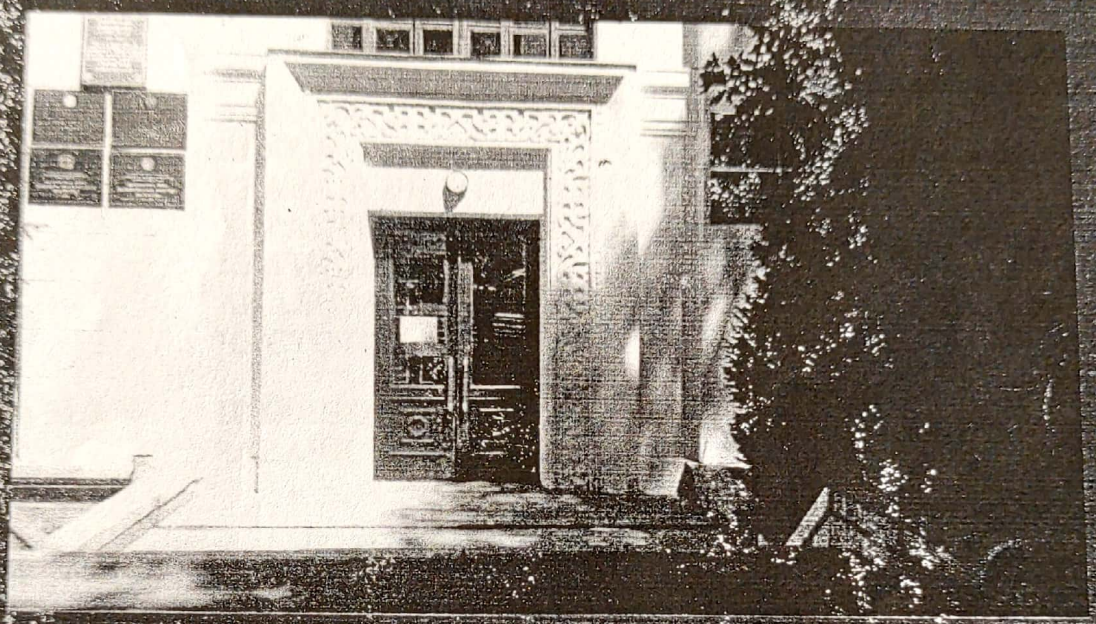
ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
ҒЫЛЫМ КОМИТЕТІНІҢ
АҚПАРАТТЫҚ ЖӘНЕ ЕСЕПТЕУІШ ТЕХНОЛОГИЯЛАР ИНСТИТУТЫ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
КОМИТЕТ НАУКИ
ИНСТИТУТ ИНФОРМАЦИОННЫХ И ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ

MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF KAZAKHSTAN
COMMITTEE OF SCIENCE
INSTITUTE OF INFORMATION AND COMPUTATIONAL TECHNOLOGIES



МАТЕРИАЛЫ

научной конференции ИИВТ МОН РК «Современные проблемы информатики и вычислительных технологий» 18-19 июня 2015 года

Алматы 2015

СОДЕРЖАНИЕ

Алтаева А.Б., Кулпешов Б.Ш.	ВОПРОСЫ ОРТОГОНАЛЬНОСТИ И НЕРАЗЛИЧИМОСТИ В СЛАБО ЦИКЛИЧЕСКИ МИНИМАЛЬНЫХ СТРУКТУРАХ	4
Алтаева А.Б.	ЛОГИЧЕСКОЕ ИССЛЕДОВАНИЕ МОДЕЛИРОВАНИЯ ПОВЕДЕНИЯ ГИБРИДНЫХ СИСТЕМ	12
Амиргалиев Б.Е., Куатов К.К., Джантасов А.К., Кеншимов Ч.А., Байбатыр Ж.Е., Кайранбай М.Ж.	МЕТОД ВЕРИФИКАЦИИ НОМЕРНОГО ЗНАКА ДЛЯ СИСТЕМ РАСПОЗНАВАНИЯ АВТОМОБИЛЬНЫХ НОМЕРОВ	15
Амиргалиев Е.Н., Мусабаев Р.Р., Мусабаев Т.Р.	АВТОМАТИЧЕСКАЯ СЕГМЕНТАЦИЯ РЕЧЕВОГО СИГНАЛА НА ОКНА СО СТАБИЛЬНЫМИ СПЕКТРАЛЬНЫМИ ХАРАКТЕРИСТИКАМИ НА ОСНОВЕ КРАТКОВРЕМЕННЫХ АЛГОРИТМОВ АНАЛИЗА СИНХРОНИЗИРОВАННЫХ С ЧАСТОТОЙ ОСНОВНОГО ТОНА	18
Арсланов М.З.	ПОЛИНОМИАЛЬНЫЙ АЛГОРИТМ ДЛЯ ЗАДАЧИ MSP3	26
Ахметова А.М., Нугманова С.А., Ануарбеков А.М.	АЛГОРИТМЫ ШИФРОВАНИЯ CAST	31
Байрбекова Г.С., Мазаков Т. Ж.	О НЕКОТОРЫХ ПРОБЛЕМАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УПРАВЛЕНИЯ ДОСТУПОМ	34
Бердышев А.С., Бекбауов Б.Е., Рахымова А.Т.	ЧИСЛЕННОЕ РЕШЕНИЕ ХИМИЧЕСКОГО ЗАВОДНЕНИЯ НА СИМУЛЯТОРЕ UTCHEM	38
Бердышев А.С., Имомназаров Х.Х., Бердышева Д.А.	МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ВОЛНОВЫХ ПРОЦЕССОВ ДЛЯ ДВУМЕРНОЙ МОДЕЛИ ПОРОУПРУГОСТИ	43
Бияшев Р.Г., Нысанбаева С.Е., Бегимбаева Е.Е.	РАЗРАБОТКА АСИММЕТРИЧНОЙ СИСТЕМЫ ЦИФРОВОЙ ПОДПИСИ НА БАЗЕ МОДУЛЯРНОЙ АРИФМЕТИКИ	48

АЛГОРИТМЫ ШИФРОВАНИЯ CAST

Ахметова А.М., Нугманова С.А., Ануарбеков А.М.
Научно-исследовательский институт КН МОН РК совместно с КазНУ им. аль-Фараби на базе РГП «Ғылым ордасы», Алматы, Казахстан, ardak_66@mail.ru
КазНПУ им. Абая, Алматы, Казахстан, nugm_s@mail.ru

В данной статье рассматривается алгоритм шифрования CAST, общие сведения и свойства стойкости, реализовано шифрование и дешифрование файла.

Введение

Алгоритм CAST-128 был создан в 1996 году Карлайлом Адамсом (CarlisleAdams) и Стаффордом Таваресом (StaffordTavares) используя метод построения шифров CAST [1].

CAST-128 состоит из 12 или 16 раундов сети Фейстеля с размером блока 64 бита и длиной ключа от 40 до 128 бит (но только с инкрементацией по 8 бит). 16 раундов используются, когда размеры ключа превышают 80 бит. В алгоритме используются 8x16 S-блоки, основанные набент-функция, операции XOR и модулярной арифметике (модулярное сложение и вычитание). Есть три различных типа функций раундов, но они похожи по структуре и различаются только в выборе выполняемой операции (сложение, вычитание или XOR) в различных местах.

Хотя CAST-128 защищён патентом Entrust, его можно использовать во всём мире для коммерческих или некоммерческих целей бесплатно.

Алгоритм CAST использует 64-битовый блок и 64-битовый ключ. CAST устойчив к дифференциальному и линейному криптоанализу. Сила алгоритма CAST заключена в его S-блоках. У CAST нет фиксированных S-блоков и для каждого приложения они конструируются заново. Созданный для конкретной реализации CAST S-блоки уже больше никогда не меняется. Другими словами, S-блоки зависят от реализации, а не от ключа. NorthernTelecom использует CAST в своём пакете программ Entrust для компьютеров Macintosh, PC и рабочих станций UNIX. Выбранные ими S-блоки не опубликованы, что впрочем неудивительно.

CAST-128 принадлежит компании Entrust Technologies, но является бесплатным как для коммерческого, так и для некоммерческого использования. CAST-256 — бесплатное доступное расширение CAST-128, которое принимает размер ключа до 256 бит и имеет размер блока 128 бит. CAST-256 был одним из первоначальных кандидатов на AES.

CAST-128

CAST-128 основан на сети Фейстеля. Алгоритм использует пару подключей за раунд: 32-битные величины Km используется в качестве "маскировки" ключа и Kr используют как "перестановки" ключа, из которых используются только начальные 5-бит.

Три различных типов функции используются в CAST-128.Типы выглядит следующим образом (где "D" является входными данными в функцию F и "Ia"- "Id" является наиболее значимый байт - наименее значимый байт I, соответственно).

CAST-128 использует восемь полей замены: поля S1, S2, S3 и S4 раундовые функции полей замены, S5, S6, S7 и S8 являются ключами развертки полей замены. Несмотря на то, что 8 полей замены требуют в общей сложности 8 Кбайт для хранения, обратите внимание на то, что только 4 Кбайта требуются во время фактического шифрования/дешифрование, так как генерация подключа обычно делается до любого ввода данных. См. Приложение для содержимого полей замены S1 - S8.

Представим 128-разрядный ключ в виде x0x1x2x3x4x5x6x7x8x9xAxBxCxDxExF, где x0 старший байт, и xF младший байт.

Представим z0..zF промежуточными (временными) байтами. Si[] представляет поле замены i и "^" представляет сложение по XOR'у.

Km1, ...,Km16 32-разрядные подключи маскировки (один на раунд). Kr1, . . . , Kr16 32-разрядные перестановки подключей (один на раунд); только младшие 5 битов используются в каждом раунде.

for (i=1; i<=16; i++) { Kmi = Ki; Kri = K16+i; }

CAST-128 Алгоритм шифрования был разработан, чтобы размер ключа мог варьироваться от 40 до 128 бит, в 8-битном шаге (т.е. допустимые размеры ключа равняются 40, 48, 56, 64..., 112, 120, и 128 битов). Для переменной работы размера ключа спецификация следующие:

1) Для размеров ключа до и включая 80 битов (т.е., 40, 48, 56, 64, 72, и 80 битов), алгоритм точно такой же, но использует 12 раундов вместо 16;

2) Для размеров ключа, больше, чем 80 битов, алгоритм использует полные 16 раундов;

3) Для размеров ключа меньше чем 128 битов ключ дополнен нулевыми байтами (в самых правых, или младших, позициях) к 128 битам (так как расписание ключа CAST 128 принимает входной ключ 128 битов).

Расшифрование совпадает с алгоритмом шифрования, приведенным выше, кроме того, что раунды (и, следовательно, пары подключей), используются в обратном порядке, чтобы вычислить (L0, R0) из (R16, L16).

CAST-256

Этот алгоритм основан на более раннем алгоритме CAST-128. Оба шифра построены на основе методологии CAST, предложенной Карлайлом Адамсом (англ. CarlisleAdams) и Стаффордом Таваресом (англ. StaffordTavares), первые две буквы имени которых формируют название методологии. В создании «дизайна» шифра принимали участие также Хейз Говард и Майкл Винер. [2] CAST-256 построен из тех же элементов, что и CAST-128, включая S-боксы, но размер блока увеличен вдвое и равен 128 битам. Это влияет на диффузионные свойства и защиту шифра.

В RFC 2612 указано, что CAST-256 можно свободно использовать по всему миру в коммерческих и некоммерческих целях.

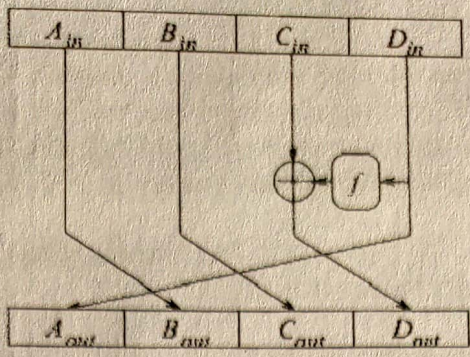
Алгоритм шифрует информацию 128-битными блоками и использует несколько фиксированных размеров ключа шифрования: 128, 160, 192, 224 или 256 битов.

В алгоритме CAST-256 48 раундов. Рассмотрим первую половину шифра [3].

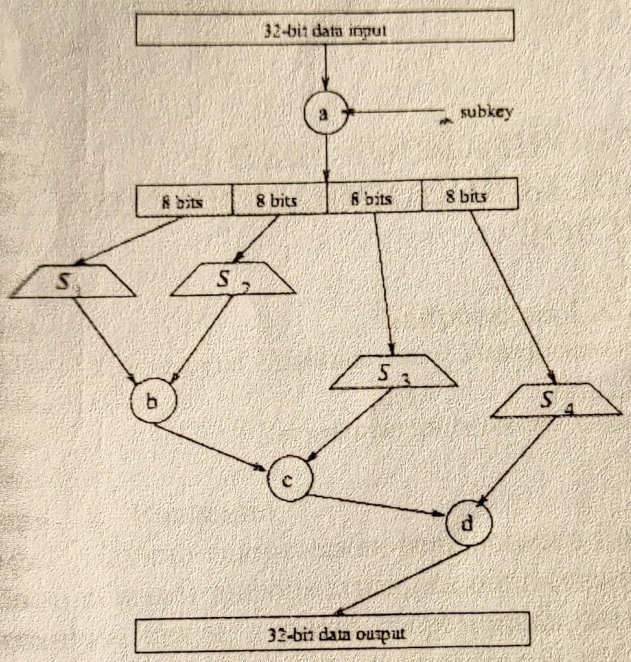
128-битный входной блок может быть разделен на четыре 32-битныхсубблока Ain, Bin, Cin и Din. Субблок Cin складывается по модулю 2 с Din, видоизмененного в зависимости от раундовой функции f. В результате, получаем субблок Dout. После сдвига входных субблоков вправо на одну позицию, получаем четыре выходных субблока: Aout, Bout, Cout и Dout. Для второй половины шифра рассматривается сдвиг субблоков на одну позицию влево.

Нелинейные функции *Sj* (где 1 <j< 4) являются подстановками из таблицы (S-бокс) 8x32 (в результате, происходит замена 8-битного входного значения на 32-битное). Из-за нелинейной природы, S-функции являются неотъемлемой составляющей безопасности шифра.

Операции «b», «c», и «d» представляют собой операции сложения и вычитания, которые выполняются с 32-битными операндами по модулю **232**. Операция «a» представляет собой наложение входного32-битного субблока и32-битногоподключа (который называется маскирующим подключом). Эта операция, используя одну из 3 операций(«b», «c», или «d»), производит вращение в зависимости от 5-битного подключа (который называется подключом сдвига). Раундовые функции CAST-256 отличаются между раундами, потому что объединение операций, используемых для «a», «b», «c» и «d», различно.



Алгоритм CAST 256



Раундовая функция CAST256

типичная раундовая функция выглядит следующим образом:

$$W = \left(\left(K_{m_i} + X_i\right)\langle\langle K_{r_i}\right) \tag{1}$$

$$Y_i = \left(\left(S_1[W_1] \oplus S_2[W_2]\right) + S_3[W_3] - S_4[W_4]\right)$$

входные 32-бита данных, *Wj* входные 8-бит данных в *Sj* функции, маскирующий подключ и подключ сдвига соответственно, *Yi*, данных, после воздействия раундовой функции, «⊕» операции собой сложение и вычитание соответственно по модулю 2. представляет левый сдвиг *V* по отношению к *U. W, Xi, Yi* и *Kmi*, собой 32-битные субблоки. *Kri* имеет длину 5 бит. Расшифровы- по аналогии с шифрованием, с той лишь разницей, что подключи ой последовательности [4].

Заключение

В данной статье был рассмотрен алгоритм шифрования CAST, его свойства стойкость. Достоинством алгоритма CAST-256 является отсутствие доказанных уязв мостей. Кроме того, плюсом является возможность выполнения расширения ключа лету», т. е. в процессе операции зашифровывания (но не расшифровывания).

Литература

1. CAST-128 [Электронный ресурс]: http://tools.ietf.org/html/rfc2144 (Дата об щения 25.05.2014)
2. CAST-256 [Электронный ресурс]:http://www.rfc-editor.org/rfc/rfc2612.txt(Д обращения 25.05.2014)
3. Алгоритм CAST-128 Блог о шифровании [Электронный ресу http://crypto.pp.ua/2010/05/algoritm-cast-128/(Дата обращения 25.05.2014)
4. Панасенко С.П. Современные алгоритмы шифрования // BYTE. 2003. С.18-22

О НЕКОТОРЫХ ПРОБЛЕМАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УПРАВЛЕНИЯ ДОСТУПОМ

Байрбекова Г.С.[1], Мазаков Т.Ж.[2]

[1] *Казахский Национальный Университет имени Аль-Фараби, Алматы, Казахстан,* zika_@mail.ru

[2] *Институт информационных и вычислительных технологий*

1. Введение

Научно-техническая революция в последнее время приняла грандиозные ма бы в области информатизации общества на базе современных средств вычислите техники, связи, а также современных методов компьютерной обработки инфор Применение этих средств и методов приняло всеобщий характер, а создаваемы этом информационно-вычислительные системы и сети становятся глобальными смысле территориальной распределенности, так и в смысле широты охвата в р единых технологий процессов сбора, передачи, накопления, хранения, поиска, ра ботки информации и выдачи ее для использования.

Создание информационной индустрии, давая объективные предпосыл грандиозного повышения эффективности жизнедеятельности человечества, пор целый ряд сложных и крупномасштабных проблем. Одной из таких проблем надежное обеспечение сохранности и установленного статуса использования терной информации, циркулирующей и обрабатываемой в компьютерных с управления и обработки информации. Данная проблема вошла в обиход под им проблемы защиты информации [1] (обеспечения информационной безопасности

Научно-технический прогресс в области связи и информатизации явился затором развития средств и методов информационного воздействия на киберне системы. Особенно остро стоит вопрос информационной уязвимости сложных зационно-технических систем управления, использующих компьютерные тех обработки информации [2]. К этой категории относят так называемые «кри системы управления и обработки информации», например, автоматизированны мы управления опасными производствами, системы управления космическим тами, воздушным и железнодорожным движением и т. п.