Отчет по лабораторной работе 8

Nikitaeva A. S.[1]

16 September, 2021 Moscow, Russian Federation

[1]RUDN University, Moscow, Russian Federation

Цель выполнения лабораторной работы

Цель

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

Результаты выполнения лабораторной работы

Исходные данные

```
P1 = "GimmeGimmeGimmeA"
P2 = "ManAfterMidnight"
```

```
Длина первой телеграммы 16 символов, а второй -- 16
```

Кодирование исходных текстов

```
Исходная телеграмма 1:  GimmeGimmeGimmeA
Исходная телеграмма 2:  ManAfterMidnight
Телеграмма 1 в 16-ой форме:  ['47', '69', '6d', '6d', '65', '47', '69', '6d', '6d', '65', '47', '69', '6d', '6d', '65', '41']
Телеграмма 2 в 16-ой форме:  ['4d', '61', '6e', '41', '66', '74', '65', '72', '4d', '69', '64', '6e', '69', '67', '68', '74']
Ключ длиной 16 байт: ['7e', '7', 'e1', '13', 'd', '68', '6e', '89', 'cc', '99', '7', '35', '78', 'e0', 'dc', '27']
Зашифрованная телеграмма 1 в 16-ой форме:  ['39', '6e', '8c', '7e', '68', '2f', '07', 'e4', 'a1', 'fc', '40', '5c', '15', '8d',
'b9', '66']
Зашифрованная телеграмма 2 в 16-ой форме:  ['33', '66', '8f', '52', '6b', '1c', '0b', 'fb', '81', 'f0', '63', '5b', '11', '87',
'b4', '53']
Зашифрованная телеграмма 1:  9nЋ~h/□дЎь@\□ЌNºf
Зашифрованная телеграмма 2:  3fЏRk□□ыЃрс[□‡rS
```

Декодирование 2-ой телеграммы, зная шаблон 1-ой

```
Зашифрованная телеграмма 1:  9nЋ~h/□дЎь@\□Ќ№f
Зашифрованная телеграмма 2:  3fЏRk□□ыЃрс[□‡ґS
Зашифрованная телеграмма 1 в 16-ой форме:  ['39', '6e', '8c', '7e', '68', '2f', '07', 'e4', 'a1', 'fc', '40', '5c', '15', '8d',
'b9', '66']
Зашифрованная телеграмма 2 в 16-ой форме:  ['33', '66', '8f', '52', '6b', '1c', '0b', 'fb', '81', 'f0', '63', '5b', '11', '87',
'b4', '53']
Шаблон:  GimmeGimmeGimmeA
Шаблон в 16-ой форме:  ['47', '69', '6d', '6d', '65', '47', '69', '6d', '6d', '65', '47', '69', '6d', '6d', '65', '41']
Вторая телеграмма в 16-ой форме:  ['4d', '61', '6e', '41', '66', '74', '65', '72', '4d', '69', '64', '6e', '69', '67', '68', '7
4']
Вторая телеграмма:  ManAfterMidnight
```

Декодирование 1-ой телеграммы, зная шаблон 2-ой

```
Зашифрованная телеграмма 1:  9nЋ~h/□дЎь@\□Ќ№f
Зашифрованная телеграмма 2:  3fЏRk□□ыЃрс[□‡ґS
Зашифрованная телеграмма 1 в 16-ой форме:  ['39', '6e', '8c', '7e', '68', '2f', '07', 'e4', 'a1', 'fc', '40', '5c', '15', '8d',
'b9', '66']
Зашифрованная телеграмма 2 в 16-ой форме:  ['33', '66', '8f', '52', '6b', '1c', '0b', 'fb', '81', 'f0', '63', '5b', '11', '87',
'b4', '53']
Шаблон:  ManAfterMidnight
Шаблон в 16-ой форме:  ['4d', '61', '6e', '41', '66', '74', '65', '72', '4d', '69', '64', '6e', '69', '67', '68', '74']
Вторая телеграмма в 16-ой форме:  ['47', '69', '6d', '6d', '65', '47', '69', '6d', '6d', '65', '47', '69', '6d', '6d', '65', '4
1']
Вторая телеграмма:  GimmeGimmeGimmeA
```

Выводы по лабораторной работе

Выводы

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

Спасибо за внимание!