Аңдатпа

Осы магистрлік диссертация шифрлік алгоритмдерінің криптографиялық тұрақтылығын көтеру әдістерін зерттеуге арналады.

Зерттудің өзектілігі - құпия шифрдің жүйесінің тез дамуын, сондай-ақ, оларды бұзу әрекетінің қатар дамуы аса жоғары криптобұрақтылығы бар жаңа жүйені құруды талап етеді.

Зерттеу жұмысына RSA алгоритмы алынған және Cryptool 2 бағдарламалық өнімнің комегімен жасалды, сондай-ақ, әртүрлі әдістер бойынша шабуыл жүзеге аырылды.

Зерттеу жұмыстарының нәтежесі бойынша келесі тұжырым жасалды – хеш-қызметін қолдану арқылы алгоритмдерді сенімді, сондай-ақ, құпия шифрлар кілтінің өлшемдерін көбейту талап етімді.

Аннотация

Данная магистерская диссертация посвящена исследованию методов повышения криптографической стойкости алгоритмов шифрования.

Актуальностью исследования заключается в том, что быстрое развитие систем шифрования, а так же сопутствующее развитие их взлома ведет к созданию новых систем с более высокой криптостойкостью.

Для исследования был выбран алгоритм RSA и произведено моделирование его алгоритма с помощью программного продукта Cryptool 2, а так же осуществлена атака по различным методам.

По результатам исследования можно сделать вывод, что надежнее использовать алгоритмы с применением хеш-функций, а так же увеличить параметры ключей шифрования.

Annotation

This master's dissertation is devoted to research methods for improving the cryptographic strength of encryption algorithms.

Relevance of the study is that the rapid development of encryption systems, as well as the concomitant development of their breaking leads to the creation of new systems with higher cryptographic strength.

The RSA algorithm was selected for the study. This algorithm was modeled using software Cryptool 2, also it was carried out attacks on various methods.

According to the study it can be concluded that it is more reliable to use algorithms with hash functions, as well as increasing the options of the encryption keys.