РЕФЕРАТ

Метою роботи є знаходження оцінок ймовірності виникнення перекриттів відрізків гамми та використання шифртексту з перекриттями для безключового криптоаналізу. Об’єктом дослідження в даній роботі є інформаційні процеси в системах захисту інформації. Предметом дослідження є математичні моделі та методи криптоаналізу функціонування потокових шифрів при перекритті гамм. У роботі запропоновано алгоритми відновлення відкритих текстів, проведено пошук областей виконання теоретичних асимптотичних результатів для оцінок ймовірності виникнення перекриття. Результати роботи можуть бути використані для криптоаналізу функціонування потокових шифрів гаммування при їхньому інтенсивному використанні.

ПОТОКОВИЙ ШИФР ГАММУВАННЯ, ГАММА ШИФРУ, КОМБІНАТОРНО-ЙМОВІРНІСНА МОДЕЛЬ ФУНКЦІОНУВАННЯ ПОТОКОВИХ ШИФРІВ, БЕЗКЛЮЧОВОВЕ ЧИТАННЯ, СТАТИСТИЧНЕ МОДЕЛЮВАННЯ.