# Лабораторна робота №2. дослідження сучасних стандартів шифрування

## Мета роботи

Ознайомитись з принципами побудови вітчизняного криптографічного стандарту шифрування «Калина». Виконати дослідження його особливостей.

## Порядок виконання роботи

1. Знайти в мережі Інтернет інформаційний опис українського стандарту *ДСТУ 7624:2014, що визначає шифр «Калина», його можливості, недоліки та переваги, режими роботи.*
2. Відшукати криптографічні бібліотеки, до складу яких включено шифр «Калина», освоїти особливості налагодження та запуску перетворення для ключів та розмірів блоків шифрування різної довжини.
3. Підібрати повідомлення, які потрібно зашифрувати та виконати дослідження з застосуванням алгоритмів, пропонованих у таблиці варіантів.
4. Дослідити можливість виконання шифрування та виконати заміри часу (у м/с) для кожного застосованого алгоритму з урахуванням можливостей ПК, на якому дослідження виконувались (технічні характеристики). Навести вхідне та шифровані повідомлення для кожного випадку.
5. Результати досліджень занести у таблицю та відобразити на діаграмі. Підготувати звіт.

**Вимоги до звіту:**

1. Титульний лист
2. Вступ (загальна інформація про стандарти шифрування)
3. Основний розділ, в якому надати:

- опис вітчизняного стандарту, його особливості, математичну модель, переваги та недоліки;

- інформацію про особливості дослідження, яке потрібно зробити згідно варіанта завдання, короткий опис алгоритмів, за якими буде виконуватися порівняння;

- загальні характеристики персонального комп’ютера, на якому проводиться дослідження та операційної системи, що застосовується;

- відомості про криптографічну бібліотеку, яка буде застосована при виконанні дослідження (інтернет-адреса для скачування, короткий опис, особливості роботи, особливості застосування);

- текст повідомлення (повідомлень), що підлягають шифруванню (у разі необхідності – опис структури цих повідомлень, як то – загальна кількість символів, мова та застосовані символи, розбиття на блоки й їх довжина;

4) Послідовність виконання експерименту;

5) короткий опис програмного забезпечення, за допомогою якого виконуються часові заміри;

6) Копії екранів, що підтверджують дослідження.

7) Порівняльні таблиці з результатами замірів, діаграми та мовний опис отриманих результатів.

8) Висновки.

**Таблиця варіантів для розробки**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Вар.** | **Довжина ключа шифру «Калина»** | **Розмір блоку** | **Алгоритми для порівняння** | | |
| **1** | **2** | **3** |
| **1** | **128** | **128** | AES-128 | Speck-128 |  |
| **2** | **256** | **128** | AES-256 | Belt | Threefish-256 |
| **3** | **256** | **256** | AES-256 | Threefish-256 | Kuznechik |
| **4** | **512** | **256** | AES-128 | Camellia | IDEA |
| **5** | **512** | **512** | Гост28147-89 | Blowfish | Threefish-512 |
| **6** | **128** | **128** | Belt | AES-128 | Speck-128 |
| **7** | **256** | **128** | Kuznechik | Cast-256 |  |
| **8** | **256** | **256** | Camellia | RC6 | AES-256 |
| **9** | **512** | **256** | Threefish-256 | IDEA | Гост28147-89 |
| **10** | **512** | **512** | Threefish-512 | Гост28147-89 | Camellia |
| **11** | **128** | **128** | Speck-128 | Kuznechik | AES-128 |
| **12** | **256** | **128** | RC6 | Belt | Cast-256 |
| **13** | **256** | **256** | Cast-256 | AES-256 | Гост28147-89 |
| **14** | **512** | **256** | Blowfish | Threefish--512 | Belt |
| **15** | **512** | **512** | IDEA | Гост28147-89 | Blowfish |

**Літературні джерела:**

1. Долгов В.И. Криптографические свойств а уменьшенной версии шифра «Калина» /*В.И. ДОЛГОВ, Р.В. ОЛЕЙНИКОВ, А.Ю. Большаков , А.В. ГРИГОРЬЕВ, Е.В. Дробатько //*Прикладная радиоэлектроника, 2010, Том 9, № 3, с. 349-354

2. Кузнецов А.А. МОДЕЛИРОВАНИЕ ПЕРСПЕКТИВНОГО БЛОЧНОГО ШИФРА «КАЛИНА» / *А.А. КУЗНЕЦОВ, Д.В. ИВАНЕНКО, Е.П. КОЛОВАНОВА //*Прикладная радиоэлектроника, 2014, Том 13, № 3, с.201-207

## Інтернет-посилання за темою:

<https://uk.wikipedia.org/wiki/Калина_(шифр)>

<http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=120158&cat_id=119123>

<https://www.slideshare.net/oliynykov/kalyna>

<https://habrahabr.ru/post/273895/>

<http://ko.com.ua/o_novom_ukrainskom_standarte_shifrovaniya_110863>

<https://github.com/Roman-Oliynykov/ciphers-speed>

<https://sourceforge.net/projects/cppcrypto/>  
<https://www.cryptopp.com/>  
<https://www.cryptopp.com/wiki/Kalyna>