0.1 Front matter

title: “Лабораторная работа №8” subtitle: “Основы информационной безопасности” author: “Пинега Белла Александровна”

0.2 Generic otions

lang: ru-RU toc-title: “Содержание”

0.3 Bibliography

bibliography: bib/cite.bib csl: pandoc/csl/gost-r-7-0-5-2008-numeric.csl

0.4 Pdf output format

toc: true # Table of contents toc-depth: 2 lof: true # List of figures lot: true # List of tables fontsize: 12pt linestretch: 1.5 papersize: a4 documentclass: scrreprt ## I18n polyglossia polyglossia-lang: name: russian options: - spelling=modern - babelshorthands=true polyglossia-otherlangs: name: english ## I18n babel babel-lang: russian babel-otherlangs: english ## Fonts mainfont: PT Serif romanfont: PT Serif sansfont: PT Sans monofont: PT Mono mainfontoptions: Ligatures=TeX romanfontoptions: Ligatures=TeX sansfontoptions: Ligatures=TeX,Scale=MatchLowercase monofontoptions: Scale=MatchLowercase,Scale=0.9 ## Biblatex biblatex: true biblio-style: “gost-numeric” biblatexoptions: - parentracker=true - backend=biber - hyperref=auto - language=auto - autolang=other* - citestyle=gost-numeric ## Pandoc-crossref LaTeX customization figureTitle: “Рис.” tableTitle: “Таблица” listingTitle: “Листинг” lofTitle: “Список иллюстраций” lotTitle: “Список таблиц” lolTitle: “Листинги” ## Misc options indent: true header-includes: -

keep figures where there are in the text

- ### # keep figures where there are in the text

1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

2 Задание

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба тек- ста. Необходимо разработать приложение, позволяющее шифровать и де- шифровать тексты P1 и P2 в режиме однократного гаммирования. Прило- жение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо

определить и выразить аналитиче- ски способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

3 Теоретическое введение

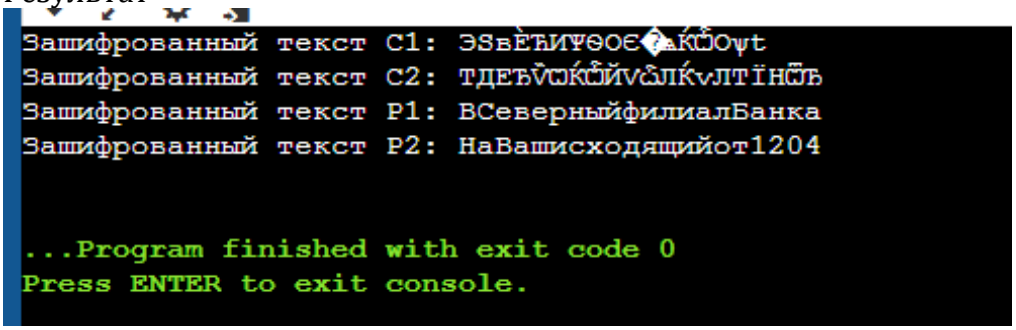
Исходные данные. Две телеграммы Центра: P1 = НаВашисходящийот1204 P2 = ВСеверныйфилиалБанка Ключ Центра длиной 20 байт: K = 05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 OB B2 70 54 Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой, приведён- ной на рис. 8.1. Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования: C1 = P1 ⊕ K, C2 = P2 ⊕ K. (8.1) Открытый текст можно найти в соответствии с (8.1), зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства (8.1) Рис. 8.1. Общая схема шифрования двух различных текстов одним ключом 1При составлении работы использовалось пособие [1]. Информационная безопасность компьютерных сетей 49 складываются по модулю 2. Тогда с учётом свойства операции XOR 1 ⊕ 1 = 0, 1 ⊕ 0 = 1 (8.2) получаем: C1 ⊕ C2 = P1 ⊕ K ⊕ P2 ⊕ K = P1 ⊕ P2. Предположим, что одна из телеграмм является шаблоном — т.е. име- ет текст фиксированный формат, в который вписываются значения полей. Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар C1 ⊕ C2 (известен вид обеих шифровок). Тогда зная P1 и учитывая (8.2), имеем: C1 ⊕ C2 ⊕ P1 = P1 ⊕ P2 ⊕ P1 = P2. (8.3) Таким образом, злоумышленник получает возможность определить те символы сообщения P2, которые находятся на позициях известного шаб- лона сообщения P1. В соответствии с логикой сообщения P2, злоумышлен- ник имеет реальный шанс узнать ещё некоторое количество символов сооб- щения P2. Затем вновь используется (8.3) с подстановкой вместо P1 полу- ченных на предыдущем шаге новых символов сообщения P2. И так далее. Действуя подобным образом, злоумышленник даже если не прочитает оба сообщения, то значительно уменьшит прос

4 Выполнение лабораторной работы

1. Код программы:

```python
def encr(t1, t2):
    t1 = [ord(i) for i in t1]
    t2 = [ord(i) for i in t2]
    return ''.join(chr(a^b) for a, b in zip(t1, t2))

P1 =  "НаВашисходящийот1204"
P2 =  "ВСеверныйфилиалБанка"

K = "05 0C 17 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54"

C1 = encr(P1, K)
C2 = encr(P2, K)

decr = encr(C1, C2)

print('Зашифрованный текст C1:', C1)
print('Зашифрованный текст C2:', C2)
print('Зашифрованный текст P1:', encr(decr, P1))
print('Зашифрованный текст P2:', encr(decr, P2))
```

2. Результат



5 Выводы

Я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

Список литературы