Київський національний університет імені Тараса Шевченка
Механіко-математичний факультет
Теорія чисел та криптографія *2019/2020 н.р., 2 семестр*

Лабораторна робота 1. Шифр Віженера. Частотний криптоаналіз

Розглядаються тексти українською мовою. При аналізі текстів пробіли, цифри та знаки пунктуації ігноруються. Мінімальна довжина ключа — 5, максимальна — 32.

Завдання для аудиторної роботи

1.1 Шифр Віженера

а) Використовуючи ключ "*зима*", зашифруйте повідомлення "*весна красна колись прийде*".

б) Використовуючи цей же ключ, розшифруйте криптотекст "*ьччжпчьишисаєяйпявааьяч*".

в) Доведіть, що послідовне шифрування шифром Віженера з ключами K_1 і K_2 буде шифруванням цим же шифром з деяким ключем K_3. Знайдіть K_3.

г) Скільки існує різних ключів, у яких літери не повторюються?

1.2 Шифр з автоключем

а) Використовуючи ключ "*зима*", зашифруйте повідомлення "*весна красна колись прийде*".

б) Використовуючи цей же ключ, розшифруйте криптотекст "*єтишфжвлчишізшюяюшен*".

Завдання для самостійної роботи

С1.1 Побудуйте гістограму частот появи літер в тексті.

С1.2 Реалізуйте алгоритм шифрування Віженера.

С1.3 Проведіть криптоаналіз шифру Віженера і розшифруйте запропонований криптотекст.

Лабораторна робота 2. Скінченні поля. Симетричні криптосистеми.

Нехай $GF(2^8)$ — поле з 2^8 елементів, $GF(2^8) = \mathbb{Z}_2[x]/(x^8 + x^4 + x^3 + x + 1)$.

Завдання для аудиторної роботи

2.1 Конвертуйте в бітову, шістнадцятіркову та цілочисельну форми такі елементи поля $GF(2^8)$:

а) $x^7 + x^5 + x^2$;

б) $x^7 + x^6 + x^2 + x + 1$.

2.2 Виконайте вказані арифметичні дії над елементами поля $GF(2^8)$. Відповідь запишіть в тій же формі, в якій задано початкові елементи:

а) $\{10010111\} \cdot \{01010111\}$;

б) $\{d7\} + \{3c\}$;

в) $\{200\} \cdot \{100\}$.

2.3 Користуючись означенням перетворення `SubBytes`, обчисліть значення цього перетворення від байта:

а) $e5$;

б) $f1$.

2.4 Користуючись означенням перетворення `SubBytes`, знайдіть значення $\texttt{SubBytes}^{-1}$ від байта:

а) $e5$;

б) $f1$.

Завдання для самостійної роботи

С2.1 Реалізуйте криптосистему AES-128, включаючи алгоритми утворення раундових ключів, шифрування і дешифрування.

С2.2 Як змінюється криптотекст, якщо у початковому відкритому тексті змінити один біт?

С2.3 Реалізуйте потокові режими CBC та CTR криптосистеми AES-128.

Лабораторна робота 3. Криптографічні хеш функції.
Завдання для аудиторної роботи

3.1 Доповніть задане повідомлення до повідомлення, бінарна довжина якого кратна 128, використовуючи 5 методів доповнень. Для всіх заданих символів використовується ASCII кодування.

а) “`The quick brown fox jumps over the lazy dog`”;

б) “`Грішний джиґіт, що хотів у Францію, позбувався цієї думки, з’їдаючи трюфель`”;

в) “`Съешь же ещё этих мягких французских булок да выпей чаю`”.

3.2 Визначимо функцію $f : \{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ правилом

$$f(a,b) = \mathbf{Enc}_b(a) \oplus b, \quad a,b \in \{0,1\}^{128},$$

де $\mathbf{Enc}_b(a)$ позначає шифрування повідомлення a з ключем b в криптосистемі AES-128.

Введемо тепер хеш функцію H, яка довільне повідомлення M перетворює в хеш-суму $H(M)$ довжини 128 за таким правилом:

а) доповнити M до повідомлення $M_1 \dots M_t$, в якому кожен блок має довжину 128;

б) обчислити $S_1 = M_1$, $S_i = f(S_{i-1}, M_i), 2 \le i \le t$;

в) покласти $H(M) = S_t$.

Доведіть, що так побудована хеш функція не є стійкою ні до взяття прообразів, ні до колізій.

Завдання для самостійної роботи

С3.1 Реалізуйте хеш функцію SHA256.

С3.2 Реалізуйте алгоритм генерування секретного ключа криптосистеми AES-128 на основі хеш функції SHA256.

С3.3 Реалізуйте алгоритм створення і перевірки HMAC на основі хеш функції SHA256.

Лабораторна робота 4. Криптосистема RSA.
Завдання для самостійної роботи

С4.1 Реалізуйте тест простоти Міллера-Рабіна.

С4.2 Реалізуйте алгоритм ініціалізації RSA.

С4.3 Реалізуйте алгоритм шифрування RSA.

С4.4 Реалізуйте алгоритм дешифрування RSA.

С4.5 *Реалізуйте RSA-OAEP.