Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Пониделко И.Н. Развитие симметричной криптографии и иных методов защиты информации // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2017. – № 05 (май). – АРТ 140/3-эл. – 0,1 п.л. - URL: http://akademnova.ru/page/875550

РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004

Пониделко Илья Николаевич
студент 2 курса, юридический факультет
ФГБОУ ВО «Ростовский государственный экономический университет» (РИНХ)
г. Ростов-на-Дону. Российская Федерация.
e-mail: 89896177110@mail.ru

Развитие симметричной криптографии и иных методов защиты информации

Аннотация: В статье рассматриваются основные этапы развития симметричной криптографии и иных методов защиты информации, а также основные методы анализа симметричных шифров.

Ключевые слова: Методы защиты информации.

Ponidelko I.N
2nd year student, Faculty of Law
FGBOU IN "Rostov State University of Economics "(RINE)
Rostov-on-Don. Russian Federation.
e-mail: 89896177110@mail.ru

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Development of symmetric cryptography and other methods of information protection

Annotation: The main stages of the development of symmetric cryptography and other methods of information protection, as well as the basic methods of analyzing symmetric ciphers are considered in the article.
Key words: methods of information protection.

С древних времен человек стремился защитить свое личное пространство и свои интересы, в частности путем использования различных способов кодирования информации, ввиду чего, можно сказать что актуальность исследования симметричных криптографических методов и способов защиты информации не только не снижается, но и растет на протяжении сотен лет.

Ключевую позицию для понимания специфики исследуемого вопроса имеет вклад Огюста Кергоффса, издавшего труд под названием «Военная криптография».

Многие исследователи, отмечают, что именно эта работа послужила толчком для развития теории информации в ее современном понимании. Так же нельзя не упомянуть Клода Шеннона, сформулировавшего в своей работе «Теория связи в секретных системах» опубликованной в 1949г. основные постулаты теоретической криптографии, которые определяют, какими свойствами должны обладать надежные шифры.

Именно Клод Шеннон своими трудами ввел в криптографию понятия перемешивания и рассеивания и предложил формировать криптографически стойкие системы на основе простейших математических преобразований.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Стоит отметить, что до XX века криптография отнюдь не являлась общедоступной наукой, а наоборот была доступна лишь единицам, узкому кругу лиц.

Подобное положение вещей было обусловлено в первую очередь непростой политической обстановкой и стремлением использовать криптографию в военных целях.

Ситуация кардинально изменилась с появлением персональных компьютеров, позволявших пользователю иметь фактически безлимитный доступ к электронной информации, что и стало основной причиной углубленного и всестороннего изучения криптографии как наиболее продуктивного способа ограничить эту информацию от несанкционированного доступа.

Первыми формами криптографии стали симметричная криптография и несколько позднее ассиметричная криптография.Симметричное шифрование, которое так же называют классическим или шифрованием с общим ключом, до изобретения шифрования с открытым ключом было единственным методом шифрования. В 1976 г. в США был утвержден стандарт шифрования данных DES (Data Encryption Standard), который использовался довольно длительное время (более 20 лет), пока в 2001 г. не был принят новый стандарт AES(Advanced Encryption Standard). В основу последнего лег алгоритм шифрования Rijndael.

В России же официальным государственным стандартом является алгоритм шифрования ГОСТ 28147-89.

Для симметричных алгоритмов шифрования характерен целый ряд свойств, однако ключевыми из них являются

1. использование одного и того же алгоритма как для зашифрования, так и для расшифрования данных;

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

2. использование одного ключа, который хранится в секрете.

Современные симметричные алгоритмы шифрования разделяются на блочные и поточные. Для блочных алгоритмов шифрование информации производится небольшими порциями – именуемыми блоками; как правило, размер блока кратен 32 битам и имеет размер в 64, 128, 192 или 256 битов. К современным алгоритмам симметричного шифрования относятся такие шифры, как DES, AES (Rijndael), RC5, ГОСТ 2814789, и многие другие.

На сегодняшний день существует два основных способа построения симметричных алгоритмов шифрования: схема Фейстеля и сеть подстановок и перестановок (SPN – Substitution-Permutation Network).

По схеме Фейстеля построены алгоритмы DES, RC5, ГОСТ 28147-89 и др. Самым ярким представителем использования сети SPN является стандарт AES.

Рассматривая симметричные системы нельзя обойти стороной основные методы их анализа. Итак, ключевым из них является дифференциальный криптоанализ, который впервые был предложен в начале 90-х годов прошлого века Э. Бихамом и А. Шамиром для анализа алгоритма шифрования DES. Хотя в книге Б. Шнайера и упоминается о том, что разработчики алгоритма DES знали о возможности такого анализа еще во время разработки алгоритма в 70-х годах XX века, широкая общественность узнала о дифференциальном криптоанализе именно из работы Метод ДК оказался первым методом, позволяющим взломать DES при оценке сложности задач менее 255.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Список использованной литературы:

1.Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. – М.: Гелиос АРВ, 2006. – С. 376.

2. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. – М.:ТРИУМФ, 2002. – С. 648.

3. *Biham E., Shamir A.* Differential Cryptanalysis of the Full 16-round DES, Crypto'92, Springer-Velgar, 1998. – P. 487.

4. *Babenko L.K., Ishchukova E.A.* Data Distribution Algoritms for Differential Cryptanalysis of DES // Proceeding of the Workshop on Computer Science and Information Technologies
(CSIT'2007), Krasnousolsk, UFA, September 13-16, 2007. – Vol. 1. UFA State Aviation Technical University, 2007. – P. 198-201.

5. Ищукова Е.А. Применение рекурсивного алгоритма поиска в Б-деревьях для дифференциального криптоанализа алгоритма шифрования ГОСТ 28147-89 // Информационная безопасность. Ч. 2. – Таганрог: Изд-во: ТТИ ЮФУ, 2007. – С. 92-97

Дата поступления в редакцию: 31.05.2017 г.
Опубликовано: 31.05.2017 г.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru