3. BLOK

Úvod do kryptografie

V kryptografii se obvykle pro popis komunikace označují komunikující strany jako ***A*** (Alice) a ***B*** (Bob) a také se musejí samozřejmě zvažovat "ti zlí" - obvykle se jako hrozba zmiňuje odposlech (angl. *eavesdropping*) – ***E*** (Eva).

3.1 Šifra, algoritmus, klíč

Kryptografie slouží k zajištění podpory mnohých aspektů bezpečnosti, nejčastěji je zmiňována *důvěrnost* a *integrita*, ale nelze nezmínit i *dostupnost* a *zodpovědnost.* Zatím zůstaňme u důvěrnosti. Přáním Alice většinou je, aby její data nemohl prohlížet nikdo jiný (ať už na počítači nebo při přenosu) - pokud mu k tomu Alice nedá výslovné svolení. Ale sama Alice aby mohla podle potřeby zase změnit podobu nazpět. Po dlouhou dobu jako Alice vystupovali hlavně diplomaté, vojáci, obchodníci a milenci.

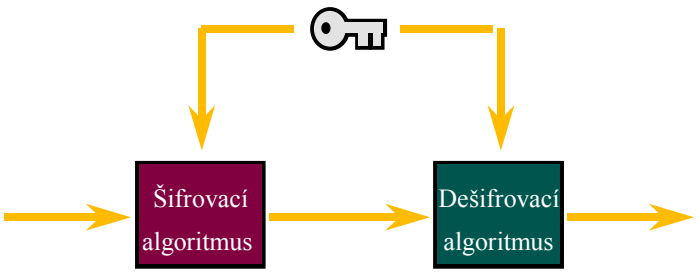
Známá je jednoduchá šifra Julia Cesara - každé písmeno textu bylo nahrazeno jiným písmenem abecedy – “posunutým” o 3 pozice. Místo “A” to bylo “D”, místo “E” pak “H” atd. Je ale jasné, že takovýto postup není příliš spolehlivý - některá písmena se v textu vyskytují častěji než jiná a tak není velkým problémem vyhodnotit relativní výskyt písmen v zašifrovaném textu, srovnat s průměrnými hodnotami pro písmena daného jazyka (latina má jiné charakteristiky než čeština), vše pak doladit metodou pokusů a omylů, nejlépe za použití počítače.

V obdobném druhu šifer jsou patrné dvě věci: každé písmeno se nahradí jiným, způsob náhrady je určen nějakým číslem (u Césarovy šifry trojkou) a také všeobecným povědomím o písmenech v abecedě a jejich řazení.

Šifrovacím algoritmem je náhrada písmen a parametr 3 je *šifrovacím klíčem*. *Šifrováním* tedy rozumíme převod *nešifrovaných* (otevřených) dat na data *šifrovaná* pomocí šifrovacího systému, který se skládá z šifrovacího algoritmu a šifrovacího klíče.

A pokud se nám jedná do převod zpět do čitelné podoby, pak mluvíme o *dešifrování*.

Zjednodušený model konvenčního šifrování



Převzato z: *Network and Internetwork Security* (Stallings)

Kryptografií pak označujeme vědu (nebo snad umění ?) zabývající se tvorbou šifrovacích a dešifrovacích algoritmů. Takže pak mluvíme o kryptografických algoritmech, klíčích, zařízeních atd. A *kryptanalýzou* se rozumí obor, který se snaží šifry překonávat a hledat jejich slabiny. Obor označovaný jako *kryptologie* pak spojuje tyto dva sourozence – siamská dvojčata.

V kryptologii se používá nejen operací šifrování a dešifrování jako operací reverzibilních, ale také např. hašování - "srážení" rozsáhlých dat na malý, leč reprezentativní řetězec. Tento řetězec (hašovací hodnota čili haš) má zásadní význam třeba u digitálního podpisu a problematika hašování má v oboru kryptologie velmi privilegované postavení.

Kryptografie i celá počítačová bezpečnost jsou záležitosti stavění překážek a hledání děr. *Základní pravidlo kryptografie je, že ochrana spočívá v tajném klíči, ne v tajném algoritmu.* Bezpečnost algoritmu je jeho schopnost odolat úsilí protivníka získat přístup k nezašifrovanému textu či spíše k šifrovacímu klíči. Absolutně bezpečný algoritmus by měl garantovat, že ze zachyceného zašifrovaného textu nelze bez klíče získat nezašifrovaný text. Jediným známým algoritmem s touto vlastností je *Vernamova šifra*, kde je nezašifrovaný text kombinován operací XOR s náhodnou neopakující se posloupností dat stejné délky a dešifrování se provede opakováním operace XOR na zašifrovaná data a onu posloupnost. Nevýhoda je zřejmá - délka klíče je stejná jako délka šifrovaného textu. Z tohoto důvodu se této metody používá jen výjimečně (i když dnes kapacity CD-ROM a jiných médií lze pro absolutně bezpečné šifrování vhodně využít).

Dobrý algoritmus je terčem analýz a “útoků” ze všech stran roky (2-3 se pokládají za minimum), kdy se ho pokouší desítky spičkových odborníků nějak pokořit. *Neveřejný algoritmus je nedůvěryhodný algoritmus*. Pro Alici nemá velký smysl chránit klíč od málo robustních dveří – Eva může třeba jen jednoduše vyšroubovat panty. Většinu uživatelů zajímá hlavně použitelnost algoritmů a ve věci konstrukce algoritmů se spoléhají na odborníky v kryptologii a bezpečnosti. Každým rokem se konají desítky kryptologických konferencí, z nich nejvýznamnější jsou americké Crypto spolu s Eurocryptem a Asiacryptem/Auscryptem. Existuje také Mezinárodní asociace pro kryptologický výzkum (IACR - *www.iacr.org*), která výše uvedené konference (spolu)pořádá. Odpověď na otázku “který algoritmus je nejlepší” neexistuje, lze se ale pokusit ve sbornících najít, které algoritmy mají nějaké slabiny, jak algoritmy vhodně používat nebo pro co je naopak raději vůbec nepoužívat. Vždy se vyplatí hledat pravdu na všech stranách a zjistit si o algoritmech i jejich aplikacích co nejvíce detailů od co nejvíce lidí.

Neformální pravidlo by se asi dalo formulovat takto - *pokud nejsou všechny zásadní detaily o algoritmu známy alespoň dva roky a nejsou o něm publikovány alespoň dva tucty nezávislých analýz a přednášek na konferencích IACR, tak nemá smysl o nasazení algoritmu vůbec uvažovat*. Přinejmenším ne v prostředí, kdy nemáte skutečně spolehlivou ochranu přístupu k vaši počítačům nebo kdy posíláte data po veřejných linkách.

3.1.1 Symetrické a asymetrické algoritmy

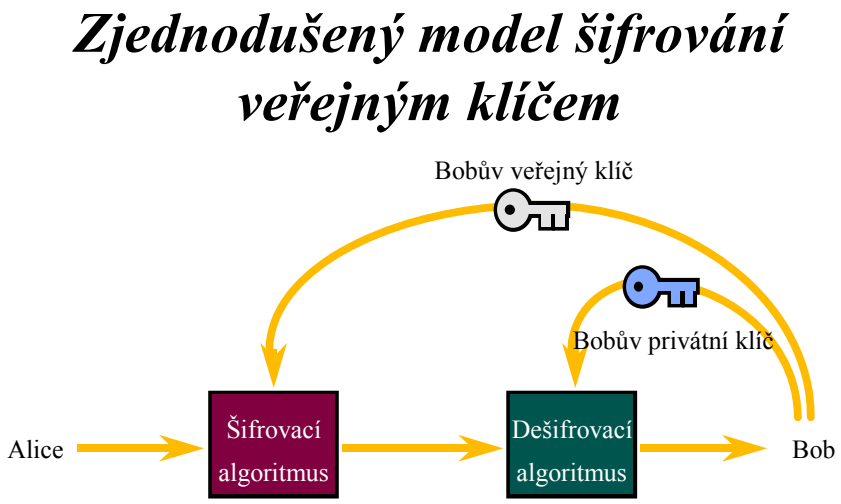
Kryptografické algoritmy se v zásadě dělí na dvě velké skupiny:

- **symetrické** algoritmy, kde se pro zašifrování i dešifrování používá stejný kryptografický klíč;

- **asymetrické** algoritmy, které používají odlišný klíč pro zašifrování (veřejný klíč) i pro dešifrování (soukromý klíč).

Obě skupiny lze dále členit podle způsobu transformace dat a jiných detailů - např. šifry proudové (zpracováván bit po bitu) či blokové (data zpracovávána v blocích). Význam rozdělení algoritmů na dvě prvně uvedené skupiny není v rozdělení algoritmů na dvě různé třídy bezpečnosti, ale v problémech ohledně správy klíčů a obecně i výkonu. Lze totiž – zjednodušeně – říct, že symetrické algoritmy jsou rychlejší. Zato si musíte s každým, s kým chcete komunikovat při využití šifrování, domluvit kryptografický klíč a obě strany jej musí pečlivě opatrovat. Asymetrické algoritmy jsou na tom sice s výkonem hůře, zato ale stačí spolehlivě zveřejnit svůj veřejný klíč a chránit si jen svůj soukromý klíč. Ono spolehlivé zveřejnění veřejného klíče a jeho případné zrušení v případě porušení nebo krádeže soukromého klíče je velice problematická záležitost. U rozsáhlých skupin komunikujících účastníků někdy může být celkově výhodnější jednodušší způsob šifrování symetrickou cestou. Nejčastějším praktickým řešením bývá tzv. *hybridní systém*, kde jsou prostředky asymetrických algoritmů použity k

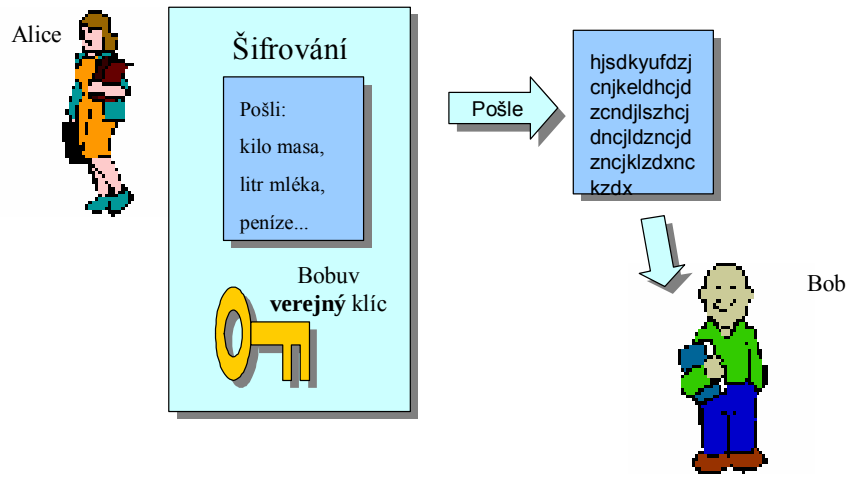
autentizaci a ustavení společného klíče pro následné symetrické šifrování - tento systém je uplatněn např. v SSL (viz níže).



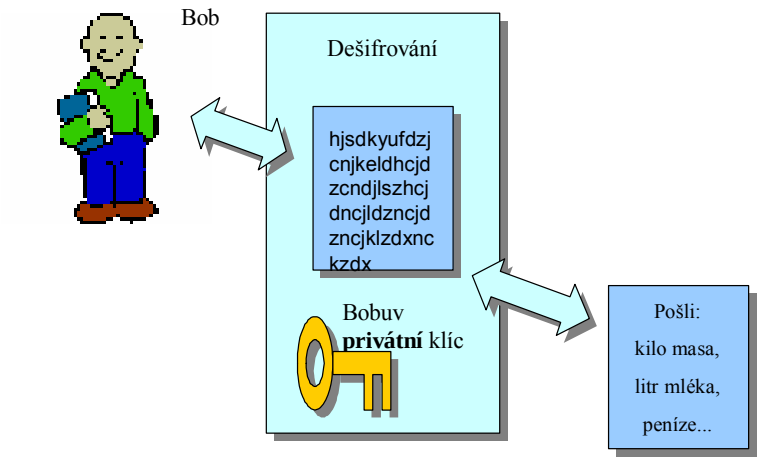
Převzato z: *Network and Internetwork Security* (Stallings)

Ale zpět ke klíčům - velmi jednoduchým příkladem na vysvětlenou mohou být klasické visací zámky. Pro symetrickou kryptografii si můžeme celou situaci představit tak, že každá z komunikujících stran A, B, C a D musí obvykle mít k dispozici zámky i klíče všech ostatních stran. Pokud chtějí tajně komunikovat všechny tyto strany společně, pak jim stačí po jedné kopii zámku a klíče. Pak ale nemá A žádnou jistotu, zda zprávu obdržela od C nebo od D. Takže obvykle má každá ze stran různé klíče ke komunikaci s různými partnery. Pokud chce Alice poslat tajnou zprávu Bobovi, pak musí vzít klíč se zámkem A-B, zprávu tímto klíčem zašifrovat a poslat Bobovi. Ten musí mít klíč k zámku A-B a zprávu odemknout – dešifrovat.

Šifrování verejným klícem



Dešifrování zprávy od Alice



V případě využití asymetrické kryptografie každá strana opatruje jen svůj soukromý klíč a kdokoliv může použít všeobecně přístupné prostředky (v našem případě připravené zámky) pro zašifrování zprávy. Je ovšem důležité mít na vývěsce prostředky správně označené, neumožnit jiným stranám změny prostředků atd. (Eva nesmí nahradit věci označené “A” svými vlastními, ani je změnit, poškodit atd.) Tady přicházejí ke slovu věci jako certifikáty

kryptografických klíčů, o kterých se dozvíme dále v tomto kurzu a ke kterým se vztahuje i podstatná část Zákona č. 227/2000 Sb. o elektronickém podpisu.

3.1.2 Délka klíče

Častým ukazatelem úrovně ochrany – i když někdy velice zavádějícím – je délka použitého kryptografického klíče. Pokud vezmeme jeden konkrétní a kvalitní algoritmus, tak platí, že čím delší je použitý klíč pro šifrování, tím lepší je úroveň ochrany. Pro případného útočníka, který nemá k dispozici dešifrovací klíč, totiž vede cesta k překonání šifry přes vyzkoušení všech možných hodnot klíče, případně hledání slabin algoritmu. Pokud útočník zná vyloženou "díru" v algoritmu, pak vám nepomůže ani milionbitový klíč... A nevadí, že zbytek světa o díře neví nebo že dokonce neví jaký algoritmus jste použili. Pokud je ale algoritmus skutečně dobrý, pak delší klíč znamená pro útočníka zdržení ze dvou důvodů:

- jednak musí vyzkoušet víc možných hodnot klíče (jednobitový klíč může nabývat dvou hodnot – 0 a 1, dvoubitový čtyř – 00, 01, 10 a 11 ... a co třeba stobitový?);

- pro algoritmy s variabilní délkou klíče také delší klíč znamená delší dobu potřebnou pro provedení výpočtu.

Uvádění bezpečnosti jen délkou klíče bez uvedení algoritmu je velice ošemetné, některé hranice ale lze zhruba načrtnout. Pro symetrické blokové šifry (DES, IDEA, RC4 atd.) se dnes má za to, že oblast 60 bitů je běžně překonatelná během několika hodin vládními superpočítači asi pro 15-20 zemí světa. A s Internetem lze dnes také provádět výpočty distribuované na stovkách i tisících strojů, takže tato hranice je překonatelná i pro odhodlaný tým "nevládních" odborníků. Ovšem cena za vyluštění jedné takové zprávy, jako byla ta v *DES Challenge* je značná, čili se není potřeba obávat, že by třeba DES nebyl "dost dobrý" pro běžnou potřebu jednotlivce nebo malé firmy. Dnes již ovšem máme k dispozici nový standard pro symetrickou blokovou šifru – AES (viz níže). U dobrých symetrických blokových šifer se má za to, že hranice 100 bitů je pro klíč dostatečnou zárukou bezpečnosti nejméně pro 3-4 další roky. Zde je taky vhodné poznamenat, že alternativa trojitý-DES nabízí ochranu ekvivalentní asi 112 bitům.

Pro asymetrické algoritmy je situace značně komplikovanější. Asi nejznámějším algoritmem je RSA (nazvaný dle svých otců – Rivesta, Shamira a Adlemana), u kterého je dnes překonatelná hranice okolo 512 bitů. Většinou se tedy pro RSA doporučují klíče buď s délkou 1024 nebo raději 2048 bitů. Pro algoritmy nad eliptickými křivkami se dnes uvádí, že cca 170 bitový klíč dává stejnou bezpečnost jako u RSA s klíčem okolo 1000 bitů, resp. klíč sym. alg. 80 bitů.

3.1.3 Advanced Encryption Standard

2. října 2000 se celý kryptografický svět od amerického NIST (National Institute of Standards and Technology) dozvěděl, že z pětice finalistů při výběru kryptografického algoritmu pro nový americký standard AES (Advanced Encryption Standard), následovníka DES, byl vybrán algoritmus Rijndael. Autory tohoto algoritmu jsou Vincent Rijmen a Joan Daemen. Rijndael sice nepatřil mezi nejlepší z hlediska odhadu bezpečnosti (společně s dalším finalistou RC6 byla bezpečnost hodnocena jako „adekvátní“ a nikoliv „vysoká“ jako u dalších tří finalistů), ale jeho hodnocení z jiných hledisek jej činilo ideální volbou dle mnoha expertů. Důležité je také rozhodnutí NIST nezavádět druhý, tzv. záložní algoritmus, což byla varianta zvažovaná jak kvůli možnosti rychle nasadit jiný algoritmus v případě nenadálého selhání primárního algoritmu, tak údajně i z jiných důvodů (např. že žádný z amerických návrhů v soutěži neuspěl). Důvodovou zprávu k výběru algoritmu a další podrobné informace najdete na *http://www.nist.gov/aes*.

3.2 Kryptografie jako zbraň

Masové rozšíření Internetu a potřeba řídit bezpečné elektronické obchodování s sebou přinesly potřebu větší dostupnosti kryptologie. Dodnes je ale s exportem šifrovacích produktů mnohde zacházeno jako s exportem zbraní: "silná" kryptografie často představuje významnou zbraň - schopnost dešifrovat komunikaci může rozhodnout výsledek konfliktu. Vládní zájmy se zde soustřeďují do dvou oblastí:

- mít jistotu, že používání kryptografických systémů nesníží schopnost dopadnout nežádoucí osoby a skupiny osob;

- zajistit, aby používání kryptografických systémů nepůsobilo proti národním zájmům dané země.

Export šifrovacích produktů je v mnoha zemích hodnocen vládními úřady stejně jako export zbraní. Je pravda, že silná kryptografie představuje významnou "zbraň" - schopnost utajit (zašifrovat) nebo naopak dešifrovat komunikaci může rozhodnout výsledek konfliktu. Uvádí se, že např. vládě USA se takto daří v oblasti kryptografických a hlavně kryptanalytických objevů udržovat náskok přibližně 10-15 let před civilním světem (a dalšími zeměmi). Americká NSA (National Security Agency), která má dvě zásadní poslání (srovnejte s principy uvedenými v úvodu článku): Získávat vládě USA přístup k informacím komunikovaným mimo území USA a také pomáhat v tom, aby nebylo možno získat přístup k informacím vlády USA. NSA je snad nejméně známou, ale velmi důležitou tajnou službou USA. NSA disponuje nejvýkonnějšími počítači, jaké jsou na povrchu této planety nasazeny a toto platí po celou dobu její existence. Má analytické pracovníky snad všude, kde jen lze získávat nějaké informace důležité pro USA. Prvním Američanem zabitým ve válce ve Vietnamu byl právě pracovník NSA. Pro ilustraci o práci NSA stojí za přečtení rozhovor s jejím bývalým

pracovníkem Perry Fellwockem na <*jya.com/nsa-elint.htm*>, nebo bezpečnostní manuál pro pracovníky NSA na <*http://www.cl.cam.ac.uk/~rja14/Papers/nsaman.pdf* >.

4. BLOK

Autentizace uživatelů a dat, digitální podpis

4.1 Autentizace

Autentizace uživatele je obvykle prvním krokem, který každodenně provádíme na začátku naší práce s počítačem. Primárním cílem autentizace je zabránit neutorizovaným uživatelům v používání počítačového systému. Sekundárním cílem je znalost systému, který uživatel s ním vlastně pracuje – tak, aby systém mohl řídit přístup uživatele k datům a službám podle daných pravidel.

Autentizační metody v zásadě dělíme do tří, resp. čtyř skupin:

1. Na základě *výlučné znalosti (co kdo zná)* – tyto metody jsou poměrně velmi dobře známy, jedná se o použití tajných hesel, PINů, algoritmů atd.

2. Podle *vlastnictví specifických předmětů (co kdo má)* – tyto metody jsou také široce rozšířeny, jsou to např. magnetické a čipové karty, ale i běžné klíče k zámkům a speciální zařízení jako jsou tzv. autentizační kalkulátory.

3. *Biometriky (co kdo je)* – tyto metody nabízí automatizované metody verifikace nebo identifikace (rozpoznání identity člověka) na základě fyziologických charakteristik jako jsou například otisk prstu či hlas. Takové charakteristiky jsou jedinečné a měřitelné, používaly se mnoho let pro zvláště kritické kontroly (armádní a vládní systémy) a v posledních letech můžeme vidět pozorovat širší nasazení biometrické autentizace.

4. *Kombinací výše uvedených metod* – takto lze dosáhnout výrazného zvýšení spolehlivosti autentizace. Typickým příkladem je použití bankovní karty v kombinaci se znalostí PINu.

Zatímco první dvě skupiny lze použít jen k verifikaci identity, biometrické techniky můžeme použít na dvě rozdílné aplikace: na verifikaci (identity) a na identifikaci. *Verifikace* je proces, při kterém subjekt předkládá svou identitu (např. vložením karty nebo zadáním hesla) a na základě této identity se srovnávají aktuální biometrické charakteristiky s uloženými charakteristikami, které této identitě odpovídají podle záznamů autentizační databáze. Při *identifikaci* (nebo také *vyhledání*) naopak člověk identitu sám nepředkládá, systém prochází všechny (relevantní) biometrické záznamy v databázi, aby našel patřičnou shodu a identitu člověka sám rozpoznal.

4.2 Biometrické systémy

Zatímco první dvě z výše uvedených skupin jsou počítačové i širší veřejnosti poměrně dobře známy, o biometrikách zatím koluje mnoho nepřesností a proto se o nich zmíníme šířeji.

Biometrických technologií existuje mnoho a jsou založeny na *měření fyziologických vlastností* lidského těla (např. otisk prstu nebo geometrie ruky) nebo *chování člověka* (např. dynamika podpisu nebo vzorek hlasu). Některé technologie jsou teprve ve stadiu vývoje (např. analýza pachů či rozmístění žil na zápěstí), avšak mnohé technologie jsou již relativně vyzrálé a komerčně dostupné (např. otisky prstů nebo systémy porovnávající vzorek oční duhovky). Systémy založené na fyziologických vlastnostech jsou obvykle spolehlivější a přesnější než systémy založené na chování člověka, protože jsou lépe opakovatelné a nejsou ve velké míře ovlivněny daným (psychickým stavem) jako např. stres nebo nemoc.

Nejvýznamnější rozdíl mezi biometrickými a tradičními technologiemi je odpověď systému na autentizační požadavek. Biometrické systémy nedávají jednoduché odpovědi typu ano/ne. Heslo buďto je 'abcd' nebo ne, magnetická karta s číslem účtu 1234 jednoduše je nebo není platná. Podpis člověka však není vždycky naprosto stejný, stejně tak pozice prstu při snímání otisku se může trochu lišit. Biometrický systém proto nemůže určit identitu člověka absolutně, ale místo toho řekne, že s určitou pravděpodobností se jedná o daného jedince.

4.2.1 Chyby a variabilita v biometrických systémech

Mohli bychom vytvořit systém, který by vyžadoval pokaždé téměř 100% shodu biometrických charakteristik. Takový systém by však nebyl prakticky použitelný, neboť naprostá většina uživatelů by byla téměř vždy odmítnuta, protože výsledky měření by byly vždy alespoň trochu rozdílné[1]. Abychom tedy udělali systém prakticky použitelný, musíme povolit určitou variabilitu biometrických charakteristik. Současné biometrické systémy však nejsou bezchybné, a proto čím větší variabilitu povolíme, tím větší šanci dáváme podvodníkům s podobnými biometrickými charakteristikami.

Variabilita tedy určuje, jak hodně podobná musí být biometrická data, aby systém uživateli povolil přístup. Tato variabilita je obvykle nazývána jako (bezpečnostní) *prahová hodnota* nebo (bezpečnostní) *úroveň*. Je-li povolená variabilita pouze malá, pak bezpečnostní úroveň nazýváme vysokou a je-li povolená variabilita větší, pak bezpečnostní úroveň nazýváme nízkou.

Existují dva typy chyb, které biometrické systémy mohou udělat:

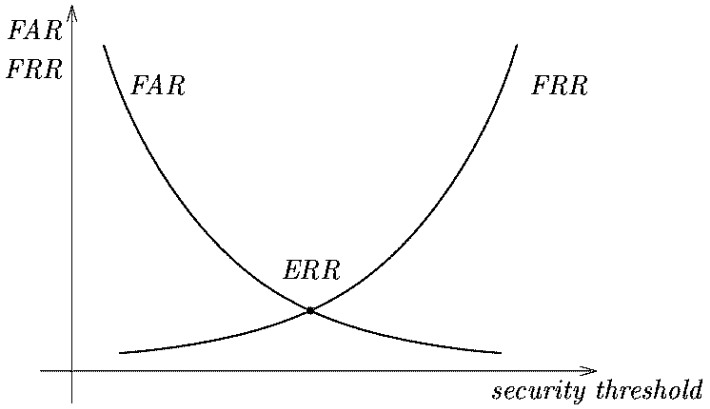
1 Stoprocentní shoda napovídá, že jsme se dostali k velmi zdařilé kopii (podvrhu).

- *nesprávné odmítnutí* (angl. false rejection) neboli chyba prvního druhu nastane, pokud je oprávněnému uživateli odmítnut přístup (protože biometrický systém nepovažuje současná biometrická data dostatečně podobná uloženému registračnímu vzorku)
- *nesprávné přijetí* (angl. false acceptance) neboli chyba druhého druhu nastane, pokud je přístup udělen neoprávněnému uživateli (protože systém považuje podvodníkova biometrická data dostatečně podobná biometrickým datům nějakého oprávněného uživatele)

V ideálním biometrickém systému by byl počet nesprávných odmítnutí i počet nesprávných přijetí nulový. V reálném systému jsou však tato čísla nenulová a závisí na nastavené bezpečnostní úrovni. Čím vyšší je tato úroveň, tím více je nesprávných odmítnutí a méně nesprávných přijetí a čím nižší je bezpečnostní úroveň, tím více je nesprávných přijetí a méně nesprávných odmítnutí. Počty nesprávných přijetí a nesprávných odmítnutí jsou tedy nepřímo úměrné.

Rozhodnutí jak vysokou bezpečnostní úroveň použít je závislé především na účelu celého biometrického systému. Správná míra tolerance musí být kompromisem mezi použitelností a bezpečností použitého systému. Biometrický systém u vchodu do zábavního parku Disney bude typicky používat nižší úroveň bezpečnosti (tj. vyšší míru tolerance) než systém u vchodu do centrály CIA.

Počet nesprávných odmítnutí a nesprávných přijetí se obvykle vyjadřuje jako procentuální podíl z celkového počtu oprávněných a neoprávněných přístupů. Tyto poměry se anglicky označují jako false rejection rate (FRR) a false acceptance rate (FAR). Čím nižší jsou tato čísla, tím přesnější je dané zařízení. Některá biometrická zařízení (nebo jejich obslužný software) vyžadují bezpečnostní úroveň jako parametr rozhodovacího procesu při požadavku autentizace. Jiná zařízení vrací skóre z nějakého intervalu a výsledné rozhodnutí je ponecháno aplikaci. Pokud zařízení podporuje několik bezpečnostních úrovní nebo vrací skóre můžeme vytvořit graf závislosti FRR a FAR na nastavené bezpečnostní úrovni. Příklad takového grafu ukazuje následující obrázek:



Křivky FAR a FRR se protínají v bodě, kde se FAR a FRR rovnají. Tato hodnota se anglicky nazývá *equal error rate* (ERR) nebo také *crossover accuracy*. Toto číslo nemá velké praktické využití (zřídkakdy chceme, aby se FAR a FRR právě rovnaly), ale je možné ho použít jako ukazatel přesnosti daného zařízení. Pokud máme dvě zařízení s ERR 1% a 10%, víme, že první zařízení je přesnější (tj. má menší chybovost). V praxi nejsou tato srovnání tak jednoduchá především proto, že není jednoduché získat srovnatelná FAR a FRR pro jednotlivá zařízení. Výrobci často uvádějí pouze nejlepší dosažitelné hodnoty (např. FAR < 0.01 % a FRR < 0.1 %). Tyto hodnoty však nejsou dosažitelné zároveň (tj. při určité bezpečnostní úrovni). Navíc jsou to hodnoty získané při testech v laboratořích a s profesionálními uživateli (často přímo s vývojáři). Hodnoty získané při nezávislých testech s neprofesionálními uživateli se od publikovaných hodnot samozřejmě podstatně liší (často i z desetin procent na desítky procent). Proto je při interpretaci jakýchkoli takovýchto hodnot obezřetnost určitě na místě.

4.3 Digitální podpis

Digitální podpis se podpisu klasickému, ručnímu, v lecčem podobá a v lecčem také liší. Podoba spočívá především v použití, jakožto prvku stvrzujícího shlédnutí podepsaného dokumentu (*autenticita* dokumentu) s tím, že toto stvrzení lze prokázat i později (*nepopiratelnost*). Liší se především ve dvou aspektech:

1. Digitální podpis je vždy závislý na podepisovaných datech – podpisy různých dokumentů jsou vždy různé, kdežto ruční podpisy jedné osoby jsou i na různých dokumentech jeden jako druhý. Tímto digitální podpis perfektně zaručuje *integritu* podepsaného dokumentu.

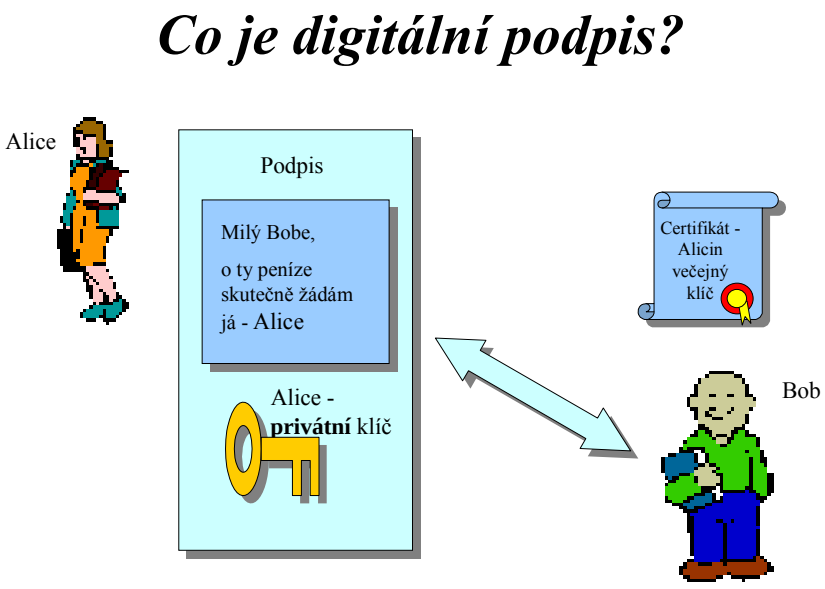
2. Ruční podpis tvoří vždy člověk (i když jej lze samozřejmě padělat), kdežto digitální podpis tvoří vždy počítač. Člověk má tedy omezenou kontrolu nad tím, co a kdy se vlastně podepisuje. Jednak nemá naprostou jistotu, že jsou podepisována data, o kterých si myslí, že jsou podepisována; také ale mohou být podpisy vytvářeny i bez vědomí uživatele (např. prostřednictvím Trojských koní).

Při podpisu digitálního dokumentu je důležitá jeho bitová reprezentace, nikoliv grafická podoba. Digitální podpis je pak také charakteristický řetězec bitů, nikoliv třeba oscanovaný ruční podpis. Pro tvorbu digitálního podpisu je potřebný jednak podepisovaný dokument, ale především jeden z páru klíčů používaných při asymetrické kryptografii. Privátní (soukromý) klíč a podepisovaná data jsou vstupními daty pro podpisový algoritmus, jehož výstupem je digitální podpis daných dat, tento podpis pak lze připojit ke zprávě.

Ve skutečnosti se ale v praxi digitální podpis vytváří následujícím způsobem (protože aplikace asymetrického algoritmu na rozsáhlé datové soubory je časově značně náročná). Takže se nejdříve vytvoří tzv. haš (kontrolní součet datového souboru), tento je vlastně přesnou reprezentací (charakteristikou) dat. Tento haš se vypočítá jednocestnou kryptografickou hašovací funkcí. A až poté se tento haš podepíše daným asymetrickým šifrovacím algoritmem za pomoci privátního klíče.

Poté si každý, kdo zná patřičný veřejný klíč podepsané osoby, může ověřit platnost digitálního podpisu aplikací tohoto veřejného klíče, podepsaných dat (či haše) a digitálního podpisu za použití tzv. verifikačního algoritmu. Pokud je výsledek verifikace podpisu daných dat v pořádku, tak můžeme mít jistotu, že zpráva byla podepsána vlastníkem privátního klíče a že po podepsání již nebyla modifikována.

Správná znalost veřejného klíče (a komu patří) je tedy kritická pro používání digitálního podpisu.



4.4 Certifikáty veřejných klíčů

Jak jsme si již říkali u asymetrické kryptografie i u digitálního podpisu, hlavním problémem správy používání veřejných klíčů je jejich integrita a spojení s dalšími informacemi o držiteli klíče atd. Částečným řešením je použití certifikátů, které spolehlivě vážou veřejný klíč k oněm dalším informacím. Spolehlivé vázání je u certifikátů řešeno digitálním podpisem - operací s privátním klíčem entity, která takto vlastně "prohlašuje" vazbu za důvěryhodnou. To, jaká je konkrétně důvěryhodnost, záleží na mnoha faktorech a bude z různých hledisek různá - stejně jako je různá důvěra dvou jedinců ve výrok pronesený třetím jedincem. Nejčastější podoba certifikátů odpovídá standardu X.509 (mj. i certifikáty ve vašich Explorerech, Navigatorech atd.).

```
Certificate  ::=  SEQUENCE  {
     tbsCertificate       TBSCertificate,
     signatureAlgorithm   AlgorithmIdentifier,
     signature            BIT STRING  }
TBSCertificate  ::=  SEQUENCE  {
     version         [0]  Version DEFAULT v1,
     serialNumber         CertificateSerialNumber,
     signature            AlgorithmIdentifier,
     issuer               Name,
     validity             Validity,   -- notBefore, notAfter
     subject              Name,
     subjectPublicKeyInfo SubjectPublicKeyInfo,  -- algID, bits
     issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
     subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
     extensions      [3]  Extensions OPTIONAL
            -- sequence of: extnID, crit, value }
```

Část certifikátu dle X.509.

Otázkou často je, zda ono certifikování svěříme nějaké "důvěryhodné" instituci - tzv. třetí straně, nebo zda jej provádíme přímo sami. Oba postupy mají své výhody a nevýhody. Obvykle platí, že odborníci na bezpečnost preferují postup, kdy mají kontrolu nad tím, komu vlastně věří a proč, sami - například podpisem PGP klíčů svých partnerů pro komunkaci. Toto ale nelze předpokládat u všech uživatelů WWW - tady je vhodnější cesta oněch třetích stran nazývaných pro tento účel certifikační autority. Je pak potřeba mít na paměti, že veškerou důvěru při ověřování vazeb klíč-držitel, často spojených s ověřováním držitele, takto uživatelé svěřují certifikační autoritě. Pokud takovýto postup vyhovuje (certifikační autoritou je někdo skutečně důvěryhodný, popř. je to skupina určená vedením podniku pro všechny jeho zaměstnance atd.), pak je tato cesta schůdnější - pro uživatele certifikátů. Je třeba si uvědomit, že pro opravdu spolehlivou certifikační autoritu, nabízející své služby na Internetu bez omezení a v kvalitě, které mají uživatelé alespoň minimální důvod věřit, se pohybují náklady na zahájení provozu asi na 2-5 mil. dolarů a náklady na roční provoz okolo miliónu.

U certifikátů podle X.509, které nalezly svoje uplatnění v zajištění bezpečnosti na Internetu, je potřeba brát v úvahu to, že sice odpovídají standardu co se položek certifikátu týče, ale jejich implementace může být odlišná pro různé typy aplikací a platforem. Tak je tomu částečně i u certifikátů pro prohlížeče od Microsoftu nebo Netscape.