Програма курсу

“Сучасні методи розробки програм”

1 семестр 2019/2020 навчального року

1. Цілочисельні решітки: означення і приклади.
2. Унімодулярні матриці, фундаментальний паралелепіпед, об’єм решітки.
3. Послідовні мінімуми решітки, теореми Блікфельда і Мінковського.
4. Задачі **SVP**.
5. Задачі **CVP**.
6. Опис алгоритму LLL.
7. Коректність алгоритму LLL.
8. Криптосистема GGH.
9. Криптосистема NTRUCrypt.
10. Булеві та арифметичні схеми, гомоморфні перетворення та гомоморфні криптосистеми.
11. Синтаксис гомоморфних криптосистем.
12. Задача наближених спільних дільників.
13. Гомоморфне шифрування на цілих числах.
14. Задачі **LWE**.
15. Дещо гомоморфна криптосистема Халеві-Вайкутанатана: опис.
16. Дещо гомоморфна криптосистема Халеві-Вайкутанатана: коректність.
17. Повністю гомоморфна криптосистема Бракерскі-Джентрі-Вайкутанатана: базова схема.
18. Повністю гомоморфна криптосистема Бракерскі-Джентрі-Вайкутанатана: основна схема.
19. Білінійне спарювання.
20. Еліптичні криві. Дивізори. Групи дівізорів.
21. Головні дівізори. Функція Вейля. Закон взаємності Вейля.
22. Алгоритм Міллера.
23. Спарювання Вейля.
24. Синтаксис шифрування на основі ідентифікаторів.
25. Безпека шифрування на основі ідентифікаторів.
26. Криптосистема на основі ідентифікаторів за допомогою спарювання Вейля: спрощена схема.

27. Метод Фуджісакі-Окамото.
28. Криптосистема на основі ідентифікаторів за допомогою спарювання Вейля: основна схема.
29. Побудова цифрового підпису за допомогою шифрування на основі ідентифікаторів.
30. Синтаксис функціонального шифрування.
31. Функціональне шифрування на основі предикатів.
32. Синтаксис шифрування на основі скалярного добутку.
33. Побудова шифрування на основі скалярного добутку.
34. Синтаксис і безпека функціонального шифрування з двома аргументами.
35. Побудова функціонального шифрування з двома аргументами.
36. Ізогенії еліптичних кривих. Графи ізогеній.
37. Суперсингулярний ізогональний протокол Діффі-Хелмана.
38. Лінійні коди. Коди Гоппа.
39. Криптосистема МакЕліс.
40. Некомутативна криптографія.