Лабораторна робота № 2.

**Тема:** Реалізація алгоритмів генерації ключів гібридних криптосистем.

**Мета роботи:** Дослідження алгоритмів генерації псевдовипадкових послідовностей, тестування простоти чисел та генерації простих чисел з точки зору їх ефективності за часом та можливості використання для гененерації ключів асиметричних криптосистем

**Завдання на лабораторну роботу**

Для першого типу лабораторних дослідити різні методи генерації випадкових послідовностей для засобів обчислювальної техніки. Дослідити ефективність за часом алгоритми тестування на простоту різних груп – імовірнісних, гипотетичних та детермінованих. Порівняти ймовірність похибки різних імовірнісних тестів (Ферма, Соловея-Штрассена та Мілера-Рабіна з різною кількістю ітерацій) з ймовірністю похибки при виконанні обчислень на ПЕОМ. Розглянути алгоритми генерації простих чисел “Чебишова” та Маурера та провести порівняльний аналіз їх складності. Розробити бібліотеку генерації псевдовипадкової послідовності, тестування простоти чисел та генерації простих чисел для Intel-сумісних ПЕОМ. Розмірність чисел – 768, 1024 біт.

Лог генерації випадкового простого числа для 768 розрядних чисел.

GetRandom:GetRandomEND:GetPrime:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:Fermat:GetRandom:GetRandomEND:Modulo:GetRandom:GetRandomEND:Modulo:7342446370864015512035075733629599938206844501200990702879919831185947621298828641658330972488021185872252635320821058562869881293545116572505092119436423