Komunikace přes nezabezpečený kanál

Filip Hlásek

Abstrakt. Tento text je volným pokračováním mého příspěvku *100 vězňů a žárovka*. Budeme uvažovat dva subjekty, které se snaží tajně si předat zprávu. Všechna jejich komunikace je sice odposlouchávána, ale naštěstí jsou informace doručeny v neporušeném stavu.

Již několik tisíciletí se spolu lidé různými způsoby dorozumívají. Od počátků komunikace se pokoušejí zprávy zabezpečit tak, aby ji mohl přijmout pouze pravý adresát. Jedním z prvních důmyslných systémů byla Caesarova šifra, která umožňuje snadno zakódovat posílaný text do zdánlivě nečitelné podoby a luštění je téměř stejně jednoduché. Od té doby lidé vymysleli několik důmyslnějších technik a s příchodem počítačů se obor, kterému se dnes říká kryptografie, začal neuvěřitelnou rychlostí rozvíjet. Pojďme se společně podívat na některé základní postupy používané v moderním šifrování. Začneme zdánlivě nesouvisející a snadnou hádankou, která nám hravou cestou ukáže důležité myšlenky.

Úloha. Alice a Bob jsou ubytováni ve stejném hotelu v oddělených místnostech, které nemohou opustit. Jediná možnost, jak si mohou něco předat, je pomocí poslíčka Evy. Bob chce poslat Alici prstýnek, ale bojí se, že by ho Eva mohla ukrást. Oba milenci mají na svých pokojích několik trezorů, visacích zámků a odpovídajících klíčů. Zamčené trezory můžeme považovat za nedobytné a navíc víme, že Eva celé trezory nekrade. Jak to mají udělat, aby se prstýnek bezpečně dostal k Alici?

Řešení. Bob uloží prstýnek do trezoru, který zamkne visacím zámkem a pošle Alici. Ta ještě zamkne trezor jedním ze svých zámků a pošle dvakrát zamčený trezor zpátky Bobovi. Chlapec odemkne svůj zámek, a když Alice obdrží trezor podruhé, zbývá na něm pouze její zámek, od kterého má ona jediná klíč. Trezor nikdy necestoval nezamčený a prstýnek se dostal od Boba k Alici. Využili jsme toho, že se zámky nemusejí odemykat ve stejném pořadí, v jakém byly zamčeny.

Úloha. Peggy právě vyřešila sudoku, se kterým si Viktor stále ještě neví rady. Zdá se mu skoro neřešitelné a vůbec Peggy nevěří, že řešení skutečně má a nikde neudělala chybu. Jak Peggy Viktora přesvědčí, že její řešení je správné, aniž by mu jakkoliv poradila?

Úloha. Dvanáct organizátorů PraSátka se při chystání soustředění baví o svých studijních výsledcích. Chtěli by spočítat, kolik za poslední ročník získali v průměru kreditů, ale každý se stydí za to, jak málo jich má. Navrhněte postup, kterým průměrný počet zjistí, aniž by někdo prozradil svůj zisk.

Úloha. Indiánka Alice a indián Bob jsou náčelníci spřátelených indiánských kmenů žijících v nedalekých indiánských vesnicích. Banditka Eva nemá žádné problémy sledovat všechny jejich zprávy předávané kouřovými signály pomocí Morseovy abecedy. Alice s Bobem se to rozhodli změnit a na schůzce se dohodnou na novém způsobu předávání zpráv pomocí kouřových signálů. Zkuste jim poradit, jak to udělat.

Symetrické šifry

Symetrická šifra je takový šifrovací algoritmus, který používá k šifrování i dešifrování jediný klíč. Ten musí být známý oběma stranám před zahájením komunikace a je potřeba si ho předem dohodnout jinou cestou. Podstatnou výhodou symetrických šifer je jejich nízká výpočetní náročnost. Mezi nejjednodušší příklady symetrických šifer patří substituční, které jsou ovšem v dnešní době již snadno rozluštitelné bez znalosti klíče za pomoci počítačů.

Asymetrické šifry

Asymetrické šifrování se vyznačuje tím, že klíč sestává ze dvou částí. Jedna část se používá pro šifrování zpráv (a příjemce zprávy ani tuto část nemusí znát), druhá pro dešifrování (a odesilatel šifrovaných zpráv ji zpravidla nezná). Je vidět, že ten, kdo šifruje, nemusí s dešifrujícím příjemcem zprávy sdílet žádné tajemství, čímž eliminují potřebu výměny klíčů.

Šifrovací klíč a dešifrovací klíč spolu musí být samozřejmě svázány, avšak nezbytnou podmínkou pro užitečnost šifry je praktická nemožnost ze znalosti šifrovacího klíče spočítat dešifrovací.

Odkazy

[1] *http://www.merkle.com/1974/PuzzlesAsPublished.pdf*
[2] *http://mathworld.wolfram.com/Diffie-HellmanProtocol.html*
[3] *https://cs.wikipedia.org/wiki/Kryptografie*
[4] *http://www.wisdom.weizmann.ac.il/ naor/PAPERS/sudoku.pdf*
[5] Simon Singh: *The Code Book*, *http://simonsingh.net/books/the-code-book/*