План лабораторного заняття № 2
Тема № 1 "Загальні аспекти захисту інформації"

Навчальний час: 2 год.
Міжпредметні зв'язки: навчальна дисципліна "Захист інформації в інформаційних системах" взаємопов'язана з такими дисциплінами як "Економіко-математичне моделювання", "Інформатика" та ін.
Мета і завдання лабораторного заняття: ознайомлення з функціями, що використовуються в теорії чисел та криптографії.

Питання для перевірки базових знань за темою лабораторного заняття:

1. Для чого в криптографії використовується функція Ейлера?
2. Назвіть властивості функції Ейлера.
3. В якому методі криптографії використовується функція Ейлера?
4. Як обчислюється функція Ейлера? Що таке факторизація7
5. Як звучить теорема Ейлера?

Завдання: автоматизувати процес обчислення функції Ейлера. Знайти функцію Ейлера для чисел 210, 80, 164, 346, 184.

Хід виконання лабораторної роботи:

Функція Ейлера – функція, що використовується в теорії чисел та криптографії, зокрема, при визначенні алгоритму RSA – криптографічного алгоритму з відкритим ключем. Останній базується на задачах факторизації великих цілих чисел.

Властивості функції Ейлера:
1) $\varphi(p^n) = (p-1)p^{n-1}$, де p – просте число;
2) $\varphi(mn) = \varphi(m)\varphi(n)$ (т.зв. «мультиплікативність» функції Ейлера);
3) $a^{\varphi(m)} \equiv 1 \pmod n$, де a та m – взаємно прості.
4) $\varphi(m^k) = m^{k-1}\varphi(m)$.

Функція Ейлера обчислюється на основі добутку:

$$\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right),$$

де p – всі прості числа, які діляться на n.

Інакше кажучи, функцію Ейлера можна отримати, використовуючи факторизацію:

якщо $n = p_1^{a1} \cdot p_2^{a2} \cdot \ldots p_k^{ak}$ (p – прості числа),

то значення функції Ейлера знаходять з:

$$\begin{aligned}&\phi(n) = \phi(p_1^{a_1}) \cdot \phi(p_2^{a_2}) \cdot \ldots \cdot \phi(p_k^{a_k}) = \\ &= (p_1^{a_1} - p_1^{a_1-1}) \cdot (p_2^{a_2} - p_2^{a_2-1}) \cdot \ldots \cdot (p_k^{a_k} - p_k^{a_k-1}) = \\ &= n \cdot \left(1-\frac{1}{p_1}\right) \cdot \left(1-\frac{1}{p_2}\right) \cdot \ldots \cdot \left(1-\frac{1}{p_k}\right).\end{aligned}$$

Нижче наведено деякі значення функції Ейлера:

Таблиця 1

Значення функції Ейлера для деяких чисел

$\varphi(n)$	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Додаткові завдання для студентів: опрацювання теоретичного матеріалу теми, написати план-конспект заняття за вибраною темою із використанням демонстраційного матеріалу.
Форми контролю знань – презентація виконаних завдань, перевірка коду програми, обговорення виконаних завдань.

Рекомендована література до теми лабораторного заняття:
Основна та допоміжна література:
1. Харин Ю.С. Математические основы криптологии: учеб.пособ. / Ю.С.Харин, В.И.Берник, Г.В.Матвеев. – Мн.: БГУ, 1999. – 319 с.
2. Зима В. Безопасность глобальных сетевых технологий / В.Зима, А.Молдован, Н.Молдован. – СПб.: БХВ-Петербург, 2003. – 368 с.
3. Щербаков А. Прикладная криптография / А. Щербаков, А.Домашев. – М., 2003. – 404 с.
4. Пономаренко Н.Н. Защита информации в телекоммуникационных системах: учеб. пособ. / Н. Н. Пономаренко. – Х.: Нац. аэрокосм. ун-т им. Н.Е. Жуковского «Харьк.авиац.ин-т», 2015. – 40 с.
5. Алферов А.П. Основы криптографии: учеб. пособ. / А.П.Алферов, А.Ю.Зубов, А.С.Кузьмин,
6. А.В.Черемушкин. – М.: Гелиос АРВ, 2002 – 480 с.
7. Басалова Г.В. Основы криптографии / Г.В. Басалова. – М.: Национальный Открытый Университет "ИНТУИТ", 2016. – 283 с. URL: https://www.twirpx.com/file/1907188/

Інтернет-ресурси:
https://books.ifmo.ru/file/pdf/56.pdf
http://booksshare.net/index.php?id1=4&category=cryptography&author=alferov-ap&book=2002

Обладнання заняття, ТЗН тощо: комп’ютери.

Укладач:_____ Задорожна А. В., доцент кафедри цифрової економіки та бізнес-аналітики
(підпис) (ПІБ, посада, науковий ступінь, вчене звання)