Об’єктом дослідження є алгебраїчні моделі криптографічних систем та протоколів Предметом дослідження є властивості алгебраїчних моделей. Для досягнення поставлених завдань у дипломному проекті використовувались алгебраїчні методи представлення симетричних і асиметричних систем у вигляді багатоосновних алгебр. У роботі були виведені алгебраїчні моделі різних криптосистеми. У якості об’єкту досліджень був обраний односторонній суматор, на основі якого було створено алгебраїчну модель, що потім була порівняна з моделлю симетричного комутативного шифру і показано, що атаку на односторонній суматор можна звести до атаки на симетричний шифр. Стровено узнагальнену алгебраїчну модель шифру. Також побудовано, алгебраїчну модель комутативного шифру Мессі-Омури. Побудована модель для протоколу Фіата-Шаміра.