Приблизний перелік індивідуальних завдань для проходження переддипломної практики студентів 4 курсу

1. Розробка лабораторних робіт з комп'ютерного практикуму для курсу «Асиметричні криптосистеми».
2. Вивчення методів криптоаналізу криптографічних протоколів. Побудова моделей , реалізація на ЕОМ, експериментальні дослідження.
3. Пошук експоненціальних перетворень над скінченним полем заданої розмірності які задовольняють визначеній множині криптографічних властивостей.
4. Побудова верхніх оцінок ймовірності цілочисельного диференціалу для раундової функції у схемі фейстеля.
5. Побудова програмної реалізації емулятора ГОСТ 28147 зі збоями для збору статистичних даних та подальшого пошуку стратегії атак зі збоями на ГОСТ 28 147.
6. Дослідження та пошук алгоритмів побудови підстановок великого степеня з допомогою спеціальних перетворень над елементами, що враховують спосіб їх зображення.
7. Дослідження алгоритмів розв'язання систем рівнянь зі спотворенням над скінченними полями та їх застосування в криптоаналізі.
8. Дослідження класичних систем застосованих на динамічному хаосі атаки побудовані на них переваги та недоліки.
9. Пошук та дослідження нових принципів та підходів для побудови статистичних тестів перевірки випадкових та псевдовипадкових послідовностей.
10. Розробка переборних алгоритмів криптоаналізу класичних шифрів із застосуванням бібліотеки паралельного програмування MPI для кластерної обчислювальної системи.
11. Дослідження та створення бібліотеки отримання фізичних випадкових послідовностей із стандартних засобів обчислювальної техніки.
12. Розробка програмного засобу реалізації модульного контролю за дисципліною «Методи реалізації криптографічних механізмів захисту інформації».
11. Дослідження алгебраїчних атак на потокові криптосистеми.
12. Опрацювання різних методик оцінювання і обчислення диференціалів псевдоейфелевських перетворень і застосування їх для одержання оцінок стійкості цих перетворень.
13. Застосування інфраструктури відкритих ключів.
14. Дослідження незбалансованих фейстелевських схем блокових шифраторів.
15. Аналіз статистичних властивостей учасника конкурсу е – Stream алгоритмуCreupt МТЗ StreamCipher.
16. Розробка та застосування алгоритму кубічної атаки до типових схем побудови потокових шифрів дослідження швидкої атаки.
17. Аналіз стійкості сучасних блокових шифрів до лінійно – різницевого криптоаналізу.
18. Дослідження стійкості алгоритмів гамування до методу ймовірного слова.
19. Аналіз методів факторизації багатослівних чисел та розробка бібліотеки програм факторизації для розподільних обчислювальних систем.
20. Аналіз методів дискретного логорифмування та розробка бібліотеки програм обчислення дискретного логарифмування для розподільних обчислювальних систем.
21. Дослідження стійкості асиметричних криптосистем, заснованих на факторизації для різних моделей обчислень.
22. Розробка механізмів шифрування та геджування для оперативних систем мобільних теміналів на прикладі ОС WindousMobile та Simbian.
23. Блокові шифратори. Принципи побудови, криптоананалізу.
24. Застосування кубічних атак до блочних, поточних шифрів та до хеш – функцій.

25. Дослідження стійкості 1024-бітного RSA та 160-бітної криптографії на елептичних кривих.

26.Реалізація механізмів автентифікації та цифрового підпису для мобільних терміналів на прикладі ОС Simbian.

27. Розробка механізмів шифрування та геджування для оперативних систем мобільних теміналів на прикладі ОС WindousMobile та Simbian.

28. Дослідження стійкості асиметричних криптосистем, заснованих на обчисленні дискретного логарифму для різних моделей обчислень.

29. Дослідження методів оптимізації реалізації основних симетричних алгоритмів для різної архітектури обчислювальної техніки.

30.Дослідження інфраструктури відкритих ключів та використання відміток часу.

31.Протоколи SSL і TLS та їх вразливості.

22. Протокол Kerberos та його реалізація.

23Дослідження доказової стійкості деяких узагальнень схеми Фейстеля до диференціального аналізу

24.Аналіз існуючих протоколів квантових грошей.

25.Криптоаналіз однієї модифікації протоколу Диффі – Хелмана вироблення спільного ключа.

26.Дослідження схеми блочного шифрування у моделі псевдо випадковості.

27. Аналіз метода вбудовування публічних параметрів для протидії атакам збоїв

28.Дослідження залежності оцінок стійкості сучасних потокових шифрів від вибору особливих точок атак компромісу.

29.Дослідження впливу лінійного замішування на диференціальні характеристики незбалансованих схем Фейстеля.

30. Побудова атак збоїв на сімейство шифрів «Калина».

31.Реалізація та дослідження атаки за побічним каналом на алгоритм шифрування IDEA.

Матеріали, що отримав студент під час виконання індивідуального завдання, можуть в подальшому бути використані для виконання кваліфікаційної роботи, для підготовки доповіді, статті або для інших цілей за погодженням з кафедрою і базою практики.