



ARX-КРИПТОСИСТЕМИ ТА ЇХ КРИПТОАНАЛІЗ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Другий (магістерський)</i>
Галузь знань	<i>11 Математика та статистика</i>
Спеціальність	<i>113 Прикладна математика</i>
Освітня програма	<i>Математичні методи криптографічного захисту інформації</i>
Статус дисципліни	<i>Вибіркова</i>
Форма навчання	<i>Очна (денна)</i>
Рік підготовки, семестр	<i>2 курс, осінній семестр</i>
Обсяг дисципліни	<i>Загальна кількість: 4 кредита ЕКТС / 120 годин Лекційних занять: 18 годин Практичних занять: 18 годин Самостійна робота студентів: 84 години</i>
Семестровий контроль/ контрольні заходи	<i>Залік, МКР, індивідуальне завдання</i>
Розклад занять	http://schedule.kpi.ua
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>доц. Яковлев Сергій Володимирович, к.т.н. (yasv@ri.kiev.ua) ас. Корж Нікіта Сергійович</i>
Розміщення курсу	<i>Google Classroom</i>

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Навчальна дисципліна «ARX-криптосистеми та їх криптоаналіз» присвячена так званим ARX-системам та ARX-архітектурі (від Add-Rotation-XOR – трьох основних операцій у структурі криптографічних перетворень), які наразі широко використовуються у системах криптографічного захисту «Інтернету речей». Розглядаються алгебраїчні аспекти ARX-систем та методи побудови криптографічних атак (в першу чергу диференціального та обертального криптоаналізу), а також застосування теорії S-функцій та автоматних моделей для автоматизованої побудови атак на ARX-системи.

Основною метою дисципліни є формування у студентів глибокого розуміння сучасних напрямків криптології, зокрема, підходів щодо використання алгебраїчних та статистичних методів криптоаналізу, а також для оцінювання ризиків безпеки. Для досягнення мети передбачається опрацювання значної кількості розрахункових та аналітичних задач, які ілюструють та розширюють лекційний матеріал, та виконання індивідуального завдання.

У результаті вивчення курсу студент повинен:

- знати основні підходи до побудови малоресурсних криптографічних алгоритмів;

б) вмiти будувати статистичнi атаки на малоресурснi алгоритми та одержувати аналітичнi чи розрахунковi оцiнки стiйкостi до таких атак.

Одержанi знання та умiння посилюють такi компетентностi та результати навчання, визначенi освітньою програмою:

ФК 5 Здатнiсть провадити теоретичний та практичний аналіз сучасних криптографiчних систем

ФК 6 Здатнiсть розроблювати новiтнi механiзми криптографiчного захисту

РН 11 Провадити аналіз криптографiчних алгоритмiв, протоколiв та систем

РН 12 Орієнтуватись у останнiх досягненнях криптологiї

РН 13 Розроблювати новi криптографiчнi алгоритми, механiзми та системи захисту

2. Пререквiзити та постреквiзити дисциплiни (мiсце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Дана дисциплiна є доповненням до дисциплiн «Методи криптоаналiзу» та «Методи реалiзацiї криптографiчних алгоритмiв» та поширює i поглиблює відповіднi компетентностi та результати навчання. Однак матерiал курсу можна вивчати i без прив'язки до зазначених дисциплiн; обов'язковим для опанування є базовi знання з алгебри, дискретної математики, теорiї iмовiрностей та математичної статистики, а також розумiння основних концепцiй криптологiї.

Головний фокус дисциплiни зосереджений на теоретичних засадах криптологiї як наукової галузi та їх iмплементацiї у статистичних та алгебраїчних методах криптоаналiзу. Отриманi навички та засвоєннi знання можуть використовуватись для проведення наукових та прикладних дослiджень у галузi криптологiї, а також для розв'язання прикладних задач у галузi криптографiчного захисту iнформацiї.

Опанування даного курсу посилює знання, навички та умiння, якi надаються такими дисциплiнами, як «Методи криптоаналiзу», «Методи реалiзацiї криптографiчних механiзмiв».

3. Змiст навчальної дисциплiни

Роздiл 1. ARX-криптосистеми

Тема 1.1. Означення ARX-криптосистем та їх опис.

Роздiл 2. Методи криптоаналiзу ARX-криптосистем

Тема 2.1. Обертальний криптоаналiз ARX-криптосистем.

Тема 2.2. Диференціальний криптоаналiз ARX-криптосистем.

Роздiл 3. Автоматнi моделi ARX-криптосистем

Тема 3.1. S-функцiї та їх застосування у криптоаналiзi ARX-криптосистем.

4. Навчальнi матерiали та ресурси

Рекомендована лiтература

1. Aumasson, J.P., Jovanovic, P., Neves, S.: Analysis of NORX: Investigating differential and rotational properties. Cryptology ePrint Archive, Report 2014/317 (2014) <http://eprint.iacr.org/>.

2. Thomas Berson. Differential cryptanalysis mod 232 with applications to MD5. In Advances in Cryptology—Eurocrypt 1992, volume 658 of LNCS, pages 71–80. Springer-Verlag, 1992.

3. Alex Biryukov and Vesselin Velichkov. Automatic Search for Differential Trails in ARX Ciphers (extended version)

4. M. Daum. Cryptanalysis of Hash Functions of the MD4-Family. PhD thesis, Ruhr-Universit'at Bochum, 2005

5. D. Khovratovich and I. Nikolic. Rotational Cryptanalysis of ARX. In S. Hong and T. Iwata, editors, FSE, volume 6147 of Lecture Notes in Computer Science, pages 333–346. Springer, 2010
6. G. Leurent. Analysis of differential attacks in ARX constructions. In X. Wang and K. Sako, editors, Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings, volume 7658 of Lecture Notes in Computer Science, pages 226–243. Springer, 2012
7. H. Lipmaa and S. Moriai. Efficient Algorithms for Computing Differential Properties of Addition. In M. Matsui, editor, FSE, volume 2355 of LNCS, pages 336–350. Springer, 2001.
8. Helger Lipmaa. On differential properties of Pseudo-Hadamard transform and related mappings. In Progress in Cryptology—Indocrypt 2002, volume 2551 of LNCS, pages 48–61. Springer-Verlag, 2002.
9. H. Lipmaa, J. Wallén, and P. Dumas. On the Additive Differential Probability of Exclusive-Or. In B. K. Roy and W. Meier, editors, FSE, volume 3017 of LNCS, pages 317–331. Springer, 2004.
10. N. Mouha, V. Velichkov, C. De Cannière, and B. Preneel. The Differential Analysis of S-Functions. In A. Biryukov, G. Gong, and D. R. Stinson, editors, Selected Areas in Cryptography, volume 6544 of Lecture Notes in Computer Science, pages 36–56. Springer, 2010.
11. V. Velichkov, N. Mouha, and C. D. B. Preneel. UNAF: A Special Set of Additive Differences with Application to the Differential Analysis of ARX. In A. Canteaut, editor. Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers, volume 7549 of Lecture Notes in Computer Science. Springer, 2012, pages 287–305.
12. Vesselin Velichkov. Recent Methods for Cryptanalysis of Symmetric-key Cryptographic Algorithms (PhD Thesis) 2012
13. Johan Wallén. Linear approximations of addition modulo 2^n . In Fast Software Encryption 2003, volume 2887 of LNCS, pages 261–273. Springer-Verlag, 2003.
14. Shafi Goldwasser, Mihir Bellare. Lecture Notes on Cryptography [електронний ресурс]. – 2008.
15. Oded Goldreich. Foundations of Cryptography [електронний ресурс]. – 1995.

Відеозаписи більшої частини лекцій викладені на Youtube-каналі кафедри ММЗІ та доступні за посиланням

<https://www.youtube.com/playlist?list=PLhCN8H4P5LvhdD8oXciqd4-sIPwmMhVNR>

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчання здійснюється на основі студентоцентрованого підходу та взаємодії викладачів та студентів для засвоєння матеріалу та опанування практичних навичок. При викладанні дисципліни використовуються такі методи навчання: для лекційних занять – пояснювально-ілюстративний метод та метод проблемного викладу; для практичних занять – пояснювально-ілюстративний метод, репродуктивний метод та метод проблемного викладу. Захист індивідуального завдання передбачає використання дискусійного методу.

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
1	ARX-криптосистеми. Повнота ARX-базису
2	Обертальний криптоаналіз ARX-криптосистем

3	Диференціальні імовірності ARX-криптосистем за операцією побітового додавання
4	Матрична форма диференціальних імовірностей ARX-криптосистем. Диференціальні імовірності ARX-криптосистем за операцією модульного додавання
5	Диференціальні імовірності операцій циклічного та нециклічного зсуву
6	Бінарні знакові різниці та NAF-форми
7	S-функції та їх диференціальний криптоаналіз
8	Криптоаналіз складних S-функцій
9	LRX-криптосистеми та їх криптоаналіз

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1	Реалізація операцій у ARX-базисі
2	Властивості пар обертання
3	Властивості диференціальних імовірностей ARX-перетворень
4	Властивості диференціальних імовірностей ARX-перетворень МКР, частина 1.
5	Побудова матричних форм диференціальних імовірностей
6	Властивості бінарних знакових різниць та NAF-форм
7	Побудова S-функцій
8	МКР, частина 2. Захист індивідуального завдання
9	Залік

6. Самостійна робота студента

Студент повинен завчасно готуватись до лекцій та практичних занять. Перед лекціями необхідно повторити теоретичний матеріал, наданий у попередніх лекціях. Перед практичними заняттями необхідно повторити відповідний теоретичний матеріал.

Обов'язковим є виконання домашніх завдань, які необхідно виконувати до наступного практичного заняття. Виконання та ревізія виконаних домашніх завдань також необхідні для підготовки до самостійних та модульних контрольних робіт.

З метою кращого засвоєння матеріалу курсу, а також формування навичок самостійної роботи студентам пропонується виконати індивідуальне завдання на тему побудови S-функції для обчислення заданого типу диференціальних імовірностей ARX-перетворень. Для підготовки до виконання індивідуального завдання слід скористатися рекомендованою літературою, конспектом та/або відеозаписами лекцій. Студенту надається не менше двох тижнів на виконання індивідуального завдання.

Розподіл годин самостійної роботи студента

№	Вид самостійної роботи	Годин СРС
1.	Опанування лекційного матеріалу	18
2.	Підготовка до практичних занять	18
3.	Виконання домашніх завдань	18
4.	Підготовка до виконання модульної контрольної роботи	4
5.	Виконання індивідуального завдання	20
6.	Підготовка до заліку	6
	Усього	84

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Студентам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються необхідні навички. Система оцінювання орієнтована на отримання балів за виконання завдань, які здатні розвинути практичні уміння та навички. Матеріал занять, які були з тих чи інших причин пропущені, необхідно опановувати самостійно.

Пропущені контрольні заходи

Студент, який без поважних причин пропустив частину МКР, одержує за неї нуль балів без можливості перескладання. Якщо пропуск стався з поважних причин (наприклад, хвороби), студент має можливість написати контрольний захід в інший узгоджений з викладачем термін без зниження оцінки. Повторне написання будь-якої частини модульної контрольної роботи не допускається.

Пропущений залік (за необхідності його складати) не зараховується незалежно від причин пропуску; у такому випадку студент отримує оцінку, сформовану на основі його семестрового рейтингу, та повинен складати залік на додатковій сесії.

Оголошення результатів контрольних заходів

Результати модульної контрольної роботи вказуються на бланках для модульної контрольної роботи (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо.

Результати письмової частини заліку вказуються на бланках для письмової залікової роботи (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо. Результати усної частини заліку оголошуються наприкінці її проходження.

Академічна доброчесність

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

У разі виявлення порушень норм академічної доброчесності під час виконання контрольного заходу студент одержує за цей захід нуль балів без можливості повторного виконання.

Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

Процедура оскарження результатів контрольних заходів

Студенти мають можливість підняти будь-яке питання, яке стосується процедури проведення та/або оцінювання контрольних заходів, та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами.

Студенти мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оціночного листа та/або зауважень.

8. Види контролю та рейтингова система оцінювання результатів навчання (PCO)

№	Контрольний захід	Макс бал	Ваговий бал	Кіл-ть	Усього
1.	Модульна контрольна робота	70	1	1	70
2.	Індивідуальне завдання	30	1	1	30
	Усього				100

Критерії оцінювання контрольних заходів

1) Модульна контрольна робота

Модульна контрольна робота (МКР) складається з декількох частин, які проводяться протягом семестру по мірі опанування теоретичного та практичного матеріалу. Кількість задач та їх вартість у балах визначається викладачами в залежності від складності самої задачі та об'єму винесеного на дану частину МКР матеріалу.

Критерії оцінювання однієї задачі МКР:

- Правильне повне розв'язання без помилок 100% оцінки
- Розв'язання з несуттєвими помилками та/або описками 90-99% оцінки
- Розв'язання з деякими неточностями 70-89% оцінки
- Розв'язання із правильною ідеєю, але грубими помилками 50-69% оцінки
- Наявність правильної ідеї розв'язку з неправильним її застосуванням або незакінченим розв'язком 30-49% оцінки
- Розв'язок повністю неправильний або відсутній 0% оцінки

Студент, який без поважних причин пропустив частину МКР, одержує за неї нуль балів без можливості перескладання. Виконання частини МКР, пропущеної з поважних причин, врегульовується за домовленістю з викладачем в індивідуальному порядку.

Максимальна кількість балів, яку можна одержати за модульну контрольну роботу, дорівнює 70. Загальна кількість балів, яку студент одержує за одну частину модульної контрольної, дорівнює сумі балів за кожне завдання у відповідності до їх вартості та наведених критеріїв оцінювання. Загальна кількість балів, яку студент одержує за модульну контрольну роботу, дорівнює сумі балів за виконання усіх її частин.

2) Індивідуальне завдання (розрахункова робота)

Індивідуальне завдання (розрахункова робота, РР) складається з декількох завдань. Кожен студент одержує своє індивідуальне завдання для виконання. Кількість задач та їх вартість у балах визначається викладачами та наводиться у завданні на РР. Оцінювання РР складається з двох етапів: безпосереднього виконання студентом індивідуального завдання та його захист у викладача; кожна частина дає до 50% від оцінки за кожну задачу РР.

Критерії оцінювання одного завдання РР:

- Повне розв'язання без помилок, правильна відповідь 50% оцінки
- Правильне розв'язання із неправильною відповіддю через неточності та арифметичні помилки 25-49% оцінки
- Розв'язання із правильною ідеєю, але грубими помилками 10-24% оцінки
- Розв'язок повністю неправильний або відсутній 0% оцінки

Критерії оцінювання захисту одного завдання РР:

- Студент демонструє вичерпне розуміння наведеного розв'язку та відповідного теоретичного матеріалу 50% оцінки
- Студент відповідає з неточностями та помилками 30-49% оцінки

- Відповідь студента містить окремі вірні положення 10-29% оцінки
- Студент демонструє повне незрозуміння теоретичного матеріалу та наведеного розв'язку 0 балів за завдання

Максимальна кількість балів, яку можна одержати за виконання та захист РР, дорівнює 30.

Здача РР після призначеного терміну виконання без поважної причини приводить до зниження оцінки за неї на 1 бал за кожен день запізнення; максимальне зниження оцінки за пропуск дедлайну – 6 балів. Через сім днів після дедлайну РР вважається невиконаною та автоматично оцінюється у 0 балів.

Заохочувальні бали

Студент, який протягом семестру виступив на науковій конференції із публікуванням доповіді (у вигляді матеріалів чи доповідей конференції) за тематикою дисципліни або подав таку доповідь та одержав підтвердження про включення в програму конференції, одержує 10 бонусних балів.

Загальна кількість заохочувальних балів, які можна одержати за дисципліну: 10 балів.

Умови одержання проміжної атестації

Проміжна атестація студентів (далі – атестація) є календарним рубіжним контролем та проводиться двічі за семестр, на 7-му та 13-му навчальному тижнях семестру. Для одержання кожної атестації поточний рейтинг студента повинен бути не менше половини від суми максимальних балів за усі контрольні заходи, які були проведені на момент атестації.

Умови одержання семестрової оцінки

Необхідною умовою одержання семестрової оцінки є семестровий рейтинг не менше 60 балів.

Студенти, які не одержали позитивну оцінку за результатами роботи у семестрі (але при цьому їх семестровий рейтинг складає не менше 10 балів), та студенти, які не погоджуються із такою оцінкою, виконують залікову роботу. При цьому їх семестровий рейтинг анулюється, а рейтингова оцінка виставляється по результату виконання залікової роботи.

Студенти, які набрали від 50 до 60 балів за семестр, за бажанням замість написання залікової роботи можуть пройти усну співбесіду із викладачем за матеріалами курсу. На співбесіді, відповідаючи на теоретичні питання (до десяти питань, одне питання = один бал), студент може підвищити свій семестровий рейтинг до мінімальної позитивної оцінки.

Студенти, які протягом семестру одержали менше 10 балів, вважаються такими, що не виконали умови одержання семестрової оцінки, та рекомендуються кафедрі на відрахування або повторне переслуховування дисципліни.

Умови проведення залікової роботи

Право писати залікову роботу мають:

- а) студенти, семестровий рейтинг яких складає 10-59 балів;
- б) студенти, семестровий рейтинг яких складає 60-100 балів, але які не згодні з одержаною семестровою оцінкою.

Студентам, які пишуть залікову роботу, анулюється семестровий рейтинг. Оцінка, яку вони одержують за дисципліну, формується за результатами складання залікової роботи.

Залікова робота проводиться на заліковому тижні в кінці семестру.

Залікова робота складається з 8 задач, які сумарно оцінюються в 100 балів. Критерії оцінювання задач практичної частини співпадають з критеріями оцінювання задач МКР.

Під час виконання залікової роботи забороняється використання будь-яких додаткових довідкових матеріалів.

Перескладання дисципліни

Перескладання дисципліни проходить у такій само формі, як і залікова робота. Для допуску до перескладання студент повинен одержати не менше 10 рейтингових балів (з урахуванням складання залікової роботи). Рейтингова оцінка студента визначається результатами перескладання.

Студенти, які після першого перескладання не одержали позитивної оцінки, йдуть на повторне перескладання дисципліни спеціалізованій атестаційній комісії. Формат повторного перескладання визначається комісією.

Підсумкова оцінка з дисципліни

Рейтингова оцінка складається з результатів виконання семестрових контрольних заходів (включно з заохочувальними) або за результатами виконання залікової роботи чи перескладання. Оцінка за стобальною шкалою переводиться до університетської шкали оцінок за наведеною таблицею відповідності.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

<i>Кількість балів</i>	<i>Оцінка</i>
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

Робочу програму навчальної дисципліни (силабус):

Склав: доцент кафедри ММЗІ, к.т.н. Яковлев Сергій Володимирович

Ухвалено кафедрою математичних методів захисту інформації (протокол №6/2 від 25.06.2025 р.).

Затверджено Методичною комісією НН ФТІ (протокол №6 від 30.06.2025 року)