СИЛАБУС
Кафедра кібербезпеки та математичного моделювання

Назва курсу	Методи побудови та аналізу криптосистем
Мова викладання	українська
Викладач (-і)	Шелест М.Є., професор кафедри кібербезпеки та математичного моделювання, д.пед.н., доцент
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/ ORCID 0000-0001-7110-4876
Контакти викладача	mishel3141@gmail.com

1. **Анотація курсу** -

Протягом багатьох років людство цікавила можливість обміну повідомленнями, які містили ту чи іншу інформацію.

У той же час існує коло людей, які зацікавлені в тому, щоб із змістом, що міститься в їх повідомленнях, могли ознайомитись тільки ті люди, для яких воно призначено. Тому люди почали придумувати шифри з того часу, як тільки захотіли вперше щось приховати.

У даному курсі, висвітлюються питанням криптографічного захисту інформації, зокрема::

° основи класичної криптографії;

° принципи побудови сучасних криптосистем з секретним і відкритим ключем;

° методи контролю цілісності та автентичності інформації, в тому числі протоколи аутентифікації і електронного підпису;

° проблеми і перспективи розвитку криптографічних методів захисту.

Змістовний модуль 1. Симетричні криптографічні перетворення

Тема 1. Основи теорії секретних систем (конфіденційності).

Основні поняття криптології. Криптографічні перетворення, класифікація та основні властивості. Основні послуги криптографічних систем захисту інформації. Математичні моделі джерел відкритих повідомлень та криптограм. Загальні умови реалізації та класифікація крипто аналітичних атак. Теоретично (безумовно) стійкі криптографічні системи (шифри) та умови їх реалізації.

Тема 2. Симетричні криптографічні перетворення та їх властивості.

Симетричні перетворення, класифікація та їх властивості. Афінні шифри та їх властивості. Основні елементарні симетричні криптографічні перетворення та їх властивості. Складність симетричних криптографічних перетворень. Методи оцінки криптографічної стійкості симетричних крипто перетворень. Блокові симетричні шифри та їх властивості. Потокові симетричні шифри та їх властивості. Модель криптографічно захищеної телекомунікаційної системи на основі застосування блокових симетричних шифрів. Модель криптографічно захищеної інформаційно-телекомунікаційної системи на основі застосування потокових симетричних шифрів.

Тема 3. Джерела ключів та ключової інформації, вимоги до них.

Джерела ключів та ключової інформації, вимоги до них. Випадкові та псевдовипадкові послідовності та їх властивості. Генерування випадкових та псевдовипадкових послідовностей. Критерії та показники оцінки властивостей випадкових послідовностей. Вимоги відносно необоротності, непередбачуваності, нерозрізнюваності та складності генерування ключів та ключової інформації.

Змістовний модуль 2. Асиметричні криптосистеми

Тема 4. Вступ в теорію асиметричних криптоперетворень.

Асиметричні крипто перетворення. Класифікація та загальна характеристика. Направлені шифри, що реалізуються в кільцях та простих полях Галуа. Загальні підходи та оцінка складності та стійкості крипто перетворень в кільцях та простих полях Галуа.

Тема 5. Асиметричні криптоперетворення в групах точок еліптичних кривих.

Асиметричні перетворення в групі точок еліптичних кривих та гіпереліптичних кривих, їх основні властивості. Базиси представлення та метрики операцій скалярного множення. Афінний та проективні базиси, порівняльний аналіз складності виконання операцій. Направлені шифри, що реалізуються в групі точок еліптичних кривих. Сертифікати відкритих ключів шифрування. Оцінка стійкості та складності криптографічних перетворень в групі точок еліптичних кривих та гіпереліптичних кривих.

Тема 6. Джерела ключів асиметричних криптосистем та вимоги до них.

Джерела ключів асиметричних криптосистем та вимоги до них. Двох ключові криптографічні (асиметричні) перетворення. Простір ключів. Методи та засоби генерування ключів для асиметричних крипто перетворень в кільцях, полях, групах точок еліптичних кривих та парних відображень. Критерії та показники оцінки властивостей ключів. Вимоги відносно необоротності, непередбачуваності, нерозрізнюваності та складності генерування ключів та ключової інформації.

Змістовний модуль 3. Криптографічні механізми та протоколи

Тема 7. Криптографічні протоколи

Визначення криптографічного протоколу. Класифікація криптографічних протоколів. Інтерактивні та протоколи з нульовими знаннями (PVS протоколи). Криптографічні протоколи на основі застосування ЕЦП. Протоколи з ЕЦП та шифруванням. Методи та приклади доведення безпечності криптографічних протоколів.

Тема 8. Криптографічний аналіз симетричних криптосистем

Методи крипто аналізу в симетричних криптосистемах. Методи брутальної сили та на основі створення колізій. Алгебраїчні методи. Складність складання та розв’язку систем рівнянь. Статистичні та ймовірнісні методи. Розв’язок систем рівнянь з випадковою правою частиною.

Тема 9. Криптографічний аналіз асиметричних криптосистем

Методи та алгоритми крипто аналізу асиметричних криптосистем в кільцях, полях та групах точок еліптичних і гіпереліптичних кривих. Оцінка складності та вартості. Квадратичне та решето загального числового поля.

Методи розв’язання дискретних логарифмів та їх застосування при крипто аналізі в полях.

2. Мета та цілі курсу -

Метою викладання дисципліни є формування компетентності майбутніх спеціалістів в галузі сучасних технологій криптографічного захисту інформації в комп’ютерних системах

Завданнями вивчення навчальної дисципліни є:

- розгляд основних етапів історичного розвитку криптографії;
- поглиблення теоретичних знань про основні методи криптографічного захисту інформації;
- розгляд математичних моделей симетричних шифрів та їх властивостей;
- удосконалення способів шифрування даних;
- застосування методів асиметричної криптографії;
- дослідження особливостей криптографічних алгоритмів та криптографічних протоколів;
- ознайомлення з основними положеннями нормативно-правового регулювання у галузі КЗІ;
- розгляд основних напрямків розвитку сучасних систем КЗІ;
- отримати знання про загрози безпеки інформаційних ресурсів, методи та стратегії, що реалізовані для управління процесу усунення несанкціонованого доступу з боку сторонніх користувачів;
- засвоїти методику і напрями використання сучасних криптографічних алгоритмів розподілу ключів і цифрового підпису;
- набути уміння та навички програмування криптографічних алгоритмів.

Отже, за результатами вивчення дисципліни буде забезпечено:

Програмні компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 1. Здатність розробляти та впроваджувати законодавчу, нормативно-правову базу, державні і міжнародні вимоги, а також інтегрувати, аналізувати і використовувати сучасні світові практики та стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

КФ 2. Здатність розробляти, впроваджувати і супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах (автоматизованих систем та їх додатків) та у інфраструктурі організації в цілому.

КФ 9. Здатність розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного

захисту інформації на об’єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації.

3. Результати навчання –

У результаті вивчення навчальної дисципліни студент повинен:

Знати:

- основні криптографічні алгоритми симетричного шифрування;
- основні криптографічні алгоритми асиметричного шифрування та цифрового підпису;
- стандартні криптографічні примітиви та порядок їх застосування при захисті інформації з обмеженим доступом;
- методи аналізу стійкості криптографічних систем та засобів криптографічного захисту інформації;
- типові вимоги до систем та засобів управління ключовими даними;
- базові стандарти в галузі криптографічного захисту інформації.

Вміти:

працювати з технічною літературою і документацією;

- моделювати (проектувати) алгоритми криптографічних перетворень та елементи криптографічного аналізу на комп’ютері;
- обґрунтувати та пропонувати стандартні криптографічні системи, криптографічні примітиви та протоколи захисту та ресурсів в комп′ютерних системах та комп′ютерних мережах;
- здійснювати загальну оцінку якості криптографічного захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, що реалізовані з використанням засобів обчислювальної техніки;
- визначати системи й методи захищеності носіїв інформації;
- створювати засобами стандартного програмного забезпечення елементи захисту інформації.

Програмні результати навчання (ПРН)

ПРН 3 - використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН 4 - аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

ПРН 6 - діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, в тому числі міжнародних в галузі інформаційної та/або кібербезпеки.

ПРН 14 - розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації.

4. Обсяг курсу. Зазначте загальку кількість кредитів, кількість занять та годин самостійної роботи

Вид заняття	Загальна к-сть годин
лекції	16
лабораторні	14
самостійна робота (РГР)	90

4. Пререквізити -

Вивчення дисципліни «Методи побудови та аналізу криптосистем» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів «Вища математика», «Спеціальні глави математики», «Основи програмування», «Основи криптографічного захисту інформації».

6. Система оцінювання та вимоги

Оцінювання проводиться за 100-бальною шкалою.

Бали нараховуються за наступним співвідношенням:

• лабораторні роботи : 20% семестрової оцінки;

• домашні завдання: 20% семестрової оцінки;

•РГР: 20% семестрової оцінки;

• іспит: 40% семестрової оцінки.

7. Політики курсу -

Політика щодо академічної доброчесності: Списування під час контрольних робіт заборонені (в т.ч. із використанням мобільних девайсів). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки лабораторних завдань.

Жодні форми порушення академічної доброчесності не толеруються. У випадку таких подій – реагування відповідно до Положення про академічну доброчесність студентів та науково-педагогічних працівників Чернігівського національного технологічного університету та Методичних рекомендацій для закладів вищої освіти з підтримки принципів академічної доброчесності

Правила перезарахування кредитів у випадку мобільності, правила перескладання або відпрацювання пропущених занять тощо: відбувається згідно з Положення про організацію освітнього процесу в ЧНТУ.

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів за вид діяльності балів).

Перескладання модулів відбувається за наявності поважних причин (наприклад, лікарняний).

Політика щодо відвідування: Відвідування занять є обов’язковим компонентом оцінювання. За об’єктивних причин (наприклад, хвороба, працевлаштування, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням.

8. Рекомендована література

Базова

1. О.В.Вербіцький. Вступ до криптології. Видавництво НТЛ., Львів, 2008, с.248.
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф.Шаньгина, - М.: Радио и связь, 2007. -328 с.
3. Баричев С.Г., Серов Р.Е. Основы современной криптографии. – М.: Радио и связь, 2015. – 152 с.
4. Молдовян А.А., Молдовян В.А., Советов В.Я. Криптография. – Серия “Учебники для вузов. Специальная литература”. – Спб.: Издательство “Лань”, 2006. – 224 с.
5. Столлингс В. Криптография и защита сетей: принципы и практики, 2-е изд.: Пер. с англ. – М.: Изд. дом «Вильямс», 2007. – 672 с.
6. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. – К.: Корнійчук, 2011. – 152 с.
7. А.О.Антонюк. Основи захисту інформації в автоматизованих системах. – К.: КМ Академія, 2006. – 244 с.
8. А.Ю.Щеглов. Защита компьютерной информации от несанкционированного доступа. НиТ:Санкт-Петербург, 2004.
9. Hoffstein J. An Introduction to Mathematical Cryptography / J. Hoffstein, J. Pipher, J. Silverman. - Springer Science+Business Media, LLC, 2008. – 524 p.
10. Jeffrey H. An Introduction to Mathematical Cryptography / H. Jeffrey, P. Jill, H. Joseph. – Berlin: Springer, 2008. – 540 p.
11. Задірака В.К. Комп’ютерна криптологія / В.К.Задірака, О.С. Олексюк. – Тернопіль, Київ, 2002. – 504 с.
12. Фергюссон Н. Практическая криптография / Н. Фергюссон, Б. Шнайер. – М.: Вильямс, 2005. – 424 с.
13. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2006. – 336 с.
14. Николайчук Я.М. Теорія джерел інформації / Я.М. Николайчук // Видання друге, виправлене, – Тернопіль: ТзОВ “Терно-граф”, 2010. – 536 с.
15. Ян С. Криптоанализ RSA / С. Ян. — Ижевск: РХД. 2011. — 312 с.
16. Srivastava A. The Rabin cryptosystem and analysis in measure of chinese reminder theorem / A. Srivastava, A. Mathur // International Journal of Scientific and Research Publications. – 2013. – Vol. 3 (6). – P. 1-4.
17. Hayder R.H. H-Rabim Cryptosystem / R.H. Hayder // Journal of Mathematics and Statistics. - 2014. – Vol. 10 (3). – P. 304-308.
18. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. – М.: ТВП. – 2001. – 254с.

Допоміжна

Бембо Мао. Современння криптографія. Теорія и практика. Москва. 2005.

Домарев В.В.. Безопасность информационных технологий. Методология создания систем защиты. — К.: ООО “ДС”, 2001. 688 с.

Казарин О.В. Теория и практика защиты программ. М.: МГУЛ, 2003. 450 с.

Смарт Н. Криптография / С.А. Кулешова (пер.с англ.). - М. : Техносфера, 2006. - 519с.

Столлингс В. Криптография и защита сетей: принципы и практика. 3-е издание. –М: Издательский дом «Вильямс», 2010. –672 с.

Фергюсон Нильс, Шнайер Брюс. Практическая криптография / Н.Н. Селина (пер.с англ.). - М.; СПб.; К. : Диалектика, 2015. - 421с.

Харин Юрий Семенович, Берник Василий Иванович, Матвеев Геннадий Васильевич, Агиевич Сергей Валерьевич. Математические и компьютерные основы криптологии : Учеб. пособие для студ. мат. и инж.-техн. спец. вузов - Минск : ООО "Новое знание", 2013. - 382с.

Інформаційні ресурси

Новітні теоретичні та практичні дані та матеріали? що стосуються теорії та практики захисту інформації рекомендується відслідковувати засобом звертання до наступних сайтів.

1. http://www.rsasecurity.com
2. http://www.nist.gov
3. http://www.eprint.iacr.org
4. http://www.citeseer.ist.psu.edu
5. http://www.ansi.org
6. http://www.cryptography.org
7. http://www.iso.org
8. http://www.linuxiso.org
9. http://www.cryptography.com
10. http://www.springerlink.com
11. http://www.cacr.math.uwaterloo.ca
12. http://www.financialcryptography.com
13. http://www.austinlinks.com
14. http://world.std.com/~franl/crypto.html
15. http://www.cryptonessie.org
16. http://www.cryptography.ru
17. http://www.osti.gov/eprints
18. http://www.intel.com
19. http://www.msdn.com
20. http://www.ph4s.ru/book_kripto.html