А.В. БАБАШ

МОНОГРАФИЯ

ДЕШИФРОВАНИЕ КЛАССИЧЕСКИХ ШИФРОВ

Теоретическая и практическая стойкость шифров

Дешифрование шифров тотальным методом

Дешифрование шифров методом эквивалентных ключей

Дешифрование шифров гаммирования

Дешифрование дисковых шифраторов
на основе развития атаки «человек посредине»

Дешифрование шифрующих автоматов
с помощью их приближенных моделей

КНОРУС

А.В. Бабаш

ДЕШИФРОВАНИЕ КЛАССИЧЕСКИХ ШИФРОВ

Монография

КНОРУС • МОСКВА • 2026

УДК 004.056.55
ББК 32+32.811.4
Б12

Рецензенты:
П.Б. Хорев, Национальный исследовательский университет «МЭИ», канд. техн. наук, доц.,
А.М. Чеповский, Российский университет дружбы народов (РУДН), Высшая школа экономики (НИУ ВШЭ), д-р техн. наук, проф.

Автор
А.В. Бабаш, Российский экономический университет имени Г.В. Плеханова

Бабаш, Александр Владимирович.
Б12 Дешифрование классических шифров : монография / А.В. Бабаш. — Москва : КНОРУС, 2026. — 164 с.

ISBN 978-5-406-11995-2

Большинство разделов написаны в автономном стиле. Для изучения материалов необходимо знать простейшие обозначения математики, в частности простейшие вероятностные понятия и обозначения.

Материал монографии сосредоточен на новых методах дешифрования классических шифров: шифр случайного гаммирования и его частный случай — шифр Вернама; шифр Виженера; шифр простой замены; шифр перестановки; шифр Джефферсона; шифр Тук-тук; шифр IA; дисковые шифраторы, блочные шифры как шифры простой замены с большой мощностью алфавита.

Для студентов специалитета и аспирантов, обучающихся по профилю «Защита информации», а также специалистов по защите информации.

Ключевые слова: шифр случайного гаммирования; шифр простой замены; шифр перестановки; шифр Джефферсона; шифр Тук-тук; дисковые шифраторы; блочные шифры.

УДК 004.056.55
ББК 32+32.811.4

Бабаш Александр Владимирович
ДЕШИФРОВАНИЕ КЛАССИЧЕСКИХ ШИФРОВ

Изд. № 678836. Формат 60×90/16. Гарнитура «Newton».
Усл. печ. л. 10,5. Уч.-изд. л. 10,2.

ООО «Издательство «КноРус».
117218, г. Москва, ул. Кедрова, д. 14, корп. 2.
Тел.: +7 (495) 741-46-28.
E-mail: welcome@knorus.ru www.knorus.ru

Отпечатано в АО «Т8 Издательские Технологии».
109316, г. Москва, Волгоградский проспект, д. 42, корп. 5.
Тел.: +7 (495) 221-89-80.

ISBN 978-5-406-11995-2

Содержание

Введение

Что же побудило автора написать эту небольшую монографию. Это, в первую очередь, появление свободного времени. И желания поспорить с Клодом Шенноном по вопросу недешифруемости шифра одноразового блокнота, появившегося у автора при написании страницы 89 книги [1] «Бабаш А.В., Шанкин Г.П. Криптография. М., СОЛОН-ПРЕСС, 2002, 512 с.». Дело в том, что К. Шеннон утверждал, что этот шифр является совершенным по открытому тексту и, следовательно, не дешифруемым. В цитированной книги было дано зеркальное понятие совершенности шифра по ключу. Авторам было очевидно, что шифр одноразового блокнота не является совершенным по ключу. Но повседневная суета, трудности с опубликованием книги, авторитет К. Шеннона затормозили работу над доказательством дешифруемости шифра одноразового блокнота. Началом поиска этого доказательства служат статьи и доклады на конференциях. В [2] впервые было упомянут факт о не совершенности шифра одноразового блокнота по ключу и, следовательно, о его возможном дешифровании.

Эта первая ласточка была полностью проигнорирована специалистами. Даже никто не заявил об ошибочности суждений докладчиков. Далее в работах [3–11] сначала уточнялись понятия «дешифруемости» шифра, а затем был проведен подход к дешифрованию шифра одноразового блокнота путем развития методов дешифрования шифра Виженера.

Не все складывалось удачно с публикацией подходов к дешифрованию шифра одноразового блокнота. Рецензенты журналов уровня Scopus, Websines писали по существу, что этого не может быть, так как К. Шеннон сказал, что этого не может быть. И редакции журналов отказывали в опубликовании. То же творилось на конференциях. Лишь в 2022 году представив на конференции РусКрипто тривиальный пример дешифрования шифра Вернама удалось убедить часть специалистов в справедливости публикаций о возможности дешифрования шифра одноразового блокнота. Доклад был опубликован в [12]. В настоящее время практически эта же статья в облегченном формате готовится к публикации в учебнике для техникумов и в журналах под названием «Шифр одноразового блокнота и особенности атаки на него методом Монте-Карло».

Что побудило автора написать небольшую монографию. Это, во вторую очередь, сомнение автора к результатам К. Шеннона по подсчету энтропии на одну букву английского языка и как следствие

сомнение в его расчете расстояния единственности шифра простой замены используемого криптографами и в настоящее время. Подходом к переходу от сомнения к уверенности считаю опубликование метода дешифрования шифра простой замены для коротких текстов с расчетом его надежности. Этот метод дешифрования шифра простой замены в совокупности с новыми методами дешифрования шифров: Джефферсона, Тук-тук, автоматных моделей дисковых шифров и блочных шифров также подтолкнули автора к написанию монографии.

Для читателей, взявших в руки из любопытства монографию, хочу пояснить, что нужно знать для понимания ее содержания. Большинство разделов написаны в автономном стиле. Для изучения материалов необходимо знать простейшие обозначения математики, в частности, простейшие вероятностные понятия и обозначения.

Например, $|M|$ – мощность M. В случае конечного множества это число элементов M. Определение вероятности $P(A)=\frac{v_A}{V}$ события A как отношение числа v_A благоприятных элементарных событий к числу всех V элементарных событий. Дискретное распределение вероятностей (вероятности $P(\zeta = k)$ равенства случайной величины ζ величине k). Условные вероятности. Формула полной вероятности. Выборка объема L из вероятностного распределения (генеральной совокупности случайной величины с заданным вероятностным распределением). Выборочная вероятность. Желательно знать понятие математического ожидания случайной величины, которое принято называть средним значением случайной величины. Остальные понятия теории вероятностей и статистики будут даваться по мере необходимости со ссылками на источники.

Введем ряд простейших алгебраических понятий. Прямое произведения $X\times K$ множеств X и K. Обозначение $K^L = K\times K\times\ldots\times K$ – L-тая степень множества K при прямом произведении K на себя L раз. Понятие функции, которое мы трактуем при необходимости, как отображение множеств. Ограничение отображения множества на его подмножество. Сюръективности и инъективности функций (отображений).

Алгебраическая модель шифра. Пусть X, K, Y – некоторые конечные множества, которые названы, соответственно, множеством открытых текстов, множеством ключей и множеством шифрованных сообщений. На прямом произведении $X\times K$ множеств X и K задана функция

$f: X \times K \to Y$ ($f(x,k) = y$, $x \in X, k \in K, y \in Y$). Функции f соответствует семейство отображений $f_k: X \to Y$, $k \in K$, каждое отображение задано так: для $x \in X$

$$f_k(x) = f(x,k).$$

Таким образом, f_k – ограничение f на множестве $X \times \{k\}$. Здесь $\{k\}$ – множество, состоящее из одного элемента. Заметим, что задание семейства отображений f_k, $k \in K$ однозначно определяет отображение f.

С точки зрения математики введенная четверка $A = (X, K, Y, f)$ определяет трехосновную универсальную алгебру, сигнатура которой состоит из функциональной единственной операции f.

Введенная тройка множеств X, K, Y с функцией f

$$A = (X, K, Y, f)$$

называется **алгебраической моделью шифра К. Шеннона** [13], коротко – шифром, если выполнены два условия: 1) функция f – сюръективна (осуществляет отображение «на» Y); 2) для любого $k \in K$ функция f_k инъективна (образы двух различных элементов различны).

Из условия 2) данного определения вытекает, что $|X| \leq |Y|$. Запись $f_k(x) = y$ называется уравнением шифрования. Имеется в виду, что открытое сообщение x зашифровывается шифром A на ключе k и получается шифрованный текст y. Уравнением расшифрования называют запись $f_k^{-1}(y) = x$ подразумевая, что шифрованный текст $y=f(x,k)$ расшифровывается на ключе k и получается исходное открытое сообщение x.

Требование инъективности отображений f_k, $k \in K$ в определении шифра равносильно требованию возможности однозначного расшифрования шифрованного текста (однозначного восстановления открытого текста по известным шифрованному тексту и ключу). Требование же сюръективности отображения f не играет существенной роли, и оно обычно вводится для устранения некоторых технических, с точки зрения математики, дополнительных неудобств, то есть для упрощения изложения. Подчеркнем, что множество X названо множеством открытых текстов. Его можно понимать, как множество текстов возможных для зашифрования на данном шифре. Это понятие и используется при синтезе шифров. В случае рассмотрения вопросов дешифрования

(определения зашифрованных открытых текстов без знания ключа) предполагают, что шифруются содержательные (читаемые тексты), вследствие чего открытые тексты понимают, как содержательные тексты. Нам же удобно считать, что множество шифруемых содержательных текстов является известным подмножеством M множества открытых текстов X.

Введенная модель шифра отражает лишь функциональные свойства шифрования, расшифрования и дешифрования в классических, с точки зрения истории криптографии, системах шифрования (системах с симметричным ключом).

Вероятностная модель шифра К. Шеннона [13].

Одно из важнейших предположений К.Шеннона при исследовании секретных систем состояло в том, что каждому возможному передаваемому сообщению (содержательному тексту из M) соответствует априорная вероятность, определяемая вероятностным процессом получения сообщения для зашифрования. Аналогично, имеются и априорные вероятности использования различных ключей шифра. Эти вероятностные распределения на множестве открытых текстов и на множестве ключей характеризуют априорные знания криптоаналитика противника относительно используемого шифра. При этом К.Шеннон предполагал, что при дешифровании сам шифр известен противнику. Так полагают и остальные криптографы. В зарубежной литературе термин дешифрование трактуют как расшифрование, а восстановление открытого текста без знания ключа называют атакой.

Вероятностной моделью шифра называется его алгебраическая модель с заданными дискретными, независимыми вероятностными распределениями $P(X)=(p(x),\ x\in X)$, $P(K)=(p(k),k\in K)$ на множествах X и K.

Естественно, вероятностные распределения на X и K индуцируют вероятностное распределение $P(Y)=(p(y),y\in Y)$ на Y, совместные распределения $P(X,K)$, $P(X,Y)$, $P(Y,K)$ и условные распределения.

Для более подробного ознакомления с понятиями, введенными в этом разделе, рекомендуем обратиться, например, к источникам [14,1].

Для удобства читателя большинство разделов написаны в автономном стиле. Нумерация понятий, формул, теорем и т.д. в каждом разделе начинается с 1 и далее.