Modulární systém dalšího vzdělávání pedagogických pracovníků JmK
v přírodních vědách a informatice
CZ.1.07/1.3.10/02.0024

Kryptografie

Poznámky pro učitele

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERSITAS MASARYKIANA BRUNENSIS
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Kryptografie - poznámky pro učitele

Tento materiál poskytuje náměty na hry/aktivity, které mohou posloužit jako motivace a úvod k tématu moderní kryptografie.

Seznam námětů :

- Kolik vážíme?
- Nepodváděj!
- Kufr

Kolik vážíme?

Typ: Interaktivní aktivita.

Předpoklady: Žádné.

Zaměření: Úvod do principů moderní kryptografie, princip náhodnosti, zachování soukromí.

Náročnost: Lehká, 5-10 minut.

Materiál: Papír, tužka pro každého účastníka.

Průběh: Představte si, že chceme zjistit, kolik všichni dohromady vážíme - chceme třeba nastoupit do výtahu a nejsme si jistí, jestli se vlezeme do jeho nosnosti. No nejjednodušší by bylo, kdybychom každý řekli kolik vážíme a všechno to sečetli. Hmotnost je ale velmi citlivá informace a ne každý vám ji ochotně sdělí. Jak tedy spočítat součet hmotností celé skupiny a přitom neprozradit svoji vlastní hmotnost? Že to nejde?

Nejprve vyzvěte jednoho studenta, aby na papír napsal libovolné náhodné číslo větší než 1000 a toto číslo si zapamatoval a uchoval v tajnosti. Poté pošle papír druhému studentovi. Ten k tomu číslu přičte svoji hmotnost, nově vzniklé číslo napíše na nový papír a pošle jej třetímu. Třetí nebude vědět, kolik váží druhý, protože nezná původní náhodné číslo. Už víte, jak budeme pokračovat? Dokola až papír obdrží zase první student. Ten přičte svoji hmotnost, odečte náhodné číslo, které napsal na začátku a je to - víme kolik váží všichni dohromady. I když se to zdálo nemožné, dokázali jsme získat potřebnou informaci a přitom zachovat soukromí všech.

Zdroj: převzato z http://csunplugged.org/information-hiding

Obměna: Místo váhy lze počítat součet/průměr čehokoliv jiného (velice citlivou informací je například plat). Cvičení se dá postavit i jako tajné hlasování.

Nepodváděj!

Typ: Interaktivní aktivita.

Předpoklady: Žádné.

Zaměření: Úvod do principů moderní kryptografie, představení jednosměrné funkce.

Náročnost: Lehká, 10 minut.

Materiál: Mince, dva identické telefonní seznamy.

Průběh: Vyvolejte jednoho studenta. Budete s ním hrát panna nebo orel o čokoládu. Hodíte mincí, když to student uhodne, dostane čokoládu. Vy mu ale budete lhát minci mu ani nebudete ukazovat, jen mu budete pořád tvrdit, že prohrává. Časem vás určitě někdo oprávněně nařkne, že podvádíte. Jak to tedy zařídit, abyste podvádět nemohli, i když s protihráčem na sebe nevidíte? Vy i student si vezmete telefonní seznam. Když znáte jméno, je lehké najít telefonní číslo, ale když znáte jen telefonní číslo je strašně težké najít příslušné jméno. Přesně to je jednosměrná funkce - jedním směrem to spočítáte snadno a druhým ne. Takže jak teď hrát? Vyberete si telefonní číslo a řeknete ho studentovi. Zeptáte se, jestli je to telefonní číslo člověka, jehož jméno začíná na R nebo na S. Student si tipne a vy pak řeknete čí telefonní číslo to je, aby si to student mohl ověřit. Zkuste to ne s telefonním seznamem ale třeba s nějakou učebnicí nebo knihou a nechte studenta hádat, jestli je určité slovo na sudé nebo liché stránce. Snadno budete moct podvádět, pokud se slovo bude vyskytovat v knize vícekrát. Nechte studenty podvot odhalit a formulovat, jakou vlastnost musí kniha, tedy jednosměrná funkce mít.

Zdroj: převzato z http://csunplugged.org/cryptographic-protocols

Kufr

Typ: Interaktivní aktivita.

Předpoklady: Žádné.

Zaměření: Úvod do principů moderní kryptografie. Ukázka, že ne vždy potřebujeme sdílet klíč.

Náročnost: Lehká, 5-10 minut.

Materiál: čokoláda, kufr, dva zámky se dvěma různými klíči.

Průběh: Alice chce Bobovi poslat čokoládu. Po cestě ale číhá mlsná Eva aby ji ukradla. Jak to provedou? Alice musí čokoládu zamčít do kufru. Ale Bob nemá klíče. Alice mu je poslat nemůže, protože Eva by je mohla ukradnout společně s kufrem a čokoládu jim ukrást. Bobovi nezbývá nic jiného než zamčít kufr ještě jednou svým zámkem. Pošle jej zpět Alici a ta kufr odemče a pošle jej zpět Bobovi. Eva k němu pořád nemůže a Bob si jej pak odemče vlastním klíčem.