УДК 517.9.621

КРИПТОГРАФИЯ НОВОГО ПОКОЛЕНИЯ: ИНТЕГРАЛЬНЫЕ УРАВНЕНИЯ КАК АЛЬТЕРНАТИВА АЛГЕБРАИЧЕСКОЙ МЕТОДОЛОГИИ*

Г.К. БРОНШПАК, И.А. ГРОМЫКО, С.И. ДОЦЕНКО, Е.Л. ПЕРЧИК

Показаны преимущества использования в криптографии положений математического анализа, обусловленные свойством функций непрерывного аргумента. В качестве них могут выступать как предварительно представленные рядами графики, таблицы, видеоизображения, так и буквы, числа, символы, в соответствие которым поставлены, например, синусы разной амплитуды. Шифрование производится путем интегрирования функций, дешифрование – путем решения интегральных уравнений. Приведены примеры реализации данных процедур в аналитическом виде. Многообразие вариантов таких преобразований, включая их применение в комбинациях, ставит перед криптоанализом практически непреодолимые проблемы. Рассмотрена возможность использования для криптографической защиты известных решений задач математической физики. Проанализирована сущность высокой эффективности шифрования, базирующаяся на зависимости функций от неограниченного числа информативных признаков.

Ключевые слова: криптография, непрерывный анализ, интегрирование, интегральные уравнения, формулы обращения.

ВВЕДЕНИЕ

В одном из источников по криптографии встретилась трактовка: $A\psi = f$ – шифрование; $\psi = A^{-1}f$ – дешифрование. Возник вопрос: может ли оператор A быть интегральным? Подразумевается следующее:

– шифрование функции $\psi(x)$ путем воздействия интегрального оператора A, как $f(x) = (A\psi)(x)$;

– дешифрование функции $f(x)$, восстановление $\psi(x)$ путем решения интегрального уравнения $(A\psi)(x) = f(x)$, т. е. $\psi(x) = \left(A^{-1}f\right)(x)$;

– соответственно, функция ψ, несущая информацию, должна быть интегрируемой, далее полагаем, что она является однозначной и кусочно-непрерывной.

Однако уловить хотя бы признаки обозначенного подхода в весьма обширной литературе по криптологии не удалось. При этом данная область знаний, будучи очень важной, для практических приложений, разрабатывается весьма интенсивно; накоплены колоссальные объемы материалов по результатам проведенных исследований, которые характеризуются как глубиной логических построений, так и, можно сказать, изощренностью алгоритмических средств реализации. Зримо ощутим громадный труд специалистов за продолжительный период времени. Наряду с чем подчеркивается – основу, как криптографии, так и криптологии, в целом, составляет аппарат дискретной математики, – это преимущественно алгебраическая наука, что в полной мере подтверждают многочисленные публикации. Но математику обычно подразделяют на арифметику, алгебру и анализ (функции непрерывного аргумента, дифференцирование, интегрирование и т. д.), в криптологии, что следует подчеркнуть, отсутствующий.

Поэтому возникают вопросы:

– нельзя ли отнести его (анализа) отсутствие на счет неких факторов историко-субъективистского свойства (по типу незыблемости идей основоположников), инициировавших высокую плотность исследований в рамках именно «алгебраической» криптографии (АК);

– не тесны ли упомянутые рамки для разрешения фундаментальных проблем криптографии с позиций их всеобъемлюще объективной постановки, а также последующего разрешения путем проведения аналитических исследований;

– иначе говоря, какой конструктивизм способен придать аппарат анализа, в первую очередь, преобразования с оператором A (см. выше), криптографии, которую назовем «интегральной» (ИК)?

Цель статьи состоит в том, чтобы на методологическом уровне продемонстрировать высокий потенциал ИК, с точки зрения защиты информации, поскольку для этого возникают качественно новые возможности, не имеющие аналогов в АК. В первую очередь, имеется в виду зависимость функции от непрерывно изменяющегося аргумента. По существу, ниже характеризуется направление глобального исследования проблемы криптографической защиты, с позиций ее практической реализации, которое является, казалось бы, совершенно очевидным, однако в силу непонятных нам причин осталось вне поля зрения специалистов.

В самом деле, – это необъяснимый парадокс, а именно: существует своего рода кладезь алгоритмических средств математического анализа, из которого практически без усилий можно черпать исключительно эффективные, по нашему мнению, варианты организации криптографической защиты. В житейской интерпретации ситуацию можно пояснить и так. Если нужно вырыть

* Статья публикуется как проблемная и редакция надеется, что она более детально будет рассмотрена специалистами.

котлован, то в принципе для этого занятия подходит множество предметов, включая атрибутику бытового обихода. Однако, игнорирование в процессе принятия решений преимуществ экскаватора (подразумеваем непрерывный анализ) представляет собой, очевидно, парадокс, который в полной мере аналогичен рассматриваемой ситуации.

1. НЕТРИВИАЛЬНАЯ СОПРЯЖЕННОСТЬ АК И ИК

Известен аналитический метод шифрования АК [1, с. 20–22]:

$$\sum_{j=1}^{n} a_{ij}\psi_j = f_i,\ i = 1, ..., n, \qquad (1)$$

где $\psi = \{\psi_j\}$ – вектор целых чисел, отвечающих номерам букв некоторого алфавита; $\{a_{ij}\}$ – целочисленная квадратная матрица того же порядка n. К достоинствам такого подхода относят возможность восстановления вектора ψ путем целочисленных преобразований, что исключает погрешность счета, а значит, и неустойчивость используемого алгоритма. Развитию теории данного класса задач посвящена книга [2], прямо не касающаяся криптографии.

Однако не следует выбирать n в (1) достаточно большим, поскольку возможны проблемы, связанные с переполнением машинной памяти, или же появлением машинного нуля [3, п. 14.3]. Наряду с чем, вычисление элементов ψ_i из системы (1), которое фактически производится по правилу Крамера, если, например, $n = 20$, даже на современном этапе, развития техники, требует совершенно нереалистичных затрат машинного времени, фигурирует порядок 10^8 лет [4, с. 43–44].

В свете сказанного, $n \to \infty$ кажется абсурдным. Однако, как отметил Р. Кук: «в то время как теория конечных матриц является частью алгебры, теория бесконечных матриц составляет раздел анализа» [5, с. 13] (заметим, говорят также классический, или непрерывный анализ, подчеркивая характер зависимости от аргумента). Действительно, пусть ψ_j – ординаты бесконечной последовательности чисел (хотя бы и целых), расставленные с шагом Δx вдоль оси абсцисс. Если формально обозначить

$$a_{ij} = k_{ij}\Delta x,\ i, j = 1, ..., n, \qquad (2)$$

то соотношения (1) приобретают вид

$$\sum_{j=1}^{n} k_{ij}\psi_j \Delta x = f_i,\ i = 1, 2, ..., n; \qquad (3)$$

однако, вследствие (2) элементы матрицы

$$\{k_{ij}\},\ i, j = 1, 2, ..., n, \qquad (4)$$

в общем случае, не представляют собой целые числа, а значит, достоинства аналитического метода АК полностью утрачиваются.

Но, на самом деле, в смысле разрешения глобальной проблемы криптографии мы получаем колоссальные преимущества. Действительно, если представить компоненты (3) в эквивалентном виде, несколько изменив обозначения:

$$k_{ij} = k(x_i, \xi_j);\ \psi_j = \psi(\xi_j);\ f_i = f(\xi_i), \qquad (5)$$

где $x_i = i\Delta x$; $\xi_j = j\Delta\xi$, $\Delta x = \Delta\xi$, координаты вектора $f = \{f_i\}$ определяем как

$$\sum_{j=1}^{n} k(x_i, \xi_j)\psi(\xi_j)\Delta x = f(x_i),\ i = 1, 2, ..., n \qquad (6)$$

(суммирование производится по точкам ξ_j; значения в точках x_i данной процедуры играют роль параметров).

Рассматривая, для определенности, отрезок $0 \le x \le 1$, посредством перехода в (6) к пределу $n \to \infty$, соответственно $\Delta x \to 0$, на основании классического определения интеграла получаем

$$(A\psi)(x) = \int_0^1 k(x, \xi)\psi(\xi)d\xi = f(x),\ x \in [0, 1] \qquad (7)$$

(совокупности значений (5) превращаются в функции непрерывного аргумента; $\Delta\xi$ обращается в дифференциал $d\xi$). Относительно функции $\psi(x)$ – это интегральное уравнение Фредгольма первого рода, с ядром $k(x, \xi)$. Мы вернемся к его рассмотрению ниже (п. 5).

Очевидно, $x_i = x$ и $\xi_j = \xi$, когда $n \to \infty$. Таким образом, вместо вектора (1), располагающегося на интервале бесконечной длины, «нужную» ∞ мы организовали посредством разбиения отрезка $0 \le x \le 1$ на бесконечно малые части:

$$\frac{1}{\Delta x} = \infty,\ \Delta x \to 0, \qquad (8)$$

иначе говоря, предельный переход от (6) к (7) осуществляется как

$$\lim_{n\to\infty} \sum_{j=1}^{n} k(x_i, \xi_j)\psi_j(\xi_j)\Delta\xi = \int_0^1 k(x, \xi)\psi(\xi)d\xi$$

и, вместе с тем, здесь присутствует тонкий момент. Действительно, если значения k_{ij} элементов матрицы (4) – конечны, то в условиях (8) элементы матрицы $\{a_{ij}\}$, согласно (2), являются бесконечно малыми. Возникает вопрос в том плане, что умножение «бесконечно малой» матрицы на вектор (1) кажется непривычным, и нет ли для этого специальной теории?

Ответ простой – подобного рода теория в данном случае не актуальна, поскольку без использования приведенных преобразований, а соответственно и аналитического метода АК, «шифровку» $f(x)$, или же уравнение (7), можно получить с помощью сугубо формального приема, а именно путем воздействия оператора

$$A_\bullet = \int_0^1 k(x, \xi)_\bullet\, d\xi, \qquad (9)$$

где ядро $k(x, \xi)$ выбирается произвольно, на функцию $\psi(x)$. Иначе говоря, в рамках исключительно ИК. В этой связи обратим внимание на ключевой, как представляется, момент настоящего изложения.

Если АК, согласно (1), имеет $n \times n$ шифрующих, скажем так, параметров a_{ij} (в примере [1] $n = 3$), то у ядра $k(x, \xi)$ в (9), их бесконечное множество (точки двухмерной функции от непрерывных аргументов). Как соотнести друг с другом по эффективности шифрования ∞ и $n^2 = 9$? Вполне очевидный ответ на этот вопрос убедительно поясняет колоссальные преимущества ИК, о которых, декларативно, упоминалось выше. Заметим также, что вследствие сказанного в отношении (9) осцилляции k_{ij} из (2), обусловленные выбором элементов a_{ij}, становятся несущественными. Мы просто исключаем процедуру упомянутого выбора, она становится ненужной, поскольку ИК ни как не базируется на АК в конструктивном смысле и, тем не менее, искусственно «погрузив» АК в непрерывный анализ, можно судить о взаимосвязанности методов.

2. ПРЕДСТАВЛЕНИЕ ИНФОРМАЦИИ И ТАКТИКА ЕЕ ЗАЩИТЫ

Итак, функция $\psi(x)$ предполагается однозначной и кусочно-непрерывной. Она может представлять:

– аналитические зависимости переменной x разнообразного содержания;

– графики, в частности, акустических амплитуд речевых сообщений, результатов геологических зондирований, тех же кардиограмм;

– фрагменты видеоизображений, сопряжение которых снимает ограничение на однозначность функции $\psi(x)$;

– таблицы чисел, для которых априори предусмотрен способ аппроксимации (так, что после преобразований можно восстановить исходную дискретность), по типу гистограмм;

– буквы, цифры, пробелы текстов, математические символы и другие обозначения, которые трактуются как непрерывные функции, в частности:

$$\psi_s(x) = \alpha_s;\ \psi(x) = \beta_s \sin \omega_s x,\ x \in [0, 1],\ s = 1, 2, \ldots, \quad (10)$$

где α_s, β_s, ω_s – константы; s – номер обозначения в соответствующем алфавите.

Назовем функции: $\psi(x)$ – сообщение; $f(x)$ – зашифрованное сообщение, шифрограмма, или же – шифровка. Фигуранты рассматриваемого процесса и «правила игры»:

– отправитель шифровки $f(x)$, он же автор сообщения $\psi(x)$;

– адресат (коллега, партнер отправителя и т. п.) – лицо, которому предназначено сообщение $\psi(x)$, после дешифрования $f(x)$;

– оппонент – лицо, преследующее целью дешифровать $f(x)$, средствами криптоанализа, для ознакомления с сообщением $\psi(x)$;

– конечно же, предполагается, что оппонент не имеет информации об операторах A, A^{-1}, кстати, как и адресат (см. ниже);

– шифровка $f(x)$ размещается на сайте, практически свободного доступа, становясь известной как адресату, так и оппоненту (очевидно, они могут быть в неединственном количестве);

– по существу $f(x)$ представляет собой именно шифрограмму – кривая на графике, очертание которой поддается подробной детализации (можно назвать ее и видеоизображением);

– предварительно в компьютер адресата отправителем заложен блок программ, позволяющих в автоматическом режиме восстанавливать сообщения $\psi(x)$ по шифровкам $f(x)$;

– упомянутый блок, прямой доступ к которому адресата жестко заблокирован, охватывает весьма большое количество M вариантов программных реализаций и обновляется через достаточно продолжительные периоды времени;

– напротив, номер режима работы $m = 1, 2, \ldots, M$ может быть изменен отправителем в произвольном порядке и сообщается адресату практически открыто, в частности, по телефону.

Что же представляют собой m-варианты программ? Это синхронизированные с шифрованием обратные процедуры восстановления $\psi(x)$ по данной шифровке $f(x)$. Причем факторами надежности, как шифрования, так и соответственно создания практически непреодолимых препятствий для криптоаналитики оппонентов выступают следующие обстоятельства (они могут реализовываться в комплексе, что следует подчеркнуть):

– деформация (попросту говоря, искажение) сообщения $\psi(x)$ под воздействием интегрального оператора A (см. конкретные примеры ниже, пп. 3 – 6);

– использование повторных A^n, $n \geq 2$, а также комбинированных $A_1 A_2 \ldots$ воздействий интегральных операторов различных типов и вида;

– перестановки частей кривых $f(x)$ на графике, а также добавление к ним «ложных» участков (можно предположить, что эффективность таких действий с функциями будет гораздо выше по сравнению с АК, где они применяются для таблиц чисел).

В свете сказанного возникает вопрос о том – можно ли получить количественную оценку эффективности шифрования? Как представляется, здесь трудно предложить что-либо за исключением показателя, характеризующего средний уровень «непохожести», скажем так, нормированных функций $\psi(x)$ и $f(x)$ вида:

$$\mu = \int_0^1 \left[\frac{\psi(x)}{\sqrt{\|\psi\|}} - \frac{f(x)}{\sqrt{\|f\|}} \right]^2 dx,$$
$$\|\psi\| = \int_0^1 \psi^2(x)\,dx;\ \|f\| = \int_0^1 f^2(x)\,dx, \quad (11)$$

или же учесть, в дополнение, большую важность отдельных локализаций по аргументу x с помощью весовых множителей.

3. ПРИМЕРЫ ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ В ЗАМКНУТОМ ВИДЕ

Интеграл

$$(A\psi)(x)=\int_0^x\left[a(x-\xi)+c\right]\psi(\xi)d\xi=f(x), \qquad (12)$$

где a, c – произвольные константы, имеет формулу обращения [6, с. 15]:

$$\psi(x)=\left(A^{-1}f\right)(x)=$$

$$=\frac{1}{c}\frac{d}{dx}\left[\exp\left(-\frac{a}{c}x\right)\int_0^x\exp\left(\frac{a}{c}\xi\right)\frac{d}{d\xi}f(\xi)d\xi\right]; \qquad (13)$$

иначе говоря, (13) представляет собой решение в замкнутом виде интегрального уравнения Вольтерра первого рода (12). Обратимся к первой из функций (10), полагая $\alpha_s\equiv 1$, а значит

$$\psi(x)=1, \qquad (14)$$

и целесообразно воспроизвести все преобразования на основе (12), (13) с тем, чтобы нас было бы легко проверить.

Интегрируя, согласно (12), получаем

$$f(x)=0{,}5ax^2+cx, \qquad (15)$$

соответственно в (13)

$$\frac{d}{d\xi}f(\xi)=a\xi+c$$

и далее:

$$\int_0^x\exp\left(\frac{a}{c}\xi\right)\frac{d}{d\xi}f(\xi)d\xi=cx\exp\left(\frac{a}{c}x\right);$$

умножение этого выражения на $\exp(-ax/c)$ и дифференцирование $c^{-1}d/dx$ восстанавливают (14).

По такой схеме может действовать программа дешифрования с использованием табличных операций интегрирования. Однако упростим задачу, предполагая, что сообщение состоит из последовательности чисел α_s. Зная это, программа определит α_s путем деления значений ординат на шифрограмме и графике (15) при том же аргументе x, поскольку соответствующие им кривые подобны. То есть, оказалось возможным обойтись без формулы обращения (13). И главное, кто скажет, по виду шифровки (15), что она похожа на сообщение (14) в условиях, когда константы a, c варьируются, образно выражаясь, во времени и пространстве? Иначе говоря, как между сообщениями, так и внутри них.

Пусть теперь в (10), а соответственно и (12), функция

$$\psi(x)=\sin\omega x; \qquad (16)$$

тогда шифровка посредством интегрирования приобретает вид

$$f(x)=\int_0^x(ax-a\xi+c)\sin\omega\xi d\xi=$$

$$=\frac{1}{\omega}(ax+c)-\frac{c}{\omega}\cos\omega x-\frac{a}{\omega^2}\sin\omega x, \qquad (17)$$

соответственно в (2)

$$\frac{d}{d\xi}f(\xi)=\frac{a}{\omega}+c\sin\omega\xi-\frac{a}{\omega}\cos\omega\xi$$

и далее:

$$\int_0^x\exp\left(\frac{a}{c}\xi\right)\left(\frac{a}{\omega}+c\sin\omega\xi-\frac{a}{\omega}\cos\omega\xi\right)d\xi=\frac{c}{\omega}e^{\frac{a}{c}x}+$$

$$+\frac{ce^{\frac{a}{c}x}}{\left(\frac{a}{c}\right)^2+\omega^2}\left(\frac{a}{c}\sin\omega x-\omega\cos\omega x\right)-$$

$$-\frac{\frac{a}{\omega}e^{\frac{a}{c}x}}{\left(\frac{a}{c}\right)^2+\omega^2}\left(\frac{a}{c}\cos\omega x+\omega\sin\omega x\right);$$

умножение этого выражения на $\exp(-ax/c)$ и дифференцирование $c^{-1}d/dx$ приводят к (16). То есть, исходная информация восстановлена.

Обратим внимание на следующие моменты:

– шифровка (17), аналогично (15), совсем не напоминает сообщение (16) и значение μ в (11) видится достаточно внушительным;

– представляет интерес построение, в аналитическом виде, рекуррентных соотношений для степеней A^n, $\left(A^n\right)^{-1}$, где A – интегральный оператор (12);

– если функция $\psi(x)$ представлена графически, принципиально отличительных особенностей в процессе преобразований, сравнительно с (16), не возникает, поскольку можно воспользоваться разложением в ряд Фурье:

$$\psi(x)=\sum_n a_n\sin\omega_n x.$$

Известен метод шифрования, посредством умножения большого количества целых чисел (односторонние преобразования). Периодически сообщается о том, что с использованием стольких-то тысяч компьютеров, продолжительность работы которых измеряется в месяцах, удалось разложить на множители результат умножения, а значит произвести дешифрование сложного сообщения. В общем, здесь своеобразный спорт и реклама. Возникает любопытный вопрос: способен ли существующий криптоанализ по графикам функций (15) и (17) определить, что они представляют собой простейшие, заметим, шифровки соответственно 1 и $\sin\omega x$?

У нас большие сомнения, хотя бы потому, что криптоанализ не имеет опыта обращения с «непрерывностью».

4. ИНТЕГРАЛЫ И АНАЛИТИЧЕСКИЕ ФОРМУЛЫ ОБРАЩЕНИЯ

Рассмотрим ряд интегральных уравнений, которые представляются весьма полезными для решения задач криптографии. Уравнения, за исключением одного, взяты из справочника [6], где они дифференцированы в разрезе:

– первого и второго рода (соответственно, функция $\psi(x)$ находится только под интегралом, или также и в явном виде, т. е. вне интеграла);

– пределы интегрирования постоянные, или же одним из них является x.

Пример 1

$$(A\psi)(x)=\int_{\rho}^{x}(ax+b\xi+c)\psi(\xi)d\xi=f(x), \qquad (18)$$

где a, b, c и ρ – произвольные константы. Заметим, что уравнение (12) представляет частный случай (18), когда $b=-a$, $\rho=0$. Таким образом, в (18) появились две дополнительные константы b и ρ, объективно затрудняющие криптоаналитику оппонента.

Формулы обращения интеграла (18) для случаев $b\neq -a$ и $b=-a$ имеют вид соответственно:

$$\psi(x)=d_x\left\{\left[(a+b)x+c\right]^{-\frac{a}{a+b}}\int_{\alpha}^{x}\left[(a+b)\xi+c\right]^{-\frac{b}{a+b}}d_\xi f(\xi)d\xi\right\};$$

$$\psi(x)=\frac{1}{c}d_x\left[\exp\left(-\frac{a}{c}x\right)\int_{\alpha}^{x}\exp\left(\frac{a}{c}\xi\right)d_\xi f(\xi)d\xi\right],$$

где $d_x=d/dx$. Однако, предположим, что конкурент догадается продифференцировать функцию $f(x)$ из (18), Тогда он получает интегральное уравнение Вольтерра второго рода:

$$\psi(x)+\frac{a}{c+(a+b)x}\int_{\rho}^{x}\psi(\xi)d\xi=\frac{d_x f(x)}{c+(a+b)x} \qquad (19)$$

с присутствием искомой функции $\psi(x)$ в явном виде.

Если речь идет об идентификации аномалии качественного характера на графике, свидетельствующей в пользу локализации месторождения, или же волнений финансового рынка, оппонент может добиться преимущества. Особенности, присущие функции $\psi(x)$, будут выделяться на фоне сглаженной интегрированием компоненты. С другой стороны, процедуры численного дифференцирования весьма не точны а, разлагая предварительно функцию $f(x)$ в некоторый ряд, оппонент способен нивелировать имеющиеся у нее особенности.

Пример 2

$$(A\psi)(x)=\int_{0}^{x}\frac{\psi(\xi)d\xi}{x+\xi}=f(x)=\sum_{n=0}^{N}a_n x^n,$$

где a_n – постоянные коэффициенты; т. е. функции $f(x)$ представляет степенной ряд. Формула обращения:

$$\psi(x)=\sum_{n=0}^{N}\frac{a_n}{b_n}x^n,\ b_n=(-1)^n\left[\ln 2+\sum_{m=1}^{n}\frac{(-1)^m}{m}\right] \qquad (20)$$

и вполне можно предположить, что оппонент догадается разложить получаемую графически функцию $f(x)$ в ряд по степеням x. Однако преимуществ от этого он не получит, поскольку далее должен отыскивать b_n фактически путем перебора вариантов, в надежде уловить предметный смысл сообщения. Но подобные действия не имеют смысла, поскольку равносильны априорному разложению в степенной ряд неизвестной функции $\psi(x)$. Напротив, в арсенале адресата, очевидно, окажется программа эффективного суммирования медленно сходящегося ряда (20).

Пример 3

$$(A\psi)(x)=\psi(x)-\lambda\int_{\rho}^{x}\frac{g(x)}{g(\xi)}\psi(\xi)d\xi=f(x), \qquad (21)$$

где функция $g(x)$ и константы λ, ρ – произвольны. Формула обращения:

$$\psi(x)=f(x)+\lambda\int_{\alpha}^{x}e^{\lambda(x-\xi)}\frac{g(x)}{g(\xi)}f(\xi)d\xi$$

и, как нетрудно заметить, в (21), аналогично (19), функция $\psi(x)$ находится в явном виде. Однако здесь обозначенную в привязке к (21) проблему особенностей $\psi(x)$ можно преодолеть, если функция $g(x)$ будет содержать достаточно большое количество их прототипов и в арсенале адресата имеется эффективная программа вычисления осциллирующих интеграла. Такой прием, по существу, представляет собой дезинформацию оппонента.

Пример 4

$$(A\psi)(x)=\psi(x)-\int_{\rho}^{x}g(x)h(\xi)\psi(\xi)d\xi=f(x),$$

где функции $g(x)$, $h(x)$ и константа ρ – произвольны. Формула обращения:

$$\psi(x)=f(x)+\int_{\rho}^{x}R(x,\xi)\psi(\xi)d\xi,$$

где резольвента

$$R(x,\xi)=g(x)h(\xi)\exp\left[\int_{\xi}^{x}g(\xi)h(\xi)d\xi\right];$$

здесь прием дезинформации предыдущего примера посредством функции $g(x)$ может быть еще более эффективным за счет дополнительных возможностей, которые предоставляет выбор $h(\xi)$.

Пример 5. Преобразование Стилтьеса

$$(A\psi)(x)=\int_{0}^{\infty}\frac{\psi(\xi)d\xi}{x+\xi}=f(x); \qquad (22)$$

формула обращения:

$$\psi(x)=\frac{1}{2\pi^2 i}\int_{c-i\infty}^{c+i\infty}x^{-\xi}\sin(\pi\xi)g(\xi)d\xi,$$
$$i^2=-1;\ 0<c<1, \qquad (23)$$

где преобразование Меллина

$$g(\xi)=\int_{0}^{\infty}x^{\xi-1}f(x)dx;$$

следует отметить конструктивизм преобразования (22) в смысле разрешения главной задачи криптографии по защите информации от оппонента. Естественно, предполагается, что адресат

оснащен программой для проведения вычислений по формуле (23).

Перед оппонентом возникает сложнейшая проблема, даже если он допускает возможность использования интегральных преобразований, поскольку:

– их очень большое количество, причем к каждому нужен сугубо индивидуальный подход;

– протестировать на все из существующих преобразований шифровку $f(x)$ практически невозможно;

– численная реализация интегралов с бесконечными пределами встречает существенные осложнения;

– это также касается практической реализации вычислительных методов в комплексной плоскости;

– аналитические преобразования сопряжены с использованием весьма нетривиального аппарата теории специальных функций.

Пример 6

$$(A\psi)(x)=\int_{-\infty}^{\infty}\frac{\psi(\xi)}{|x-\xi|^{1-\lambda}}d\xi=f(x),$$

$$\int_{-\infty}^{\infty}|f(x)|^{p}<\infty;\ 1<p<1/\lambda;\ 0<\lambda<1;$$

формула обращения:

$$\psi(x)=\frac{\lambda}{2\pi}tg\left(\frac{\pi\lambda}{2}\right)\int_{-\infty}^{\infty}\frac{f(x)-f(\xi)}{|x-\xi|^{1+\lambda}}d\xi;$$

можно почти повторить комментарии к предыдущему примеру. Однако обратим внимание, в отличие от него здесь появился параметр λ, допускающий варьирование.

Пример 7

$$(A\psi)(x)=\int_{-\infty}^{\infty}\frac{\psi(\xi)d\xi}{\xi-x}=f(x);$$

формула обращения:

$$\psi(x)=\frac{1}{\pi^2}\int_{-\infty}^{\infty}\frac{f(\xi)d\xi}{\xi-x},$$

где сингулярные интегралы понимаются в смысле главного значения по Коши. Методы вычисления этих интегралов – отдельная тема.

Пример 8. Уравнение Шлемильха

$$(A\psi)(x)=\int_{0}^{\pi/2}\psi(x\sin\xi)d\xi=f(x);$$

формула обращения:

$$\psi(x)=\frac{2}{\pi}\left[f(0)+x\int_{0}^{\pi/2}d_{\xi}f(\xi)d\xi\right]$$

(известно также решение обобщенного уравнения Шлемильха). Подразумевается, что функцию $\psi(z)$ нужно разложить в некоторый ряд по переменной z и затем сделать подстановку $z=x\sin\xi$.

Пример 9. Уравнение Бейтмена

$$(A\psi)(x)=\int_{-1}^{1}\frac{\psi(\xi)d\xi}{\left(1-2x\xi+x^2\right)^{\alpha+1}}=f(x),\ \alpha>-1;$$

формула обращения:

$$\psi(x)=\left(1-x^2\right)^{\alpha+1/2}\int_{0}^{\pi}\gamma\left(x+\sqrt{x^2-1}\cos\vartheta\right)\sin^{2\alpha+1}\vartheta d\vartheta,$$

где

$$\gamma(z)=(\alpha+1)f(z)+zd_zf(z);\ z=x+\sqrt{x^2-1}\cos\vartheta;$$

функции $f(x)$ и $\gamma(z)$ представляют степенные ряды.

Пример 10

$$(A\psi)(x)=\int_{\rho}^{x}k(\xi)\psi(x)\psi(\xi)d\xi=f(x);\qquad(24)$$

формула обращения:

$$\psi(x)=\pm f(x)\left[2\int_{\varepsilon}^{x}k(\xi)f(\xi)d\xi\right]^{-1/2}$$

(неоднозначность $\psi(x)$ в данном случае не принципиальна). Однако уравнение (24) является нелинейным, что вносит заметные изменения. В самом деле, дифференцируя его, получаем:

$$k(x)\psi(x)+d_x\psi(x)\int_{\rho}^{x}k(\xi)\psi(\xi)d\xi=d_xf(x)\qquad(25)$$

и если ядру $k(x)$ придать особенности, о которых говорилось в привязке к (21), трудность идентификации тех особенностей, которые объективно присущи функции $\psi(x)$, у оппонента возрастают. Это обусловливается сложностью выражения (25), включая фактор нелинейности.

Пример 11

$$(A\psi)(x)=\int_{\rho}^{x}k(x,\xi)w(\xi,\psi(\xi))d\xi=f(x);\qquad(26)$$

замена

$$w(x)=w(x,\psi(x))\qquad(27)$$

приводит к линейному уравнению

$$\int_{\rho}^{x}k(x,\xi)w(\xi)d\xi=f(x),\qquad(28)$$

что порождает предпосылки неординарно эффективной защиты информации. В самом деле, дифференцируя (28), получаем

$$k(x,x)w(x)+\int_{\rho}^{x}\partial_xk(x,\xi)w(\xi)d\xi=d_xf(x),$$

однако, в отличие от (19), здесь присутствие функции $w(x)$ практически не представляет опасности, поскольку имеется неограниченный выбор вариантов зависимости (27). Несомненно, он может быть сделан так, что по виду $w(x)$ не удастся выносить какие-либо заключения в отношении сообщения $\psi(x)$. В целом, оптимизация структуры зависимости (27) под углом зрения защиты информации (и в контексте (26)) представляет, по нашему мнению, весьма интересную тему самостоятельного исследования.

5. ИНТЕГРАЛЬНОЕ УРАВНЕНИЕ ФРЕДГОЛЬМА ПЕРВОГО РОДА

Итак, вновь займемся уравнением (7), которое представляет собой совершенно особый объект. Если, например,

$$k(x,\xi)=k(\xi);\ k(x,\xi)=xk(\xi), \qquad (29)$$

шифровка приобретает вид соответственно:

$$f(x)=c_0;\ f(x)=c_1x, \qquad (30)$$

где c_0, c_1 – некоторые константы. Таким образом, в процессе интегрирования происходит уничтожение информации о функции $\psi(x)$, восстановить которую, в принципе, невозможно. Математически это проявляется в бесконечном множестве решений уравнения (7), ядра и свободные члены которого определяются согласно (29), (30).

Решение уравнения (7) является единственным, если ядро $k(x,\xi)$ замкнуто, что означает:

$$\int_0^1 k(x,\xi)\varphi(\xi)d\xi=0,\ x\in[0,1], \qquad (31)$$

лишь в том случае, когда функция $\varphi(x)=0$; математики дополняют данное равенство понятием «почти всюду» [7, с. 119, 185–187] и, кроме того,

$$\sum_{n=1}^{\infty}a_n^2\lambda_n^2<\infty,\ a_n=\int_0^1 f(\xi)\psi_n(\xi)d\xi,$$

где λ_n; $\psi_n(x)$ – характеристические числа и собственные функции ядра $k(x,\xi)$, которое предполагается симметричным, т. е. $k(x,\xi)=k(\xi,x)$. Отметим, что процедуры определения λ_n, $\psi_n(x)$ в целом благоприятны для их реализации (отдельная тема, см. [8, п. 10]). Своя специфика возникает, когда ядро $k(x,\xi)$ несимметрично, или же уравнение (31) имеет конечное число нетривиальных решений, однако в настоящем она менее актуальна.

В качестве ядра уравнения (7) подходит, например:

$$k(x,\xi)=\begin{cases}(1-x)\xi,\ 0\le\xi\le x;\\ x(1-\xi),\ x\le\xi\le 1\end{cases} \qquad (32)$$

[8, с. 149]; здесь приведен целый ряд аналогичных выражений. Заметим, что замкнутые ядра могут быть искусственно сконструированы, их множество является неограниченным. Так, вполне подходит решение элементарной задачи об изгибе балки единичной длины и переменного сечения, свободно опертой по краям. В таком случае $k(x,\xi)$ представляет прогиб в сечении с координатой x от единичной силы, приложенной в сечении с координатой ξ.

Однако в чем заключается упомянутая выше особенность интегрального уравнения, с точки зрения, как можно понять, его необычности? Суть в том, что без знания ядра $k(x,\xi)$ восстановление функции $\psi(x)$ из уравнения (7) является невозможным, даже теоретически. Иначе говоря, такой способ шифрования обладает абсолютной надежностью. Казалось бы, исключительно важный результат для криптографии, ее можно назвать безоговорочная «победа» над криптоанализом. Но где формула обращения интеграла (7), которая была бы аналогичной тем, которые приводились выше? Ответ простой: ее не существует. Тогда должен быть программно-алгоритмический продукт, иначе как же справится с шифрограммой адресат?

Все обстоит иначе и ситуация в данной сфере является весьма интересной, поскольку алгоритм и работающая в автоматизированном режиме по данным уравнения (7) программа до настоящего времени, остаются трудно стыкующимися между собой субстанциями. Фундаментальная причина здесь в том, что решение интегрального уравнения Фредгольма первого рода (7) с ядром без благоприятствующих особенностей (для нас они, на данном этапе, неактуальны), представляет собой некорректную задачу. Подразумевается, что малые вариации данных в совершенно неадекватной степени сказываются на решении. Даже вычислив $f(x)$ в аналитическом виде по формуле (7) для ядра (32) и, например, функции $\psi(x)=\sin\omega x$, не удается восстановить ее обратно, оставаясь в рамках исключительно теперь уже интегрального уравнения (7) из-за округлений значащих цифр в машинной памяти.

Что же делают в такой ситуации? Существует несколько разных подходов, которые хорошо раскрыты в справочнике [9, п. 4]. Наиболее популярная идея состоит в рассмотрении вместо (7) интегрального уравнения:

$$\alpha\psi(x)+\int_0^1 k(x,\xi)\psi(\xi)d\xi=f(x),\ x\in[0,1], \qquad (33)$$

где $\alpha>0$ – малый параметр. Формально (33) – весьма хороший объект для численной реализации: интегральное уравнение Фредгольма второго рода, однако, если параметр α не слишком мал. Но в таком случае решение уравнения (33) – совсем другая задача, нежели (7). В общем, «игра» идет на паллиативе выбора α.

Но хуже другое обстоятельство. В не имеющей, наверное, аналогов книге, которая посвящена достаточно объективной апробации большого количества вычислительных методов, Р.П. Федоренко отмечает: «Автором была предпринята попытка использовать этот подход, однако она оказалась неудачной: трудно подобрать нужное значение α. При слишком малых α не получалось гладкого решения, при больших α значение F_0 заметно превосходило минимальное» [10, с. 349–350]. Здесь F_0 – функционал, отвечающий уравнению (33). И далее описывается, как автор выходил из положения с использованием искусственных приемов. Иначе говоря, задача решалась в режиме вычислительного эксперимента с участием человека, что следует подчеркнуть.

Аналогично и А.Ф. Верлань, и В.С. Сизиков по итогам аналитического обзора предлагают свой «способ модельных (эталонных) примеров». «Он заключается в том, что значение α в неко-

тором исходном примере (уравнении, задаче) P выбирается на основе решения вспомогательного (модельного) примера Q (или нескольких модельных примеров) с известным (заданным) точным решением» [9, с. 246–249]. Последующий материал о практической реализации метода свидетельствует, что он также базируется на проведении вычислительного эксперимента, а значит участии человека. Что в этом плохого для криптографии? Суть в том, что существующие методы решения интегральных уравнений Фредгольма первого рода являются не формализованными (о чем профильные источники предпочитают умалчивать), а значит, их нельзя запрограммировать для работы в автоматизированном режиме, т. е. без какого-либо участия адресата. Иначе он превращается в криптоаналитика, или же должен кого-то нанять, что является для нас совершенно неприемлемым, также и с точки зрения вероятных утечек информации.

Претензия (поскольку конкретные вычисления не производились) на разработку в полной мере формализованного алгоритма решения интегральных уравнений Фредгольма первого рода содержится в работе [11]. Идея состоит в том, что причина его некорректности всем понятна: сглаживание информации процедурой интегрирования. Так следует не только лишь иметь это в виду и обговаривать, а благоприятным для последующих выкладок способом смоделировать математически. Предложена модель такого сглаживания, или же – погрешности, которая принимается равной нулю, с искомой функцией $\psi(x)$ в явном виде:

$$\delta(x)=\psi(x)-\lambda\int_{-1}^{1}h(x,\xi)\psi(\xi)d\xi=0,\ x\in[0,1],\quad(34)$$

где λ – постоянный параметр; $h(x,\xi)$ – ядро Пуассона в области $x\in[0,1]$, $\xi\in[-1,0]$.

Наряду с чем, без использования (34) мы имеем уравнение (7), полностью отвечающее причинно-следственной связи в постановке прямой задачи: изгиб балки; отражение светового луча и т. п. Однако формулировать обратную задачу путем тривиального переименования известной и неизвестной функций в (7), без использования дополнительной информации, является недопустимым. Действительно, процесса «хождения луча назад» не существует. В результате, вообще говоря, нетривиальных преобразований на основе (7) и (34) вычисление функции $\psi(x)$, в предположении ее гармоничности, сводится к решению интегрального уравнения Фредгольма второго рода. Предельный переход $r\to1$ в ядре данного уравнения позволяет свести рассматриваемую задачу к решению весьма благоприятной системы линейных алгебраических уравнений относительно коэффициентов ряда Фурье функции $\psi(x)$. Таким образом, она перетекает в более представительный класс функций, квадратично суммируемых на интервале $0\le x\le1$.

6. ДРУГИЕ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

Выше рассматривались формулы обращения, дающие решения интегральных уравнений в аналитическом виде. Но наряду с этим существуют эффективные алгоритмы численного решения интегральных уравнений [9, пп. 1, 3]. Это касается интегрального уравнения Фредгольма второго рода

$$(A\psi)(x)=\psi(x)-\lambda\int_{0}^{1}k(x,\xi)\psi(\xi)d\xi=f(x),\quad x\in[0,1],\quad(35)$$

где λ – параметр, отличный от характеристического числа, решение которого, может быть представлено также и через резольвенту:

$$\psi(x)=f(x)+\lambda\int_{0}^{1}R(x,\xi,\lambda)f(\xi)d\xi,\ x\in[0,1];$$

следует отметить метод численной реализации $R(x,\xi,\lambda)$, разработанный С.Г. Михлиным [12, п. 12]. В целях защиты информации ядро $k(x,\xi)$ можно задавать с разрывами по переменной x, координаты которых, синхронно с программой адресата, варьирует отправитель. Еще проще, нежели (35), решаются интегральные уравнения Вольтерра второго рода:

$$(A\psi)(x)=\psi(x)-\int_{0}^{x}k(x,\xi)\psi(\xi)d\xi=f(x);$$

свои интересные возможности содержит оператор Вольтерра первого рода, существенно искажающий информацию о функции $\psi(x)$, а также аппарат теории нелинейных интегральных уравнений (см. в частности, [7, пп. 4.5, 4.6]). Заметим, что весьма существенные трудности для оппонента может доставить использование ядер $k(x,\xi)$, приводящих к необходимости вычисления интегралов вида

$$\int_{0}^{1}\varphi(x)\exp\left[\mu w(x)\right]dx,$$

где μ – большой параметр; функция $w(x)$ является достаточно гладкой. Для этого требуются тонкие методы асимптотического анализа, которые в очень ясной форме представил М.В. Федорюк [13].

И здесь весьма важное обстоятельство, суть которого заключается в следующем. Данные интегральных уравнений задач математической физики, в первую очередь, ядра определяются содержанием рассматриваемых задач предметной области. От свойств упомянутых ядер зависит, в частности, возможность решения нелинейных интегральных уравнений путем последовательных приближений. Однако дешифрование $f(x)$ позволяет задавать ядра из соображений совсем иного толка, вследствие чего могут параллельно решаться вопросы упрощения вычислительных процедур. В общем, сфера защиты информации выдвигает перед теорией интегральных уравне-

ний необычные для нее постановки задач, которые, как нам представляется, заинтересуют специалистов.

Возникает вопрос – не могут ли, наряду с интегральными уравнениями, оказаться полезными для аналогичных целей также и дифференциальные уравнения? Рассмотрим простейший пример для дифференциального уравнения первого порядка

$$d_x\psi + a(x)\psi = f(x), \qquad (36)$$

имеющего решение:

$$\psi(x) = \exp\left[-\int a(x)dx\right]\left\{c + \int f(x)\left[\exp\int a(x)dx\right]\right\}dx,$$

где c – константа интегрирования, определяемая из начального условия:

$$c = \frac{\psi(0)}{\exp\left[-\int a(x)dx\right]} - \int f(x)\left[\exp\int a(x)dx\right]dx\Bigg|_{x=0},$$

а значит, наряду с функцией $f(x)$, адресату нужно знать величину $\psi(0)$, которая зависит от конкретного сообщения. Данное обстоятельство является очень неудобным. Однако мы легко преодолеваем его путем сведения (36) к интегральному уравнению относительно функции $\psi_*(x) = d_x\psi(x)$, откуда с учетом начального условия

$$\psi(x) = \int_0^x \psi_*(\xi)d\xi + \psi(0).$$

Можно ли на этом основании сделать вывод о том, что дифференциальные уравнения для шифрования не нужны? Нет, они могут быть очень полезны, однако в другом контексте. Подразумевается, например, восстановление линейного оператора задачи Штурма – Лиувилля по его спектральным характеристикам [14, с. 9–11]. Как отметил Б.М. Левитан, это могут быть спектры (для разных граничных условий), спектральная функция, данные рассеяния. Применительно к рассматриваемой проблематике, вначале отправитель решает прямую задачу:

$$-d_x^2u + \psi(x)u = \sigma u,\ d_xu(0) = d_xu(\pi) = 0 \qquad (37)$$

для данной функции $\psi(x)$, которая предполагается непрерывной, по определению собственных значений σ_0, σ_1, ...

Эту или же аналогичную ей, информацию программное обеспечение адресата использует для решения обратной задачи восстановления $\psi(x)$ на основе математического аппарата [14]. Обратим внимание, здесь присутствует принципиально новый инструмент защиты информации по сравнению с материалом, который изложен выше, а именно: восстановление полезной информации осуществляется путем решения, с использованием глубоко продвинутой математики, весьма содержательной задачи (37). В связи с чем, на оппонента, можно сказать, обрушивается огромный объем информации высокого потенциала, которую, с его позиций, можно назвать «лишней».

Аналогичный инструмент защиты информации предоставляет нам пример из книги [15, с. 4] для уравнения с частными производными. Пусть $\psi(x)$ – непрерывная на всей числовой оси x функция и $u(x, y)$ – решение задачи Коши:

$$\left[\partial_x + \partial_y + \psi(x)\right]u = 0,\ u(x, 0) = \varphi(x), \qquad (38)$$

где функции $\psi(x)$; $\varphi(x)$ даны. Задача определения $u(x, y)$ – корректна, для существования классического решения достаточно потребовать непрерывной дифференцируемости $\varphi(x)$. Постановка обратной задачи предполагает отыскание функции $\psi(x)$ из (38) по информации о решении: $u(0, y) = \phi(y)$. Если $\phi(x) \neq 0$ в рассматриваемой области, то решение этой задачи однозначно. Для его существования необходимо и достаточно выполнение условий: функция $\phi(y)$ – непрерывно дифференцируема; $\phi(y)/\varphi(y) > 0;\ \phi(0) = \varphi(0)$. В таком случае решение имеет вид

$$\psi(x) = -\frac{d}{dx}\ln\frac{\phi(x)}{\varphi(x)}.$$

В.Г. Романов рассмотрел также целый ряд гораздо более сложных задач, с использованием решений которых мы могли бы весьма эффективно загружать оппонента потоками лишней информации. К ним, в частности, относятся обратные задачи определения плотности тепловых источников и коэффициента диффузии [15, пп. 6.1, 6.2]. В таком же аспекте очень эффективен аппарат парных уравнений, на высоком уровне представленный Н.А. Вирченко [16]. В самом деле, как подлежащая шифрованию функция $\psi(x)$, так и шифровка $f(x)$ подвергаются здесь эшелонированному воздействию, можно сказать, информационно супернасыщенных операторов. Причем, вновь на передний план выходят процедуры интегрирования. Приведем лишь сравнительно несложный пример [6, с. 459].

Решение парного интегрального уравнения

$$\int_0^\infty g(\xi)J_0(x\xi)\psi(\xi)d\xi = f(x),\ 0 < x < a; \qquad (39)$$

$$\int_0^\infty \xi J_0(x\xi)\psi(\xi)d\xi = 0,\ a < x < \infty, \qquad (40)$$

где функция $g(x)$ – дана; $J_0(x)$ – функция Бесселя нулевого порядка, имеет вид

$$\psi(x) = \int_0^a \varphi(\xi)\cos(x\xi)d\xi; \qquad (41)$$

функция $\varphi(x)$ определяется из интегрального уравнения Фредгольма второго рода:

$$\varphi(x) - \frac{1}{\pi}\int_0^a K(x, \xi)\varphi(\xi)d\xi = \phi(x),\ 0 < x < a, \qquad (42)$$

симметричное ядро $K(x, \xi)$ и свободный член $\phi(x)$ даются выражениями

$$K(x, \xi) = 2\int_0^\infty \left[1 - g(\vartheta)\right]\cos(x\vartheta)\cos(\xi\vartheta)d\vartheta; \qquad (43)$$

$$\phi(x)=\frac{2}{\pi}\frac{d}{dx}\int_0^x\frac{\xi f(\xi)}{\sqrt{x^2-\xi^2}}d\xi. \qquad (44)$$

Обратим внимание на следующие моменты:

– по формуле (39) отправитель, казалось бы, аналогично предыдущему (см. пп. 3, 4), вычисляет $f(x)$, шифруя сообщение $\psi(x)$, $0<x<a$, однако с выбором функции $g(x)$, а также произведения $g(x)\psi(x)$, $x>a$, возникает неопределенность;

– очевидно, для существования интегралов (39), (40) на функции $\psi(x)$, $g(x)$, $x>a$ должны налагаться некоторые ограничения;

– программа адресата восстанавливает $\psi(x)$ по формуле (41) что, как и решение интегрального уравнения (42), вообще говоря, не должно вызывать принципиальных осложнений, однако, многое определяется выбором функции $g(x)$, это касается также интеграла (43),

– весьма непростым, вследствие сингулярности, без предварительной подготовки, является вычисление функции (44);

– резюмируя обозначенные моменты, можно сделать вывод о том, что нет у оппонента малейшего шанса для идентификации сообщения $\psi(x)$, $0<x<a$, если ему не известна постановка задачи (39), (40).

7. ИЗ СОВРЕМЕННОЙ АЛГЕБРЫ В НЕПРЕРЫВНЫЙ АНАЛИЗ: ОБРАТНО (НАЗАД)

Конечно, под «алгеброй» здесь подразумеваются алгебраическая геометрия и алгебраическая теория чисел, лежащие, как известно, в основе АК. То есть, это разделы современной алгебры, развитию которых способствовали теория чисел, алгебра, а также, в первую очередь, наверное, анализ, о чем свидетельствует приведенная ниже выдержка, в их классическом понимании. В этой связи интересно пояснение С.М. Никольского: «Математический анализ – часть математики, в которой функции и их обобщения изучаются методами пределов. Понятие предела тесно связано с понятием бесконечно малой величины, поэтому можно также говорить, что математический анализ изучает функции и их обобщения методом бесконечно малых. ... В математическом анализе исходят из определения функции по Лобачевскому и Дирихле. Если каждому x из некоторого множества F чисел в силу количественного закона приведено в соответствие число y, то этим определяется функция $y=f(x)$ от одного переменного x» (МЭ, 1982. – Т. 3. – С. 591).

Большой интерес представляют соображения Ф.А. Медведева о взаимосвязи анализа с теорией функций, поскольку последняя в значительной мере повлияла на облик АК (см. ниже): «Если исключить из классического анализа теорию дифференциальных уравнений и теорию функций комплексного переменного, выделившихся в огромные самостоятельные отрасли математического знания, то можно сказать, что теория функций действительного переменного есть просто расширенный, углубленный и обобщенный математический анализ» [17, с. 9]. И далее: «Тесная взаимосвязь анализа и теории функций порой неуловимые переходы их друг в друга приводят к вопросу о взаимоотношении этих двух математических дисциплин. Действительно ли это разные науки, и если да, то чем они отличаются одна от другой?

Первое бросающееся в глаза отличие заключается в отсутствии в явном виде теоретико-множественных представлений в классическом анализе и привлечения их в очень большом объеме к теории функций. Исходный объект анализа – функция – всегда определена на некоторой нерасчлененной части области – отрезке, прямой, куске плоскости, объеме пространства. Напротив, в теории функций она вообще задается на некотором множестве точек, и ее свойства существенно зависят от характера множества, на котором она задана; естественно поэтому, что изучению функций здесь предпосылается изучение множеств. Более того, такое предпослание необходимо и потому, что решение многих вопросов теории функций зависит от решения теоретико-множественных вопросов.

Укажем только один пример. В классическом анализе для того, чтобы решить вопрос интегрируема или нет заданная функция, нужно было попросту вычислить ее интеграл, или установить, что рассматриваемая функция принадлежит определенному классу функций, для которых определено понятие интеграла, причем сам этот класс вводится способом, не апеллирующим к теории множеств. Напротив, для того, чтобы ответить на вопрос об интегрируемости функции по Риману, необходимо и достаточно узнать, равна ли нулю мера множества точек ее разрывов. Так обстоит дело в большинстве вопросов теории функций. И не случайно еще на заре зарождения современной теории функций один из ее основателей Р. Бэр, писал в 1899 г.: «... в том порядке идей, которыми мы занимались, все проблемы относительно функций сводятся к вопросам, относящимся к теории множеств; и в той мере, в какой эти последние продвинуты или могут быть продвинуты вперед, в такой же мере можно решить более или менее полно данную проблему» [17, с. 10].

В первой половине 1930-х гг., появились два курса под одинаковым названием «Теория функций», которые приобрели большую известность, став классическими [18, 19]. При этом авторы очень различно трактуют содержание предмета теории функций. Объединяет их, пожалуй, лишь отсутствие теоретико-множественных конструкций. У Е. Титчмарша в чистом виде анализ с охватом широкой проблематики, по которой даны разъяснения наиболее тонких моментов. В общем, корреляция ИК с методологией [18] очевидна. В этом смысле материал [19] можно назвать противоположным, поскольку здесь преимущественно комплексный анализ в контексте

его геометрических интерпретаций. Во второй части [19] рассмотрены эллиптические функции, а также кривые, причем на данный материал ссылаются в качестве его идейной предтечи алгебраической геометрии. «Эллиптическая кривая является истоком большей части современной алгебраической геометрии. Но исторически теория эллиптических кривых возникла как часть анализа – «теории эллиптических интегралов и эллиптических функций» (МЭ, 1985. – Т. 5. – С. 979). Таким образом, существует прямой путь к АК от раздела классического анализа через теорию функций, в смысле [19].

Другая основа АК – алгебраическая теория чисел, естественно, обусловливается тем, что традиционный инструмент шифрования – целое число. Как представляется, здесь АК в большей мере адаптировалась к уже сложившейся теории. Однако весьма интересное обстоятельство заключается в том, что из классической алгебры можно также перейти к непрерывному анализу, включая ИК. Только лишь следует взять подходящий для этого ее раздел, а именно – линейную алгебру. Напомним, что выше (п. 1) мы уже продемонстрировали предельный переход от конечного алгебраического ряда к анализу и ИК, следуя [5]. Однако сейчас обратим внимание на теорию Фредгольма, в которой вывод интегрального уравнения, а также построение общей теории его решения осуществляются путем предельного перехода к бесконечной системе линейных алгебраических уравнений.

Как отметил И.И. Привалов: «Полное исчерпывающее решение задачи было дано Фредгольмом в 1904 г., и эта работа Фредгольма содержит самое выдающееся открытие начала XX в. в области анализа, после которого быстро развивается теория интегральных уравнений. Основная идея Фредгольма состоит в том, что интегральное уравнение (35) рассматривается как предельное состояние для системы n линейных алгебраических уравнений с n неизвестными, когда n неограниченно возрастает» [20, с. 39]. По мнению, Э. Гурса, полученный Фредгольмом результат о том, что «резольвента есть частное от деления двух функций, целых относительно λ, ..., т. е. мероморфная функция параметра λ, является очень существенным, и предвидеть его заранее было бы трудно» [21, с. 51].

Приведем некоторые соображения:

– как АК, так и ИК имеют истоки в классической алгебре, однако – разных ее разделах (в первом случае – это многочлены и группы, во втором – системы линейных уравнений);

– АК также имеет одним из своих истоков классический анализ (эллиптические функции), тогда как ИК полностью, и очень органично, находится в его сфере;

– напротив, АК на переднем крае математики (современная алгебра), а соответственно ей присущи большая степень абстракции, сложность для восприятия и т. п. аспекты;

– однако при этом АК осталась «алгеброй», которая оперирует с целыми числами, ставя перед криптоанализом задачи дискретного характера (т. е., в них конечное число неизвестных);

– ИК, напротив, оперирует с функциями, за каждой из которых неограниченное количество информативных, скажем так, признаков – значений в точках непрерывного аргумента.

Вместе с тем, функции можно рассматривать и как символы. В самом деле, за символом, например, sin располагается неограниченное множество его значений, отвечающих бесконечно малому приращению аргумента ωx на интервале $0 \le x \in \le 1$. Хотя и ωx можно трактовать как функцию x. Причем, преобразуется до полной неузнаваемости (для оппонента) как единственный символ, так и их сложные композиции. Соответственно значения функции, например, $\sin \omega x$, после дешифрования путем преобразований, зачастую, также в категориях, исключительно символов, адресат может определять с высокой степенью точности. Подробнее раскроем принципиальное преимущество ИК, заключающееся в том, что данные, которые подлежат шифрованию, включая буквы и обозначения, можно представлять функциями непрерывного аргумента.

У них, во-первых, радикально более широкий спектр возможных преобразований, по сравнению с наборами целых чисел АК. И, во-вторых, в ИК мы имеем качественно отличительную особенность своего рода экономичности, поскольку преобразования происходят с объектами высоко-информационной насыщенности, а именно – функциями непрерывного аргумента, которые выражаются символам. Вследствие этого, они ничтожно малы в машинной памяти. С другой стороны, данные символы можно трактовать и в качестве операторов, воздействующих на функции, причем даже когда мы имеем графики, поскольку они разлагаются в ряды, представляющие собой аналитические выражения. Соответственно в машинной памяти не требуется хранить большие массивы чисел, по ходу реализации алгоритма их генерируют операторы. Подобного рода возможностей абсолютно лишена существующая криптография.

В заключение хотелось бы отметить, что представленный материал, конечно, заслуживает того, чтобы в совершенно ином ракурсе оценить потенциал криптологии в целом. Причем, его содержание является, в общем-то, несложным, хотя и охватывает широкий спектр позиций, а идейная сторона, как говорится, лежала на поверхности. В этом отношении мы уже выражали недоумение (введение). Однако, глядя на ситуацию с другой стороны, приведем определения: «Алгебра – часть математики, посвященная изучению алгебраических операций» (МЭ, 1977. – Т. 1. – С. 114). «Алгебраическая операция – n-арная операция на множестве A – отображение $\omega: A^n \to A$ n-й декартовой степени множества A в само множе-

ство A. Число n называется арностью алгебраической операции. ...В XX в. появилось понятие бесконечно местной операции, т. е. отображение $\omega: A^{\alpha} \to A$, где α – произвольное кардинальное число» (там же, с. 159).

Имеется в виду следующее. Если человек действительно мыслит категориями теории множеств, да еще и разделяет мрачное, как нам представляется, «пророчество» Бэра (см. цитату [19] выше), то для такой ментальности наш материал, наверное, окажется чужеродным. Кстати, следует заметить, что математическая «современность» для криптографии далеко не главный показатель. На первом месте здесь, очевидно, должна быть коммерческая эффективность, а также и аспекты социально-политического характера. В общем, мы, как смогли, постарались пояснить название раздела о том, почему целесообразно вернуться назад (подразумевается развитие математической науки во времени) – в сферу непрерывного анализа.

ВЫВОДЫ

1. Как показал информационный поиск, аппарат непрерывного анализа не привлекают для целей криптографической защиты, что представляется удивительным с позиций следующего подхода: шифрование посредством интегрирования функции, которая может олицетворять хотя бы и число; дешифрование – путем решения интегрального уравнения.

2. Аналитический метод криптографической защиты, с помощью перемножения целочисленных матрицы и вектора, удается использовать лишь в случае очень малой размерности, однако, казалось бы, парадокс – в условиях ее неограниченности мы получаем интегральное уравнение Фредгольма первого рода, что свидетельствует в пользу непрерывного анализа.

3. Поскольку подходящих для криптографической защиты интегральных операторов весьма много, то дешифрование, в автоматизированном режиме, целесообразно производить для большого количества номеров настроек, которые сообщаются адресату, хотя бы и открыто, прямого доступа к программному обеспечению он иметь не должен.

4. В целом ряде случаев, как интегрирование функций, так и их восстановление по формулам обращения удается производить в замкнутом виде, более того, вручную, причем, как показывают конкретные примеры, шифрограммы совсем не напоминают исходные сообщении, а значит, у криптоанализа возникают весьма серьезные проблемы.

5. Приведен ряд интегралов, с формулами обращения в аналитическом виде, на основании которых, учитывая их последовательные применения, различного рода комбинации, а также другие приемы, становится совершенно очевидным, что предлагаемый метод криптографической защиты ставит перед криптоанализом, по нашему мнению, практически неразрешимые задачи.

6. Интегральное уравнение Фредгольма первого рода, вследствие своей некорректности, представляет особый интерес, поскольку, не зная ядра, криптоаналитик не в силах выполнить дешифрование даже теоретически, однако, алгоритмы его решения не могут работать без участия человека (производится вычислительный эксперимент); преодолению данного обстоятельства посвящена наша публикация 2005 года.

7. Для целей криптографической зашиты можно «заглянуть» также и в другие разделы анализа, в частности, это – задачи математической физики, решения которых, вследствие своей содержательности, могут преподносить криптоаналитику большой объем лишней для него информации, в условиях, когда сообщение адресату представляет, например, какой-нибудь коэффициент теплопроводности.

8. Истоком алгебраической геометрии, на которой в значительной мере базируется криптология современного формата, является математический анализ и поскольку использование функций непрерывного аргумента имеет в процедурах шифрования – дешифрования неоспоримые преимущества над дискретностью, то следует, по нашему мнению, образно выражаясь, «вернуться назад» (т. е., в непрерывный анализ).

Литература

[1] *Крыжановский А.В.* Средства обеспечения информационной безопасности в сетях передачи данных: задачи и методические указания / А.В. Крыжановский, Н.В. Киреева, В.В. Пугин. – Самара: Поволжская государственная академия телекоммуникаций и информатики. – 2008. – 61 с.

[2] *Грегори Р.* Безошибочные вычисления. Методы и приложения / Р. Грегори, Е. Кришнамурти. – М.: Мир, 1988. – 208 с.

[3] *Форсайт Дж.* Численное решение систем линейных алгебраических уравнений / Дж. Форсайт, К. Молер. – М.: Мир, 1969. – 168 с.

[4] *Форсайт Дж.* Машинные методы математических вычислений / Дж. Форсайт, М. Малькольм, К. Моулер. – М.: Мир, 1980. – 280 с.

[5] *Кук Р.* Бесконечные матрицы и пространства последовательностей / Р. Кук. – М.: Физматгиз, 1960. – 472 с.

[6] *Полянин А.Д.* Справочник по интегральным уравнениям / А.Д. Полянин, А.В. Манжиров. – М.: Физматлит, 2003. – 608 с.

[7] *Трикоми Ф.* Интегральные уравнения / Ф. Трикоми. – М.: Изд-во иностр. лит., 1960. – 300 с.

[8] *Краснов М.Л.* Интегральные уравнения / М.Л. Краснов, А.И. Киселев, Г.И. Макаренко. – М.: Наука, 1976. – 216 с.

[9] *Верлань А.Ф.* Интегральные уравнения: методы, алгоритмы, программы. Справочное пособие / А.Ф. Верлань, В.С. Сизиков. – К.: Наукова думка, 1986. – 544 с.

[10] *Федоренко Р.П.* Приближенное решение задач оптимального управления / Р.П. Федоренко. – М.: Наука, 1978. – 488 с.

[11] *Перчик Е.* Методология синтеза знаний: преодоление фактора некорректности задач математического моделирования / www.pelbook.narod.ru (2-я ред.)

[12] *Михлин С.Г.* Некоторые вопросы теории погрешностей / С.Г. Михлин. – Л.: Изд-во Ленингр. ун-та, 1988. – 334 с.

[13] *Федорюк М.В.* Асимптотика: Интегралы и ряды / М.В. Федорюк. – М.: Наука, 1987. – 544 с.

[14] *Левитан Б.М.* Обратные задачи Штурма – Лиувилля / Б.М. Левитан. – М.: Наука, 1984. – 240 с.

[15] *Романов В.Г.* Обратные задачи математической физики / В.Г. Романов. – М.: Наука, 1984. – 264 с.

[16] *Вірченко Н.О.* Парні (*N*-арні) інтегральні рівняння / Н.О. Вірченко. – К.: Задруга. – 2009. – 475 с.

[17] *Медведев Ф.А.* Очерки истории теории функций действительного переменного / Ф.А. Медведев. – М.: Наука, 1975. – 248 с.

[18] *Титчмарш Е.* Теория функций / Е. Титчмарш. – М.: Наука, 1980. – 465 с.

[19] *Гурвиц А.* Теория функций / А. Гурвиц, Р. Курант. – М.: Наука, 1968. – 648 с.

[20] *Привалов И.И.* Интегральные уравнения / И.И. Привалов. – М.; Л.: ОНТИ, 1937. – 248 с.

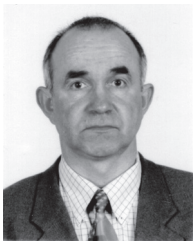
[21] *Гурса Э.* Курс математического анализа / Э. Гурса. – М.; Л.: Гостехиздат, 1934. – Т. 3. – Ч. 2. – 320 с.

Поступила в редколлегию 22.06.2014

Громыко Игорь Алексеевич, кандидат технических наук, доцент, профессор кафедры безопасности информационных систем и технологий факультета компьютерных наук Харьковского национального университета имени В. Н. Каразина. Научные интересы: построение базовых основ информационной безопасности, разработка Всеобщей парадигмы защиты информации в Украине, разработка теоретических основ и действующих базовых функциональных элементов для принципиально новой квантовой системы дистанционного получения информации в акустическом диапазоне с поверхностей помещений; исследования материальных процессов субъектного преодоления пространственно-временного континуума с целью получения ретро и экспресс-информации; исследование возможности локального ограничения процесса распространения акустических колебаний в воздушном пространстве.

Броншпак Геннадий Кимович, кандидат экономических наук, председатель совета директоров АО «Фудзиленд». Научные интересы: задачи и методы экономико-математического моделирования; системный анализ на уровне объединения предприятий.

Перчик Евгений Львович, кандидат технических наук, старший научный сотрудник, начальник информационно-аналитического отдела АО «Научно-технологический институт транскрипции, трансляции и репликации». Научные интересы: методы математического моделирования; задачи математической физики; теория интегральных уравнений.



Доценко Сергей Ильич, кандидат технических наук, доцент, профессор кафедры электроснабжения и энергетического менеджмента Харьковского национального технического университета сельского хозяйства имени Петра Василенка. Научные интересы: теория и практика энергетического менеджмента, теория деятельности, теория функциональных систем, информационные технологии интеграции предприятия.

УДК 517.9.621

Криптографія нового покоління: інтегральні рівняння як альтернатива алгебраїчній методології / Г.К Броншпак, І.А. Громико, С.І. Доценко, Е.Л. Перчик // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 337–349.

Показано переваги використання в криптографії положень математичного аналізу, зумовлені властивістю функцій неперервного аргументу. Як такі можуть виступати як попередньо представлені рядками графіки, таблиці, відеозображення, так і букви, числа, символи, відповідно яким поставлені, наприклад, синуси різної амплітуди. Шифрування проводиться шляхом інтегрування функцій, дешифрування – шляхом розв'язання інтегральних рівнянь. Наведено приклади реалізації даних процедур в аналітичному вигляді. Різноманіття варіантів таких перетворень, включаючи їх застосування в комбінаціях, ставить перед криптоаналізом практично нездоланні проблеми. Розглянуто можливість використання для криптографічного захисту відомих розв'язань задач математичної фізики. Проаналізовано сутність високої ефективності шифрування, що базується на залежності функцій від необмеженого числа інформативних ознак.

Ключові слова: криптографія, неперервний аналіз, інтегрування, інтегральні рівняння, формули обернення.

Бібліогр.: 21 найм.

UDC 517.9.621

Cryptography of a new generation: integral equations as an alternative of algebraic methodology / G.K Bronshpak, I.A. Gromyko, S.I. Dotsenko, E.L. Perchik // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 337–349.

The advantages of using points of mathematical analysis in cryptography due to the properties of continuous argument functions are shown. Pre-series presented graphs, tables, videos and letters, numbers, symbols may act in their capacity, for example, sinuses of different amplitude are placed in correspondence with. Encryption is performed by integration of functions, decryption is realized by solving integral equations. Examples of realizing these procedures in an analytical form are provided. A variety of options of such transformations, including their use in combinations, poses almost insurmountable cryptanalytic problems. The possibility of using the known solutions of problems of mathematical physics for cryptographic protection is considered. The essence of high performance encryption based on the dependence of the functions upon an unlimited number of informative features is analyzed.

Keywords: cryptography, continuous analysis, integration, integral equations, inversion formulae.

Ref.: 21 items.