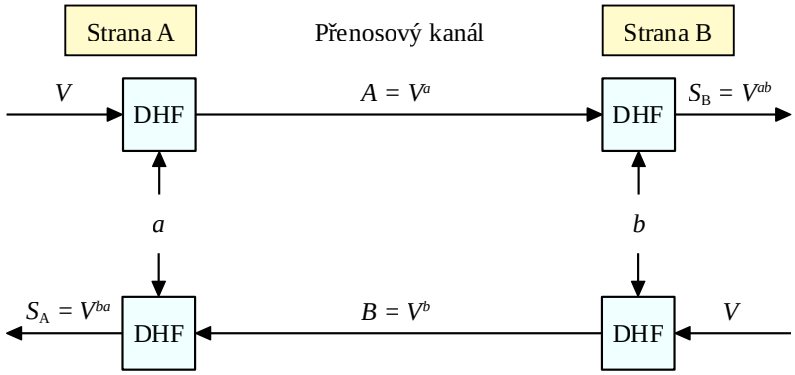
$$B = \mathrm{DHF}(V, b) = V^b.$$

Ze všeobecně známých vlastností mocnin pak pro Diffie-Hellmanovu funkci vyplývá, že

$$\mathrm{DHF}(B, a) = B^a = (V^b)^a = V^{b \cdot a} = (V^a)^b = A^b = \mathrm{DHF}(A, b).$$

Ze získané rovnosti vidíme, že pokud kryptogram B zašifrujeme tajným klíčem a (viz levá strana předchozí rovnice), tak vznikne zcela stejný výsledek, jako když kryptogram A zašifrujeme tajným klíčem b (pravá strana rovnice). Jinými slovy můžeme říci, že pokud vstup V zašifrujeme klíčem b, tak získáme kryptogram B, který když poté zašifrujeme klíčem a, tak získáme tentýž výsledek, jako když vstup V nejprve zašifrujeme klíčem a (výsledkem je kryptogram A) a poté klíčem b. Uvedenou vlastnost lze obecně formulovat tak, že výsledek série několika po sobě jdoucích šifrování různými klíči nezávisí na pořadí použitých klíčů, ale závisí jen na jejich součinu.

Nyní si můžeme popsat samotný DH protokol. Jeho účastníky jsou strany A a B (viz obr. 1.7).



Obrázek 1.7: Schéma Diffie-Hellmanova protokolu

Strana A si vygeneruje tajný klíč a a vypočítá $A = \mathrm{DHF}(V, a)$. Strana B si vygeneruje svůj klíč b a vypočítá $B = \mathrm{DHF}(V, b)$. Kryptogramy A a B si obě strany prostřednictvím veřejného kanálu vymění. Strana A z přijatého kryptogramu vypočítá hodnotu $S_A = \mathrm{DHF}(B, a)$ a strana B vypočítá $S_B = \mathrm{DHF}(A, b)$. Z rovnice u předchozího odstavce vyplývá, že $\mathrm{DHF}(B, a) = \mathrm{DHF}(A, b)$, tj. platí, že $S_A = S_B = S = \mathrm{DHF}(V, a \cdot b)$.

Diffie-Hellmanův protokol umožňuje stranám A a B sestrojit pomocí veřejného kanálu (tj. kanálu, který může být pod kontrolou neoprávněných osob) sdílenou tajnou hodnotu S (tzv. semeno – "seed"). Z této hodnoty pak lze pomocí funkce ODF (viz dále) odvodit tajné klíče pro symetrické kryptosystémy a těmito kryptosystémy další komunikaci mezi A a B ve veřejném kanálu chránit. Bezpečnost protokolu spočívá v tom, že neoprávněné osoby sice mohou v kanále zachytit oba kryptogramy A a B, avšak k sestrojení semena S_A, resp. S_B potřebují zjistit tajný klíč a, resp. b. Již jsme si však uvedli, že funkce DHF je konstruována tak, aby to ze známých hodnot V, A a B nebylo prakticky možné.

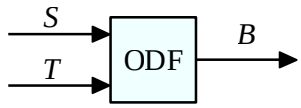
Poznamenáváme, že v Diffie-Hellmanově protokolu se klíče a a b, resp. kryptogramy A a B často nazývají soukromé, resp. veřejné klíče. To je však matoucí označení, neboť hodnoty A i B v tomto případě roli klíče neplní. Klíč má v kryptografických funkcích význam parametru, tj. údaje, který z rodiny všech možných přiřazení (např. rodiny všech možných šifrovacích přiřazení) určuje právě jedno konkrétní přiřazení (např. právě jedno konkrétní přiřazení výstupních kryptogramů vstupním zprávám). Pokud se však na obr. 1.7 podíváme například na funkci DHF vpravo nahoře, tak vidíme, že podle zmiňované terminologie má tato funkce celkem dva parametry (klíče A a b), ale žádný argument. To je logický nesmysl, a proto budeme používat jinou terminologii.

Navržená terminologie vychází z toho, že funkce DHF je v pravém slova smyslu zobrazením na grupě. Prvky této grupy mohou být buď čísla (tuto variantu jsme si popisovali), nebo body eliptické

křivky, a tak vstupní prvek V budeme obecně nazývat DH vzor a výstupní prvky A, resp. B budeme nazývat DH obraz strany A, resp. B. Semeno S je pak DH obrazem vzoru V vytvořeným společně oběma stranami a čísla a a b jsou tajné klíče jednotlivých stran. U některých popisů budeme používat konvenci, kdy strana X má tajný klíč K_X a pro obvykle veřejně známý DH vzor V má tato strana svůj DH obraz $Q_X = \mathrm{DHF}(V, K_X)$.

1.6 Odvozovací funkce

Odvozovací funkce ODF (obr. 1.8) primárně slouží k odvozování hodnot klíčů symetrických kryptosystémů na základě tajné hodnoty semena S a tzv. kontextu T. Kontextem se přitom rozumí neutajované (tj. veřejně známé) hodnoty, které mohou mít charakter konstant ale i variabilních hodnot. Kontexty slouží k individualizaci odvozovací funkce (např. podle účelu odvozeného klíče, či podle jejích uživatelů). Z důvodů vyšší bezpečnosti nebo z důvodu odvození různých druhů klíčů se odvozovací funkce mohou používat vícenásobně, takže výstupem odvozovací funkce může být i hodnota nového semene.



Obrázek 1.8: Odvozovací funkce

Obvyklé použití odvozovací funkce ODF je následující. Obě komunikující strany A a B si nejprve jednorázově sjednají společné semeno S. K tomu se nejčastěji využívá technika Diffie-Hellmanova protokolu, ale lze použít i techniku fyzického transportu semena v bezpečném paměťovém úložišti pomocí kurýra, nebo techniku přenosu semena šifrovacím kryptosystémem. V případě potřeby nového klíče (např. před navázáním komunikace, nebo po uplynutí určené doby používání klíče) obě strany vygenerují svá náhodná čísla N_A, resp. N_B a tato čísla si prostřednictvím veřejného kanálu navzájem vymění. Z obou čísel každá strana sestrojí společný kontext T (např. $T = N_A \parallel N_B$) a pomocí funkce ODF pak vygenerují stejný pseudonáhodný číselný blok B potřebné délky. Formálně pak

$$B = \mathrm{ODF}(S, T).$$

Získaný blok B obě strany podle stanovených pravidel rozdělí na klíče pro jednotlivé symetrické kryptosystémy. Obvykle jedná o šifrovací klíč KE_{AB} pro směr komunikace z A do B, klíč KE_{BA} pro šifrování ve směru z B do A, pečetící klíč KP_{AB} pro provoz z A do B a klíč KP_{BA} pro pečetění v opačném směru. Potom můžeme psát, že

$$\mathrm{ODF}(S, T) = B = KE_{AB} \parallel KE_{BA} \parallel KP_{AB} \parallel KP_{BA}.$$

Abychom si však popisy kryptosystémů co nejvíce zjednodušili, tak v dalším výkladu klíče podle směru komunikace rozlišovat nebudeme.

Výhodou funkce ODF je skutečnost, že při dlouhodobé platnosti semene S lze hodnoty klíčů pro symetrické kryptosystémy často a operativně měnit. Tímto způsobem se podstatně zvyšuje bezpečnost komunikace. Přirozeným požadavkem na odvozovací funkci je praktická nemožnost odvodit tajné semeno S na základě znalosti kontextu T a výstupního bloku B.

Z hlediska terminologie poznamenáváme, že především ve starších pramenech se semeno S nazývá klíč. Pro oba tyto pojmy je společné, že jsou tajné. Rozdílem však je, že semeno je argumentem funkce, kdežto klíč je parametrem funkce. Za poznámku rovněž stojí, že funkce ODF z hlediska svého účelu připomíná generátor pseudonáhodné posloupnosti. Semeno zde určuje počáteční stav generátoru a kontext hraje roli parametru, jímž se individualizuje fungování generátoru. Rozdílem je, že funkce ODF slouží ke generování pseudonáhodné posloupnosti pro blok klíčů i ze semena, které nemusí být ideálně náhodné (typicky DH obraz), avšak na druhou stranu ji nelze použít ke generování velmi dlouhých posloupností (např. pro proudovou šifru).

1.7 Kryptografické proměnné

S kryptografickými proměnnými jsme se již setkali a zde si je utřídíme. Kryptografické proměnné jsou číselné posloupnosti, jejichž variabilita zajišťuje vyšší úroveň bezpečnosti kryptosystémů (například cestou časté změny hodnot tajných klíčů) a zároveň také zajišťuje unikátnost kryptografických systémů různých uživatelů (například každý uživatel může mít svůj unikátní soukromý klíč).

Kryptografické proměnné lze podle požadavku na jejich utajení klasifikovat následovně.

- Utajované proměnné:
  - tajné klíče symetrických kryptosystémů,
  - soukromé klíče asymetrických kryptosystémů,
  - semena.
- Veřejné proměnné:
  - veřejné klíče asymetrických kryptosystémů,
  - unikáty.

Kryptografické funkce přiřazují každému argumentu (tj. každé hodnotě z množiny vstupních hodnot) právě jednu výstupní hodnotu. Konkrétní přiřazení je definováno pomocí klíče. Klíče tak jsou parametry, které z množiny všech možných přiřazení (z tzv. rodiny funkcí) definují jedno konkrétní přiřazení (funkci). Dalším typem proměnné je semeno, což je tajná hodnota, která je argumentem kryptografické funkce (např. ODF), případně počátečním stavem pseudonáhodného generátoru. Poslední kryptografickou proměnnou je unikát, což je veřejně známý argument,

kterým se individualizuje vykonání (a tedy i výstup) kryptografické funkce. Unikátem může být náhodné číslo, aktuální čas, nebo pořadové číslo.

1.8 Ustavení klíčů

Bezpečnost naprosté většiny moderních kryptosystémů je budována na pesimistickém předpokladu, že útočník ví o daném kryptosystému úplně vše, kromě tajného, resp. soukromého klíče. Ustavení klíčů (tj. bezpečné získání klíčů komunikujícími stranami) je proto kritickým problémem každého kryptosystému.

U symetrických kryptosystémů jsme si uvedli, že obě strany disponují tajným klíčem K. Tento klíč je možné ustavit více způsoby. První možností je transport klíče kurýrem, druhou možností je šifrovaný transport klíče veřejným kanálem a třetí možností je sestrojení klíče Diffie-Hellmanovým protokolem. Technika transportu kurýrem je založena na fyzické přepravě speciálního paměťového úložiště („key loader"). Klíč K se jednoduše do tohoto transportního úložiště zapíše a spolehlivý kurýr doručí úložiště komunikující straně X. Tato strana se vůči úložišti stanoveným způsobem autentizuje (např. heslem), a to následně dovolí přečtení klíče ze své paměti.

Druhou možností je šifrovaný transport klíče K pomocí veřejného kanálu, a to buď symetrickým, nebo asymetrickým kryptosystémem. V případě symetrického kryptosystému mají obě strany sjednán tzv. transportní klíč KT, který je vyhrazen pouze pro transport klíčů. Tento klíč má dlouhodobou platnost a je obvykle doručen kurýrem. Postup je takový, že například strana A vygeneruje hodnotu klíče K pomocí generátoru náhodných čísel (tj. $K = \mathrm{GEN}$), tento klíč zašifruje transportním klíčem do podoby kryptogramu $C = \mathrm{ENC}(K, KT)$ a kryptogram veřejným kanálem předá protistraně B. Ta kryptogram dešifruje a získá tak klíč $K = \mathrm{DEC}(C, KT)$. Ten pak obě strany používají k šifrovanému přenosu zpráv.

V případě asymetrického kryptosystému je postup obdobný. Například opět strana A vygeneruje klíč K pomocí generátoru náhodných čísel (tj. $K = \mathrm{GEN}$). Tento klíč však nyní zašifruje veřejným klíčem protistrany B (tj. klíčem VK_B) do podoby kryptogramu $C = \mathrm{ENC}(K, VK_B)$ a kryptogram C veřejným kanálem předá straně B. Ta kryptogram dešifruje svým soukromým klíčem SK_B, čímž získá klíč $K = \mathrm{DEC}(C, SK_B)$. Klíč K pak obě strany opět používají k šifrovanému přenosu zpráv.

Třetí možností je sestrojení klíče pomocí Diffie-Hellmanova protokolu. Pomocí tohoto protokolu (viz podkapitola 1.5) si obě strany sjednají tajné semeno S, navzájem předají své unikáty a z těchto hodnot následně pomocí odvozovací funkce ODF (viz podkapitola 1.6) odvodí klíč K.

V případě ustavení klíčů u asymetrických kryptosystémů je zapotřebí rozlišovat mezi soukromým a veřejným klíčem. U soukromého klíče žádný problém s jeho ustavením není. Pokud si například strana B vygeneruje dvojici soukromý klíč SK_B a veřejný klíč VK_B, tak svůj soukromý klíč nikomu nemusí poskytovat – klíč SK_B bezpečně uloží na vhodné paměťové úložiště a používá jej podle

potřeby. V případě veřejného klíče se ohledně jeho ustavení zdánlivě o žádný problém rovněž nejedná. Klíč VK_B je přece veřejný, a tak jej lze přenášet veřejným kanálem. Vzniká se tu však problém autentičnosti klíče. Pokud je například straně A doručena zpráva Z, v níž se uvádí, že strana B má veřejný klíč VK_B, tak sice může jít o pravdivou zprávu, ale stejně tak může jít o zprávu podvodnou. Podvod spočívá v tom, že si útočník U vygeneruje svoji dvojici soukromý klíč SK_U a veřejný klíč VK_U, přičemž straně A zašle klíč VK_U s tvrzením, že se jedná o veřejný klíč strany B. Strana A pak tímto klíčem bude šifrovat zprávy, resp. ověřovat podpisy a přitom si bude myslet, že bezpečně komunikuje se stranou B. Ve skutečnosti však bude komunikovat s útočníkem U. K eliminaci popsaného podvodu vznikly tzv. certifikační autority.

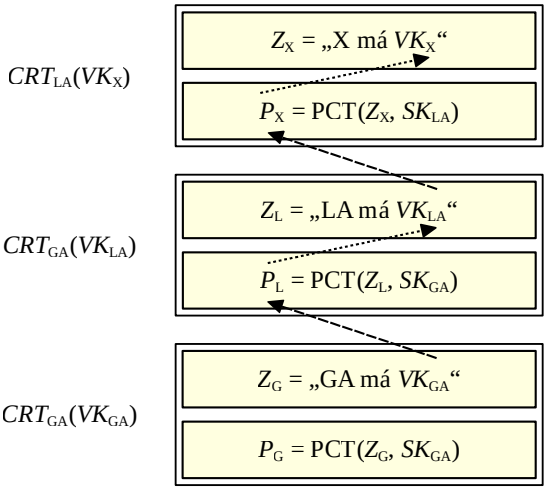
Certifikační autorita CA je důvěryhodná strana, která vydává tzv. certifikáty. Zájemce o certifikát nejprve certifikační autoritě prokáže svoji identitu X a vlastnictví veřejného klíče VK_X. Ta mu pak vydá certifikát, což je prakticky autoritou podepsaná zpráva Z_X = „Strana X má klíč VK_X“. Certifikát strany X vydaný certifikační autoritou CA je tedy dvojice (Z_X, P_X), kde podpis $P_X = \mathrm{PCT}(Z_X, SK_{CA})$ a SK_{CA} je soukromý podepisovací klíč CA. Uvedený certifikát budeme zkráceně zapisovat jako $CRT_{CA}(VK_X)$.

Veřejný klíč VK_{CA}, který stranám slouží k ověřování certifikátů certifikační autority CA, je obvykle distribuován ve formě tzv. kořenového certifikátu $CRT_{CA}(VK_{CA})$, což je certifikát, který autorita podepsala sama sobě. Platí tady, že $CRT_{CA}(VK_{CA}) = (Z_{CA}, P_{CA})$, přičemž zpráva Z_{CA} = „CA má klíč VK_{CA}“ a podpis $P_{CA} = \mathrm{PCT}(Z_{CA}, SK_{CA})$. Ostatní strany tento kořenový certifikát získají bezpečným způsobem (např. osobní návštěvou certifikační autority). Pokud pak strana Y disponuje takovýmto kořenovým certifikátem a strana X ji zašle svůj certifikát $CRT_{CA}(VK_X)$, tak si strana Y může klíčem VK_{CA} z kořenového certifikátu ověřit, že podle certifikační autority protistrana X skutečně existuje a že disponuje veřejným klíčem VK_X. Jednorázovým bezpečným získáním jediného klíče (klíče VK_{CA}) nyní může každá strana bezpečně ustavit veřejný klíč s například všemi desetitisíci stranami, jimž certifikační autorita certifikát vydala.

Aby jednotlivé strany nemusely ve svém paměťovém úložišti uchovávat velký počet kořenových certifikátů, tak byla do světa certifikačních autorit zavedena hierarchie. Tuto hierarchii si budeme ilustrovat na jednoduché dvoustupňové hierarchii, v níž budeme rozeznávat hierarchicky vyšší autority (nazveme je globální – GA) a hierarchicky nižší (tzv. lokální – LA) autority. V popsaném uspořádání pak platí, že lokální autority podepisují certifikáty pro komunikující strany a globální autority podepisují certifikáty pro lokální autority. Na obrázku 1.9 máme příklad dvoustupňové hierarchie, v němž globální autorita GA (např. DigiCert) vydala lokální autoritě LA (např. certifikační autoritě banky B) certifikát $CRT_{GA}(VK_{LA})$. Lokální autorita LA přitom vydává certifikáty zařízením své banky, přičemž konkrétně serveru X vydala certifikát $CRT_{LA}(VK_X)$. Jak dále uvidíme, tak potom každé straně Y, která chce bezpečně komunikovat se zařízeními banky B, nyní postačí mít pouze kořenový certifikát $CRT_{GA}(VK_{GA})$ globální certifikační autority a nepotřebuje bezpečně získat kořenový certifikát lokální certifikační autority.

Při zahájení komunikace server X protistraně Y zašle certifikáty $CRT_{GA}(VK_{LA})$ a $CRT_{LA}(VK_X)$. Jejich napojením na kořenový certifikát $CRT_{GA}(VK_{GA})$ vznikne pro stranu Y souvislý řetězec

certifikátů. Strana Y si nejprve z kořenového certifikátu ověří správnost klíče VK_{GA}. S jeho pomocí si pak ověří podpis P_L z $CRT_{GA}(VK_{LA})$ (čárkovaná šipka od VK_{GA} k P_L). A protože strana Y důvěřuje GA, tak potom věří i jí podepsané zprávě, že „LA má VK_{LA}“ (tečkovaná šipka k VK_{LA}). Pomocí tohoto VK_{LA} ověří podpis P_X z $CRT_{LA}(VK_X)$ (čárkovaná šipka od VK_{LA} k P_X). A pokud se strana Y rozhodne důvěřovat i LA, tak bude věřit jí podepsané zprávě, že „X má VK_X“ (tečkovaná šipka k VK_X). Tímto způsobem si libovolná strana Y může relativně bezpečně ověřit, že server X skutečně existuje a že disponuje klíčem VK_X. Řetězce certifikátů mohou v praxi sestávat i z většího počtu certifikátů (vícestupňová hierarchie). Výhodou techniky řetězení je, že s několika bezpečně získanými kořenovými certifikáty, lze ustavit veřejné klíče prakticky s jakýmkoliv dalším zařízením na této planetě.



Obrázek 1.9: Řetězec certifikátů