Šifry

Martin Dungl

Přednáška bude složena ze dvou částí. V první části objasním základní kryptologické pojmy a zásady a budeme se zabývat starými šiframi a způsoby jejich prolomení. Ve druhé části si povíme něco o asymetrické kryptologii, která vznikla až ve 2. polovině 20. století a je založena na složitosti některých matematických problémů. Náplní bude hlavně systém RSA, hašovací funkce a s nimi související elektronický podpis. Zbude-li čas, řekneme si i o tom, jak se dá házet mincí po telefonu `:-)`.

Pojmy.

- *kryptografie* – věda o skrývání obsahu (šifrování) zpráv
- *kryptoanalýza* – věda o dešifrování zpráv, tedy o tom, jak z šifrového textu odvodit otevřený text bez znalosti klíče
- *kryptologie* – kryptografie + kryptoanalýza
- *steganografie* – věda o skrývání existence zpráv
- *text* – posloupnost znaků nějaké abecedy, standardně se používá anglická abeceda; v moderní kryptografii je to posloupnost nul a jedniček
- *otevřený text* – původní zpráva před zašifrováním
- *šifrový text* – to, co dostaneme zašifrováním otevřeného textu
- *klíč* – volitelný element měnící obecný šifrovací algoritmus ve specifický postup šifrování; útočník smí znát šifrovací algoritmus, nesmí však znát klíč

Definice. *Nechť M je množina možných otevřených textů, S množina šifrových textů, K množina možných klíčů. Pak se zobrazení $C : K \times M \to S$ prosté pro $\forall k \in K$ nazývá šifrovací algoritmus. Nechť $m \in M$, $k \in K$. Značíme $C_k(m) := C(k, m)$. Dešifrovacím algoritmem se rozumí zobrazení $D_k : D_k(C_k(m)) = m$.*

Časem se ukázalo nemožné nebo nepraktické zatajovat šifrovací algoritmus. Je tedy žádoucí zvolit jej tak, aby množina klíčů K byla dost velká a útočník nemohl vyzkoušet všechny klíče v ní obsažené. Klíč musí bezpodmínečně zůstat utajen. Vyvstává problém bezpečného předání klíče zamýšlenému příjemci. A. Kerckhoffs formuloval na konci 19. století následující pravidla výměny klíčů:

- Nikdy neposílat klíč stejným přenosovým kanálem jako šifrový text.
- Nikdy nešifrovat více zpráv jedním klíčem.
- Nikdy nešifrovat jednu zprávu více klíči.

Historie zná mnoho příkladů, kdy porušení těchto pravidel mělo tragické důsledky. Jedná se např. i o prolomení německého kódu Enigma ze 2. světové války.

Jednoduché šifrovací algoritmy

Dělíme na transpoziční a substituční. Při substituci je každý znak nebo blok otevřeného textu nahrazen v šifrovém textu jiným znakem nebo blokem stejné délky. Transpoziční šifra místo toho přemístí každé písmeno ve zprávě na jiné místo. Nejprve uvedu několik substitučních šifer. Někde budu pod pojmem písmeno myslet jeho pořadové číslo v abecedě mod 26.

• **Caesarova šifra.** Šifrový text vznikne z otevřeného posunutím abecedy o k znaků, kde $k \in \{0, \ldots, 25\}$. Tedy $s_i = C_k(m_i) = (m_i + k) \bmod 26$, kde s_i resp. m_i značí i-tý znak šifrového resp. otevřeného textu. Nevýhoda Caesarovy šifry – pouze 26 klíčů (z nichž jeden je slabý), lze je tedy vyzkoušet všechny.

• **Jednoduchá záměna.** Každý znak je nahrazen obecně jiným znakem téže abecedy. Klíčem k šifře je tedy permutace $\Pi : \{1, \ldots, 26\} \to \{1, \ldots, 26\}$. $s_i = C_\Pi(m_i) = \Pi(m_i)$. Pro velký prostor klíčů (je jich 26!) nebude fungovat stejný postup, jako při řešení Caesarovy šifry. Lze však spolehlivě postupovat tzv. frekvenční analýzou, tedy podle četnosti znaků v šifrovém textu najít jejich pravděpodobné vzory. K šifrovému textu o 30 znacích už je zpravidla otevřený text určen jednoznačně, na text o délce 50 – 100 znaků již lze použít spolehlivé algoritmy.

• **Vigenerova šifra.** Stejně jako v Caesarově šifře se posouvá abeceda, zde však o proměnlivý počet znaků. Tedy $s_i = (m_i + k_1) \bmod 26$, $s_{i+1} = (m_{i+1} + k_2) \bmod 26$, $s_{i+n-1} = (m_{i+n-1} + k_n) \bmod 26$, $s_{i+n} = (m_{i+n} + k_0) \bmod 26$, atd. Klíč k je řetězec o n znacích, k_i značí i-tý znak klíče. Šifru lze řešit např. tak, že statistickými metodami určíme délku klíče a dále postupujeme frekvenční analýzou.

• **Knižní šifra.** Podobně jako u Vigenerovy šifry sčítáme po znacích otevřený text s klíčem. Ten je však delší než otevřený text, nedochází tak k žádnému opakování. Informace o otevřeném textu však lze zjistit z toho, že v knize se vyskytují slova z nějakého jazyka. Zvolíme slovo, o kterém očekáváme, že se v knize vyskytuje, a zkoušíme jej odečíst postupně od šifrového textu. V okamžiku, kdy rozdíl dává smysl, máme část otevřeného textu. Z té pak postupně můžeme určit celek.

• **Vernamova šifra.** Absolutně bezpečná. Otevřený text je sčítán s náhodným řetězcem – klíčem. Nevýhodou je, že klíč je stejně dlouhý jako otevřený text a vyvstává nutnost nějak si jej předat. Zkuste si také rozmyslet, k čemu by vedlo opakované použití stejného klíče.

• **Transpoziční šifry.** Různými způsoby je měněno pořadí znaků v textu. Použití transpoziční šifry poznáme tak, že v textu je cca stejný poměr výskytu jednotlivých znaků, jako v běžném jazyce.

• **Steganografické metody.** Vytetujete-li zprávu na vyholenou hlavu otroka, počkáte až mu narostou vlasy a pošlete jej za příjemcem, používáte steganografii `:-)`. Později se přešlo k používání neviditelných inkoustů, ještě později k mikrofilmům s fotkou zprávy. V dnešní době lze data zakódovat např. do komprimovaných obrázků

nebo MP3 nahrávek. Použití tam, kde není žádoucí, aby protivník věděl o přenosu informace.

Asymetrická kryptografie

Používají se dva klíče, které jsou vygenerovány zároveň – veřejný a privátní. Veřejný klíč slouží k šifrování, privátní pak k dešifrování. Informace o privátním klíči je obsažena v klíči veřejném, jeho získání je však ekvivalentní s vyřešením výpočetně velmi složité matematické úlohy. Ve většině šifrovacích algoritmů však není tato ekvivalence dokázána.

• **Systém RSA.** Objeven v r. 1977, stále nejpoužívanější. Spoléhá na velkou výpočetní složitost faktorizace velkých čísel. Mějme dáno celé číslo n, cílem je najít jeho zápis ve tvaru $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$, kde p_i jsou prvočísla a e_i přirozená čísla. Pro účely RSA volíme modul n tak, aby měl řádově stovky číslic (za bezpečné se považuje 1024 bitů), $k = 2$ a $e_1 = e_2 = 1$.

Jak funguje RSA? Vygenerujeme nezávisle dvě velká (zhruba stejně) prvočísla p a q, $p \neq q$. Spočteme $n = p \cdot q$, $\lambda = NSD(p-1, q-1)$. Zvolíme náhodné číslo $e : 1 < e < \lambda$, aby $NSD(e, \lambda) = 1$. Někdy se e volí pevně ($e = 3, e = 65537$). Spočteme d takové, že platí $1 < d < \lambda$ a $e \cdot d \equiv 1 (\mathrm{mod}\ \lambda)$. Pak veřejným klíčem je dvojice (n, e) a privátním dvojice (n, d).

Šifrování pak vypadá následovně: Zpráva pro šifrování se zformátuje tak, aby byla obsažena v čísle m. Pro m musí platit $0 \leq m \leq n-1$. Je-li na to zpráva příliš dlouhá, rozdělí se na více částí. Šifrový text získáme takto $c = RSA_e(n, m) = m^e \bmod n$. Z c může získat otevřený text pouze příjemce, a to následovně: $m' = RSA_d(n, c) = c^d \bmod n$. Zbývá dokázat dvě věci – že $m = m'$ a že prolomení RSA je ekvivalentní s faktorizací modulu n. Důkaz $m = m'$ provedu na přednášce, opírá se o malou Fermatovu větu. Ekvivalenci RSA s faktorizací se zatím nepodařilo prokázat, považuje se však za pravděpodobnou. Na faktorizaci velkého čísla neexistuje uspokojivě rychlý algoritmus.

• **Hašovací funkce.** Jsou to takové funkce $f : M \to S$, jejichž vstupní kód může být prakticky libovolně dlouhý, výstupní kód má předem pevně stanovenou délku (zejména 128, 160 nebo 256 bitů) a pro něž je snadné z jakékoli hodnoty $m \in M$ vypočítat $s = f(m)$, ale pro nějaký náhodně vybraný obraz $s \in S$ nelze (je to pro nás výpočetně nemožné) najít nějaký jeho vzor $m \in M$ tak, aby $s = f(m)$. Této vlastnosti říkáme bezkoliznost. Příklady využití: kontrola integrity, ukládání a kontrola přihlašovacích hesel, prokazování autorství, jednoznačná identifikace dat (jednoznačná reprezentace vzoru, digitální otisk dat, jednoznačný identifikátor dat, to vše zejména pro digitální podpisy), generátory pseudonáhodných čísel.

• **Elektronický podpis.** Je to analogie standardního podpisu pro elektronické dokumenty. Jsou na něj dva požadavky – nepopiratelnost (třetí strana dokáže rozhodnout, zda daný subjekt dokument podepsal) a nepadělatelnost (neexistuje zpráva, jejíž podpis je výpočetně schůdné najít pouze pomocí veřejného klíče a jiných podepsaných zpráv). Autor zprávy m na ni nejprve použije hašovací funkci h, její výstup t pak zašifruje asymetrickou šifrou f při použití privátního klíče. Její výstup s přiloží ke zprávě. Příjemce pak dostane zprávu a podpis. Pokud platí $s = f_{s\ veřejným\ klíčem}\ (t) = h(m)$, je podpis platný.