Відомості про роботу: робота складається з 54 сторінок, 3 рисунків, 4 таблиць, 11літературних посилань.

Об'єктом дослідження єінформаційні процеси в асиметричних системах криптографічного захисту.

Предметом дослідженняє оцінка складності вибору параметрів алгоритмів асиметричної криптографії та побудови асиметричних криптографічних систем.

Мета роботи:отримання оцінок складності вибору параметрів асиметричних криптосистем та складності побудови відомих криптографічних систем RSA,Рабіна, Ель-Гамаля, Diffie-Hellman.

В бакалаврській роботі розглянуто криптосистеми з відкритим ключем, побудовані математичні моделі вибору параметрів асиметричних систем, отриманні оцінки складності вибору параметрів та оцінки складності відомих криптосистем RSA,Рабіна, Ель-Гамаля, Diffie-Hellman.