

Федеральное агентство связи
Ордена Трудового Красного Знамени
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский технический университет связи и информатики»

Кафедра теории Информационная безопасность

Отчет по лабораторной работе №4
по дисциплине «Основы информационной безопасности»
на тему:
«Электронно-цифровая подпись и приемы хеширования»

Выполнили: студенты группы
БВТ1905

Колышев Николай Игоревич

Шведчиков Алексей
Сергеевич

Щербань Артём Евгеньевич

Руководитель:

Тауфик Бен Режеб Бен Камель

Москва 2020

Оглавление

1 Тема	3
2 Цель работы	3
3 Ход работы	3
4 Постановка задачи	3
5 Листинг программы	3
6 Результат выполнения программы	10
7 Вывод	10

1 Тема

Электронно-цифровая подпись и приемы хеширования.

2 Цель работы

Получение основных теоретических сведений и практических навыков по оценке стойкости парольной защиты.

3 Ход работы

1. Ознакомиться с теоретической частью данной работы.
2. Составить программу-генератор паролей.
3. Составить отчет по проделанной работе.
4. Защитить работу.

4 Постановка задачи

Составить программу шифрования методом контрольных сумм и методом хеширования с применением гаммирования. Пусть $a = 71$, $b = 13$, $c = \text{MaxVal} + 1 = 256$, $t_0 = 144$. Вычислить контрольные суммы для нескольких сообщений методом контрольных сумм (KSumm) и методом хеширования с применением гаммирования (SummKodBukvOtkr): а) $P = '100009'$, KSumm = ?, SummKodBukvOtkr – ?; б) $P = '900001'$, KSumm = ?, SummKodBukvOtkr – ?; в) $P = '100009'$, KSumm = ?, SummKodBukvOtkr – ?; г) $P = '190000'$, KSumm = ?, SummKodBukvOtkr – ?

5 Листинг программы

```
<!DOCTYPE html>
```

```
<html>
```

```
<head>
```

```
<meta http-equiv="Content-type" content="text/html; charset=utf-8">
```

```
<meta http-equiv="Content-Security-Policy" content="default-src 'none'; style-src 'unsafe-inline'; img-src data;; connect-src 'self'">
```

```
<title>Page not found &middot; GitHub Pages</title>
```

```
<style type="text/css" media="screen">
```

```

body {
background-color: #f1f1f1;
margin: 0;
font-family: "Helvetica Neue", Helvetica, Arial, sans-serif;
}

.container { margin: 50px auto 40px auto; width: 600px; text-align: center; }

a { color: #4183c4; text-decoration: none; }
a:hover { text-decoration: underline; }

h1 { width: 800px; position: relative; left: -100px; letter-spacing: -1px; line-height: 60px; font-size: 60px; font-weight: 100; margin: 0px 0 50px 0; text-shadow: 0 1px 0 #fff; }

p { color: rgba(0, 0, 0, 0.5); margin: 20px 0; line-height: 1.6; }

ul { list-style: none; margin: 25px 0; padding: 0; }
li { display: table-cell; font-weight: bold; width: 1%; }

.logo { display: inline-block; margin-top: 35px; }
.logo-img-2x { display: none; }

@media
only screen and (-webkit-min-device-pixel-ratio: 2),
only screen and ( min--moz-device-pixel-ratio: 2),
only screen and ( -o-min-device-pixel-ratio: 2/1),
only screen and ( min-device-pixel-ratio: 2),
only screen and ( min-resolution: 192dpi),
only screen and ( min-resolution: 2dppx) {
.logo-img-1x { display: none; }

```

```
.logo-img-2x { display: inline-block; }  
}
```

```
#suggestions {  
margin-top: 35px;  
color: #ccc;  
}
```

```
#suggestions a {  
color: #666666;  
font-weight: 200;  
font-size: 14px;  
margin: 0 10px;  
}
```

```
</style>
```

```
</head>
```

```
<body>
```

```
<div class="container">
```

```
<h1>404</h1>
```

```
<p><strong>File not found</strong></p>
```

```
<p>
```

The site configured at this address does not
contain the requested file.

```
</p>
```

```
<p>
```

If this is your site, make sure that the filename case matches the URL.

For root URLs (like <code>http://example.com/</code>) you must provide an
<code>index.html</code> file.

</p>

<p>

Read the full documentation

for more information about using GitHub Pages.

</p>

<div id="suggestions">

GitHub Status —

@githubstatus

</div>

](#)

<img width="32" height="32" title="" alt="" src="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAEAAAABA CAYAAACQaXHeAAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFnZVJlYWR5ccllPAAAAyRpVFh0WE1MOmNvbS5hZG9iZS54bXAAAAAAADw/eHBhY2tldCBiZWdpbj0i77u/LiBpZD0iVzVNME1wQ2VoaUh6cmVTek5UY3prYzlk


[FVy4Plz8xKAGWjjAKFk6lCBMDR/MJjLLMSQNm43xAiQKTaA+9/wewhDjL+JVl1kkTSSOTcKbMTwPqESAot6dn6Fr1gHwVJju6IRuyiByPuUUBAg5DGkAgBmxlvdgIEK9gDkohdY/BJo4CAG0R8miRSsGABkgVQs4KXu098IgUXSSRsFAoKZiVAVDY2WUiiPTjYRi41KwGisrGsLtlsth8Fiwnz2fBkQvWfRtlE3iF2yW63/yCacXZ1dW02GwGyTFaRd4idJnCKHRaCxYRHoG5LTKT6SyiToP1fJHbmAYPYRR0UnZQtMnA6s0zg+GZBlT0Gdo7EPHgpE3Q6nZ8YyLhc8Xj8MJh/aKTAY+5FPAKHLE7RdwuYJZmNwzyCMkBCYyKROJBMJI9B/PXXCjmmCmDOVzH3fiPpObEWGqoKe4EBI8v1hlqsdLvd23mkxHM9pc9kMpmno9HoeTii7ewbHEZPPx1ztLS1tV3AnGuMjiNjvbQFuHw6zDo5By7dTPAQNBgMLrRarTkSlslmnwT7uwp9virx9QzbW/HuV/j5d/b+6jniKlIlP8lkeONJDk+dq9GsQTnC4fB1heO0K47Hwe7WdDr9nAKgXwOBwHI+C45HtjlD6sd429TUNEcmUdc+PRaLHcyn87dXW4ugzdsaGxufL94NFv9zi1J7GVbhlvb2dnaJ3SVrxfc+n2+NTsZ7/H7/Mr3g5XdSIHyJSH1PZ+7fToyl2+ErqilgZ4NaLYB9goVGaHjR93Hv1ZrU4XDsfT20kH3PObzbWk0CgG1jacVIUnAQb9F+VexyLMzkpcLv0IJV7AHQIOCAUYHx7v5qgScmYHtTqSAyZLEJTK22Bie4iq3xsqpm4SAf9Hq9a2DnJ4uLK3SEULcdRvp3i3zHySqpfixEdsQc1NrlYXXvR+O7qASSezXB+h1SuUomgg9LL8BUoV4749EIolKh+EiqWmqVEZIDgHks2pxHw7xTqUQw9J5NcAXOK10AGIoZ6Zli6JY6Z1Q461KoZ4NiKLHarW+KDsxlDUPHZ5zPQZqUVDPIsTqb5n9malbpAh8C2XXDLl62+WZIDFRUINVOiwencnNU3aQEKL+cDMSoLvZo2fQB7AJssNAuFuvorlDVVkk2I87+jo2K2QAVphDrfyViK5VqtO34OkaxXCp+7drdDBCAdubm6eidX+2WwqT5komwh4YQLk+H4aE93h8Xg2gvHekQZOGSgLTZTLyDTLJ4Lx9/KZWKBSainT4Iy3FqQBfnUZr42PKQFksBr9QKVXCPusD3OiA/RkQ5kP8qV/Jl1WywAp/6+dcmPM2zL1UrUahe4JqfnWWKXIul3uUbfP8njAFLW1OFr3gdFtZ72cNH+PtQT7/brW+NXqJAHh0y9V8/U/A1U7AfwIMAD7mS3pCbuWJAAAAAEIftkSuQmCC">](#)

</div>

</body>

</html>

6 Результат выполнения программы



- 1 Генератор паролей
- 2 Аутентификация
- 3 Оценка пароля
- 4 **Хеширование**
- Отчеты
- О нас

MTUCI.OIB

#

Хэширование

a=71, b=13, c=MaxVal+1=256, t0=144

Что хешируем? *

KSumm: undefined
SummKodBukvOtkr: undefined

MTUCI.OIB © и Копатыч и Лёха и Тема 2020.

7 Вывод

В процессе работы над лабораторной получены основные теоретические сведения и практические навыки по оценке стойкости парольной защиты.