Додаток

Типова тематика курсового проекту з дисципліни
МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

- Програмна реалізація та дослідження шифрів заміни. Оцінка їх властивостей.
- Програмна реалізація та дослідження шифрів перестановки. Оцінка їх властивостей.
- Програмна реалізація та дослідження шифру Плейфера. Оцінка його властивостей.
- Програмна реалізація та дослідження шифру Хілла. Оцінка його властивостей.
- Програмне моделювання та дослідження алгоритму симетричного шифрування AES.
- Програмне моделювання та дослідження алгоритму симетричного шифрування DES.
- Програмне моделювання та дослідження алгоритмів стеганографічного приховування інформації в цифрових зображеннях.
- Програмне моделювання та дослідження алгоритмів стеганографічного приховування інформації в аудіо файлах.
- Програмне моделювання та дослідження алгоритмів генерації цифрового підпису.
- Проведення порівняльного аналізу алгоритмів формування хеш-функцій SHA-0 та SHA-1.
- Дослідження криптографічної функції хешування SHA-2.
- Проведення порівняльного аналізу алгоритмів формування хеш-функцій MD-2 та MD-4.
- Дослідження криптографічної функції хешування MD-5.
- Програмна реалізація і дослідження ефективності процедури факторизації натуральних чисел (розкладання на прості множники) ро-методом Полларда.
- Програмна реалізація і дослідження системи шифрування на еліптичних кривих.
- Програмна реалізація і дослідження генерації простих чисел на основі методу Міллера-Рабіна.
- Програмна реалізація і дослідження ефективності арифметичних операцій на еліптичних кривих.
- Програмна реалізація і дослідження ефективності факторизации натуральних чисел методом Шенкса безперервних дробив і порівняння з ро-методом Полларда.
- Порівняльне вивчення і програмна реалізація на комп'ютері алгоритму обчислення дискретного логарифма в кінцевих полях.
- Програмна реалізація і дослідження алгоритму Шенкса-Тоннеллі визначення квадратного кореня в кінцевих полях.
- Програмна реалізація і дослідження методу обчислення складових псевдопростих чисел для різних баз.
- Програмна реалізація і дослідження бінарного алгоритму Евкліда. Порівняння з класичним алгоритмом Евкліда.