МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Кафедра физики и аэрокосмических технологий

Аннотация к дипломной работе

АЛГОРИТМ ШИФРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКИХ СИГНАЛОВ И ЕГО КРИПТОАНАЛИЗ

Жуковец Денис Александрович

Научный руководитель – доктор технических наук,
профессор *Сидоренко А.В.*

Минск, 2015

РЕФЕРАТ

Дипломная работа содержит 54 страниц, 24 рисунка, 9 таблиц, библиография содержит 22 наименований.

Ключевые слова: КРИПТОАНАЛИЗ, ДИФЕРЕНЦИАЛЬНЫЙ, ЛИНЕЙНЫЙ, АЛГОРИТМ, ШИФРОВАНИЕ, СЕТЬ ФЕЙСТЕЛЯ, ДИНАМИЧЕСКИЙ ХАОС.

Объектом исследований является алгоритм шифрования, построенный на основе сети Фейстеля с использованием динамического хаоса

Целью работы является разработка алгоритма и программных средств для шифрования/расшифрования на основе динамического хаоса и проведение исследований алгоритма на его устойчивость к различным видам криптографических атак

Решаются следующие задачи:

- разработка программы для алгоритма шифрования на основе динамического хаоса;
- оценка устойчивости к различным видам криптоатак;
- обоснование и выбор методов криптоанализа для алгоритма шифрования с использованием динамического хаоса;
- разработка программ для криптоанализа;
- реализация дифференциального и линейного криптоанализа зашифрованных текстов с использованием динамического хаоса.

В результате проведенных исследований нами был разработан алгоритм, а также программа для шифрования и расшифрования открытого текста с использованием динамического хаоса. Для доказательства стойкости алгоритма шифрования проведено определение количественных параметров, таких как информационная энтропия, числовых характеристик распределения значений байт в открытом и зашифрованном тексте, корреляция, процент бит изменивших значение (лавинный эффект), процент пикселей изменивших значение (Number of Pixels Change Rate), среднее изменение интенсивности (Unified Average Changing Intensity). Проведен линейный и дифференциальный криптоанализ алгоритма шифрования

РЭФЕРАТ

Дыпломная праца ўтрымоўвае 54 старонак, 24 малюнка, 9 табліц, бібліяграфія утрымоўвае 22 найменняў.

Ключавыя словы: КРЫПТААНАЛІЗ, ДЫФЕРЭНЦЫЯЛЬНЫ, ЛІНЕЙНЫ, АЛГАРЫТМ, ШЫФРАВАННЕ, СЕТКА ФЕЙСТЕЛЯ, ДЫНАМІЧНЫЯ ХАОС.

Аб'ектам даследаванняў з'яўляецца алгарытм шыфравання, пабудаваны на аснове сеткі Фейстеля з выкарыстаннем дынамічнага хаосу

Мэтай працы з'яўляецца распрацоўка алгарытму і праграмных сродкаў для шыфравання / расшыфравання на аснове дынамічнага хаосу і правядзенне даследаванняў алгарытму на яго ўстойлівасць да розных відаў крыптаграфічных нападаў

Вырашаюцца наступныя задачы:

- распрацоўка праграмы для алгарытму шыфравання на аснове дынамічнага хаосу;
- ацэнка ўстойлівасці да розных відаў крыптаатак;
- абгрунтаванне і выбар метадаў крыптааналіза для алгарытму шыфравання з выкарыстаннем дынамічнага хаосу;
- распрацоўка праграм для крыптааналіза;
- рэалізацыя дыферэнцыяльнага і лінейнага крыптааналіза зашыфраваных тэкстаў з выкарыстаннем дынамічнага хаосу.

У выніку праведзеных даследаванняў намі быў распрацаваны алгарытм, а таксама праграма для шыфравання і расшыфравання адкрытага тэксту з выкарыстаннем дынамічнага хаосу. Для доказу стойкасці алгарытму шыфравання праведзена вызначэнне колькасных параметраў, такіх як інфармацыйная энтрапія, лікавых характарыстык размеркавання значэнняў байт у адкрытым і зашыфраваным тэксце, карэляцыя, працэнт біт якія змянілі значэнне (лавінны эфект), працэнт пікселяў якія змянілі значэнне (Number of Pixels Change Rate), сярэдняе змяненне інтэнсіўнасці (Unified Average Changing Intensity). Праведзены лінейны і дыферэнцыяльны крыптааналіз алгарытму шыфравання

ABSTRACT

Diploma thesis contains 54 pages, 24 figures, 9 tables, bibliography contains 22 references.

Keywords: CRYPTANALYSIS, DIFFERENTIAL, LINEAR, ALGORITHMS, FEISTEL CIPHER, DYNAMIC CHAOS.

The object of research is the encryption algorithm based on a Feistel network using dynamic chaos

The aim is to develop algorithms and software for encryption / decryption based on dynamic chaos and conducting research algorithm on its resistance to various types of cryptographic attacks

Solved the following problems:

- develop programs for the encryption algorithm based on dynamic chaos;
- evaluation of resistance to various types of cryptographic attacks;
- the rationale and selection method of cryptanalysis for the encryption algorithm using dynamic chaos;
- develop programs for cryptanalysis;
- implementation of differential and linear cryptanalysis of the encrypted text using dynamic chaos.

As a result, of the research we have developed an algorithm and a program for encryption and decryption of plaintext using dynamic chaos. To prove the stability of the encryption algorithm carried out quantitative determination of parameters such as information entropy, numerical characteristics of distribution of byte values in the open and encrypted text, correlation, the percentage of bits change the value (avalanche effect), Number of Pixels Change Rate, Unified Average Changing Intensity. Carried out linear and differential cryptanalysis of the encryption algorithm