Vybrane kapitoly z kryptografie

DOMACA ULOHA #1.

Datum odovzdania: 9. oktober

Zakladne pravidla odovzdania domacej ulohy:

- uvedte na kazdej strane vase meno
- strany musia byt cislovane; na zaciatku ulohy uvedte, kolko ma uloha stran
- jasne oznacte, ktory problem riesite a zoradte priklady podla poradia zo zadania
- riesenie kazdeho problemu napiste pozorne a s dostatocnymi detailmi, ktore mi umoznia vyhodnotit kvalitu vasho riesenia; ak si nie ste isti, radsej napiste viac
- domacu ulohu musite vypracovat samostatne a o radu mozete ziadat len mna
- ak budu dve ulohy vyzerat prilis podobne, obe ulohy dostanu 0 bodov
- uloha musi byt bud naklepana alebo napisana velmi jasne a scanovana
- ulohu odovzdavate v "moodle" v pdf formate
- oneskorena domaca uloha bude prijata len v nezavinenej situacii

1. (10 bodov)

a) Vymyslite zmysluplnu "vzdialenost" medzi dvoma rozdeleniami frekvencii znakov abecedy v roznych jazykoch (podobne rozdelenie frekvencii maju malu vzdialenost, rozdielne maju vacsiu vzdialenost, takze napr. frekvencie cestiny a slovenciny by mali byt blizko (asi nie su totozne) a frekvencia slovenciny a baskictiny by mali byt daleko)

b) Vypocitajte vzdialenost frekvencii styroch jazykov a porovnajte, ci koresponduju s geografickou vzdialenostou narodov, ktore nimi hovoria

c) Otestujte nasledovnu hypotezu: Preklad z jazyka x do jazyka y bude mat rozdelenie frekvencie znakov mierne odlisne od rozdelenia jazyka y a priblizi sa rozdeleniu jazyka x. Vyberte si akekolvek dva jazyky, kde viete ziskat ich frekvencie a dostatocne dlhy preklad.

2. (10 bodov) Uvazujte "slovnikovy preklad" znak po znaku, t.j., bijekciu $\psi \in \mathbb{S}_{26}$ z abecedy 26 znakov do abecedy 26 znakov.

a) Ak na desifrovanie bez kluca potrebujete otestovat 26! bijekcii, odhadnite kolko operacii potrebujete v priemere otestovat, ak viete cyklovu strukturu ψ ako prvku $\mathbb{S}_{26}$

b) Rozhodnite o kolko sa stazi desifrovanie, ak sa na sifrovanie pouzije kompozicia n permutacii z $\mathbb{S}_{26}$

c) Rozhodnite a zdovodnite svoje rozhodnutie, ci je tazsie desifrovat spravu zasifrovanu 13 involuciami alebo spravu zasifrovanu cyklom dlzky 26

3. (10 bodov) Uvazujte nasledovnu sifrovaciu schemu: Plaintext sa rozdeli na bloky dlzky n a zasifruje sa tak, ze sa poradie znakov v kazdom bloku poprehadzuje pomocou permutacie $\phi \in \mathbb{S}_n$ (takze blok dlzky n zostane dlzky n, ale prve pismeno sa presunie do pozicie $\phi(1)$, druhe pismeno do pozicie $\phi(2)$, ...).

a) Popiste rozdiel v distribucii symbolov medzi slovnikovym prekladom a touto schemou.

b) Navrhnite utok na takuto schemu, ktory je podstatne rychlejsi ako skusanie vsetkych permutacii v $\mathbb{S}_n$

c) Aky typ informacie o ϕ by vam pomohol zrychlit vas utok?

4. (10 bodov)

a) Najdite formuly na pocet $n \times n$ oznacenych a neoznacenych sifrovacich mriezok.

b) Navrhnite rychly utok na text sifrovany $n \times n$ mriezkou.

c) O kolko sa zrychli desifrovanie sifrovaneho textu, ak pozname prvych k symbolov povodneho plaintextu?

d) Predstavte si, ze ste prijali dve sifrovane spravy, kde zhodou okolnost viete, ze plaintext druhej je oprava plaintextu prvej spravy, v ktorom pred sifrovanim chybal prvy symbol spravy (t.j., $\mathcal{P}_1 = a_2, a_3, \ldots, a_{n^2}$ a $\mathcal{P}_2 = a_1, a_2, \ldots, a_{n^2}$). O kolko sa zrychli desifrovanie?

5. (10 bodov) Suppose a message is written in the Morse code with the spaces left out (so it becomes a sequence of dots and lines), and then is encrypted as follows: a four digit number $n = i_1 i_2 i_3 i_4$ is chosen as the secret key and the sequence of dots and lines is then broken into blocks of length 4 and each of the blocks is encrypted by comparing the four symbols in the block with n and changing the j-th symbol in the block to the opposite symbol (i.e., a dot to a line and a line to a dot) if i_j is odd (and not changing the symbol if i_j is even).

a) Can Oscar break this encryption by using frequency analysis? Why or why not?

b) Devise a brute force algorithm for Oscar to break this encryption system.

c) Find a buddy in the class and send him/her a message encrypted this way without telling him/her the secret key. Have him/her send you a message encrypted this way as well (and again without giving you the key). Decrypt the message you get from your buddy.

6. (10pts) Let $[a_1, a_2, a_3, \ldots, a_n]$ be a weight vector of different weights, and assume that you are solving an altered knapsack problem where you can choose not to use a weight a_i or use it once or use it twice (unlike the usual knapsack where you only have the options of using a weight once or not at all). Find a definition analogous to that of a super increasing sequence that, when applied to $[a_1, a_2, a_3, \ldots, a_n]$, would guarantee a fast solution for the altered knapsack problem for the sequence $[a_1, a_2, a_3, \ldots, a_n]$. Describe the solution algorithm and show your method on a reasonably sized example that requires using at least one of the weights twice.