Богдан Уладзіслаў

ФПМІ, 4 курс, 3 група

Лабараторная работа 1

Крыптааналіз метадаў простай падстаноўкі

1-2. Рэалізацыя праграмнага сродка для шыфравання/дэшыфравання тэкставага файла.

Праграма рэалізаваная на мове Go. Працуе з тэкстамі на ангельскай і беларускай мовах (падтрымка іншых моваў дадаецца праз вызначэнне дадатковых алфавітаў). Прыклады камандаў, якія ажыццяўляюць шыфраванне/дэшыфраванне:

Шыфраванне тэкста на ангельскай мове (мова па змоўчванні) метадам Цэзара з выпадкова-згенераваным зрухам:

```
./lab1-substitutions -encrypt -file=in.txt -out=out.txt
```

Дэшыфраванне тэкста на беларускай мове, зашыфраванага метадам Цэзара; ажыццяўляецца з прымяненнем частотнага аналіза:

```
./lab1-substitutions -decrypt -file=out.txt -out=result.txt -lang=be
```

Шыфраванне тэкста на ангельскай мове з заданнем ключавога слова (метад Віжэнэра):

```
./lab1-substitutions -encrypt -file=in.txt -out=out.txt -vigenere_keyword="plot"
```

Дэшыфраванне тэкста на беларускай мове, зашыфраванага метадам Віжэнэра; ажыццяўляецца па метадзе Касіскі:

```
./lab1-substitutions -decrypt -file=out.txt -out=result.txt -lang=be -kasiski_decryption
```

Зыходны код даступны на GitHub: https://github.com/uladbohdan/uni-code/7-security/lab1-substitutions

Магчымасці праграмы могуць быць пратэставаныя скрыптом, які знаходзіцца разам з зыходным кодам (патрэбныя кампілятар go і утыліта diff):

```
bash run_tests.sh
```

3-4. Эксперыментальнае даследаванне залежнасці імавернасці паспяховага правядзення атакі па метадзе Касіскі ад даўжыні шыфратэкста і даўжыні ключавога слова.

тэкст / даўжыня ключавога слова	2	3	4	5	6	7
кароткі ангельскі: 445 сімвалаў	−(2)	−(6)	−(8)	−(5)	−(6)	−(245)
сярэдні ангельскі: 1686 сімвалаў	+	+	− (1)	+− (5)	+− (6)	−(1)
доўгі ангельскі: 27103 сімвала	+	+	−(2)	+	−(2)	+
кароткі беларускі: 559 сімвалаў	+− (4)	+	(8)	−(10)	−(204)	−(1)
сярэдні беларускі: 1775 сімвалаў	+	+	+	+	+	+
доўгі беларускі: 61241 сімвал	+	+	−(2)	+	+	+

Па табліцы:

1. + - тэкст цалкам расшыфраваўся, − - тэкст не расшыфраваўся, +− - тэкст расшыфраваўся часткова, так, што яго можна чытаць.

2. у дужках - даўжыня кодавага слова па прадказанні метада Касіскі. Часам даўжыня была ўгаданая правільна, але алгарытм не здолеў расшыфраваць тэкст праз тое, што кепска спрацаваў частотны аналіз.

3. вынікі эксперымента дастаткова суб'ектыўныя, вельмі моцна вынік залежыць ад падабранага тэкста. Агульная тэндэнцыя, тым не менш, заўважная.

4. з ростам памера тэкста надзейнасць расце: гэта звязана з тым, што правільнасць выканання частотнага аналіза проста залежыць ад памера ўваходных дадзеных.

5. з ростам даўжыні ключавога слова дэшыфраванне працуе горш. Прычыны: (а) зашыфраваныя ўчасткі паўтараюцца радзей, адпаведна, складаней высветліць даўжыню ключавога слова; (б) неабходнасць выканання частотнага аналіза на тэкстах, даўжыня якіх падае з ростам даўжыні ключавога слова.