При этом время открытого состояния электромагнитов 17 и 18 соответствует длительности прямоугольных импульсов формируемых одновибратором 26 который является достаточными для полного заполнения углеводородовоздушным смесям камеры детонационного генератора 21.

В конце выходного импульса одновибратора 26 на выходе генератора коротких импульсов 25 формируется короткий прямоугольный импульс (Рис.2*б* - момент времени $t_1$) который воздействуют на вход системы инициирование 24.

В результате, которого на выходе системы инициирование 24 формируется высоковольтный импульс напряжения который воздействуют на вход устройство зажигании 23. После чего из-за разгона фронта пламени внутри детонационного генератора 21 на его выходе формируется ударная волна.

При воздействие ударной вольны на поверхности земли возбуждается многочастотные гармонические затухающие сейсмические волны. Формы колебаний и частотный состав которого зависит от многих факторов таких как характера импульса воздействия, поглощающие свойства среды а также особенности строения границ раздела на пути волны и т.п. В современной сейсморазведке где используется мощные взрывные источники, которые располагают длительность импульса воздействие несколько сотни миллисекунд частотная полоса спектра возбуждаемых сейсмических волн составляет 1 – 200 Гц.

Автоматизированная система для геофизической разведки предназначены для обнаружения и первичной классификации объектов по их акустической жесткости и может, быть использовано для проведения геофизической разведки на малой глубине (до 100,0 м).

**Литература**

1. Данько Д.А. Сравнение методов детерминистической акустической инверсии для выделения акустически контрастных объектов по сейсмическим данным // Геофизика. 2016. № 1. С. 2-11.

Е.Л. Емельянова, Л.П. Усольцев

## САМАРСКИЙ АЛГОРИТМ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ МЕТОДИКИ М.ВИНЕРА В RSA-КРИПТОГРАФИИ

(Самарский национальный исследовательский университет
имени академика С,П, Королева)

В работе предложен разработанный авторами новый алгоритм практической реализации известной методики М. Винера организации атаки на одну из наиболее надежных и широко используемых публичных криптосистем, обесценивающий эту систему шифрования сообщений.
Ключевые слова: криптосистема RSA; атака М.Винера.

## Введение

Уже в текущем столетии публичные криптографы (так называют криптографов, публикующих свои работы в открытой печати) отзывались о криптосистеме RSA весьма восторженно. Например, в книге [1] из серии "Современная математика" на стр. 11 содержится такое высказывание: "Из всех существующих на сегодняшний день криптосистем эта система является самой надежной и именно она обеспечивает безопасность информации в современных компьютерных сетях".

Итак, пусть мы имеем криптосистему RSA с известным модулем $N \geq 25$ ($N = pq$), где $p$ и $q$ – секретные простые числа с условием $q < p < 2q$), известной шифрующей экспонентой (открытым ключом) $e$ $(2 \leq e < \varphi(N))$, (e, $\varphi(N)$)=1), секретной расшифровывающей экспонентой(секретным ключом) $d$ $(2 \leq d < \varphi(N))$ и так называемой "односторонней функцией с секретом" (часто говорят: "с лазейкой"), определяемой соотношением

$$ed \equiv 1\ (mod\ \varphi(N)), \qquad (1)$$

связывающим параметры $e$, $d$ *и* $N$.

Заметим, что при каждом натуральном значении $e < \varphi(N)$, в силу условия (e, $\varphi(N)$)=1, существует лишь одно значение $d < \varphi(N)$, удовлетворяющее соотношению (1), причем для этого значения $d$ выполняется условие ($d$, $\varphi(N)$)=1.

Вследствие секретности чисел $p$ и $q$, величина $\varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1)$ также является секретной, но нетрудно показать (см., например, [2], стр. 286 или [3], стр. 355), что

$$\varphi(N) > N - 3\sqrt{N} \qquad (2)$$

(и, следовательно, $\varphi(N) > \frac{2}{5}N$).

В 1989 г. М. Винер ([4], см. также [2] стр.286 или [3], стр. 368) предложил остроумную и достаточно простую (по меркам теории чисел) методику организации "взлома" криптосистемы RSA (называемую теперь "атакой М.Винера"), позволяющую в случае, когда

$$d \leq \frac{1}{3}N^{\frac{1}{4}}, \qquad (3)$$

эффективно находить значение экспоненты $d$ (по известным значениям параметров $N$ и e), связанной с экспонентой $e$ соотношением (1), используя разложение дроби $\frac{e}{N}$ в цепную дробь, а в 1999г. Д.Бонех и Дерфи ([5], см. также [3], стр.368) заменили ограничение (3) более слабым:

$$d \leq N^{0,292}.$$

Рассмотрение М. Винером криптосистемы RSA не в полной мере учитывало теоретико-числовые нюансы, связанные с соотношением (1), что не позволило ему "выжать" из своих идей максимум возможного. В предлагаемой же нами работе эти недостатки методики М. Винера устраняются и в результате предлагается новый алгоритм (ради удобства с терминологией назовем его самарским алгоритмом) практической реализации указанной методики, позволяющий "расколоть" криптосистему RSA во всех возможных случаях.

**Замена исходных параметров и односторонней функции криптосистемы**

Взяв произвольное натуральное число $m$, вычислим $N^m$ и $e^m$ (коль скоро числа $N$ и $e$ известны – они не являются секретными) и будем разлагать в цепную дробь $\frac{e^m}{N^m}$ с любым натуральным $m$, а не только с $m = 1$, как это сделал М. Винер. При $m = 1$ наши рассуждения просто совпадают с рассуждениями М. Винера, и мы этот случай опускаем, а при $m \geq 2$ будем, в частности, использовать неравенство Бернулли (см., например, [6], стр. 339, п. 3.1.1.4): Если $0 < \alpha < 1$, то справедливо неравенство

$$(1-\alpha)^m > 1 - m\alpha. \quad (4)$$

Так как обе части сравнения можно возвести в одну и ту же степень (см., например, [7], стр. 41, §2, п. c), то в силу соотношения (1), справедливо соотношение

$$e^m d^m \equiv 1\ (mod\ \varphi(N)), \quad (5)$$

а значит, и сравнения

$$e_m\ d_m \equiv 1\ (mod\ \varphi(N)) \quad (6)$$

и

$$e^m d_m \equiv 1\ (mod\ \varphi(N)) \quad (7)$$

с $e_m = e^m mod\ \varphi(N) < \varphi(N)$ и $d_m = d^m mod\ \varphi(N) < \varphi(N)$. Однако, использовать сравнения (5)-(7) в конкретных вычислениях мы не можем, поскольку в этих сравнениях степени $e^m$ и $d^m$ можно использовать лишь в привязке к неизвестному модулю $\varphi(N)$ для этих сравнений. То, что мы не знаем конкретно $d_m$, - неважно, оно появится как знаменатель дроби из подходящих дробей разложения рациональной дроби $\frac{e^m}{N^m}$ в цепную дробь. А вот существующее чисто теоретически число $e_m$ нас не устраивает, поскольку нам нужно конкретное число в качестве числителя дроби $\frac{e^m}{N^m}$ при разложении ее в цепную дробь. Поэтому помня, что $e_m = e^m mod\ \varphi(N) < \varphi(N)$, мы в вычислениях будем оперировать с конкретным числом $e^m < (\varphi(N))^m$. Таким образом, сравнение (1), порождающее одностороннюю функцию с секретом, мы заменим сравнением

$$e^m \delta_m \equiv 1\ (mod\ (\varphi(N))^m), \quad (8)$$

порождающим свою одностороннюю функцию с секретом. Заметим, что сравнение (8) относительно неизвестного $\delta_m$ разрешимо и имеет ровно одно решение (см., например, [7], стр. 55, §2, п.d). Покажем, что этим решением является $\delta_m = d_m$. Действительно, известно (см., например, [7], стр. 48, §3, п.d), что из сравнения (8) вытекает сравнение

$$e^m \delta_m \equiv 1\ (mod\ \varphi(N)).$$

Сравнивая последнее сравнение со сравнением (7), видим, что $\delta_m = d_m$, а значит, сравнение (8) можно переписать в виде

$$e^m d_m \equiv 1\ (mod\ (\varphi(N))^m). \quad (9)$$

Наконец, из соотношения (9) вытекает справедливость равенства

$$e^m d_m = 1 + k(\varphi(N))^m, \quad (10)$$

где $k$ – некоторое натуральное число.

Как уже сказано, мы считаем, что у нас $m \geq 2$.

Теорема. Пусть при некотором целом $m \geq 2$

$$d \leq \frac{2}{5\sqrt{m}} N^{\frac{4m-3}{4m}}. \quad (11)$$

Тогда при этом $m$ величина $d_m = d^m mod\ \varphi(N)$ эффективно вычислима.

Доказательство. Последовательно используя формулы (10), (2) и (4), получаем:

$$\left|\frac{e^m}{N^m} - \frac{k}{d_m}\right| = \frac{|e^m d_m - kN^m|}{N^m d_m} = \frac{|1+k(\varphi(N))^m - kN^m|}{N^m d_m} < \frac{k(N^m - (\varphi(N))^m)}{N^m d_m} = \frac{kN^m\left(1-\left(\frac{\varphi(N)}{N}\right)^m\right)}{N^m d_m} = \frac{k\left(1-\left(\frac{\varphi(N)}{N}\right)^m\right)}{d_m} < \frac{e^m d_m}{(\varphi(N))^m} \frac{\left(1-\left(\frac{N-3\sqrt{N}}{N}\right)^m\right)}{d_m} = \frac{e^m\left(1-\left(1-\frac{3}{\sqrt{N}}\right)^m\right)}{(\varphi(N))^m} < 1 - \left(1 - \frac{3m}{\sqrt{N}}\right) = \frac{3m}{\sqrt{N}}. \quad (12)$$

Далее, в силу неравенства (11) и неравенства $\varphi(N) > \frac{2}{5}N$, имеем:

$$d \leq \frac{2}{5\sqrt{m}} N^{\frac{4m-3}{4m}} = \left(\frac{2}{5\sqrt{m}} N\right)^{\frac{m-1}{m}} \left(\frac{2}{5\sqrt{m}} N^{\frac{1}{4}}\right)^{\frac{1}{m}} < \frac{1}{\sqrt{m}} (1+\varphi(N))^{\frac{m-1}{m}} \left(\frac{2}{5\sqrt{m}} N^{\frac{1}{4}}\right)^{\frac{1}{m}} < (1+\varphi(N))^{\frac{m-1}{m}} \left(\frac{2}{5\sqrt{m}} N^{\frac{1}{4}}\right)^{\frac{1}{m}},$$

$$d_m = d_m mod\ \varphi(N) < (1+\varphi(N))^{m-1} \left[\frac{1}{5\sqrt{m}} N^{\frac{1}{4}}\right] mod\ \varphi(N) = \left[\frac{2}{5\sqrt{m}} N^{\frac{1}{4}}\right] < \frac{2}{5\sqrt{m}} N^{\frac{1}{4}},$$

$$\sqrt{N} > \frac{25m{d_m}^2}{4}$$

$$\frac{3m}{\sqrt{N}} < \frac{12}{25(d_m)^2} < \frac{1}{2(d_m)^2} \quad (13)$$

Из (12) и (13) следует, что

$$\left|\frac{e^m}{N^m} - \frac{k}{d_m}\right| < \frac{1}{2(d_m)^2} \quad (14)$$

Неравенство (14) означает, что величина $\frac{k}{d_m}$ является подходящей дробью для разложения дроби $\frac{e^m}{N^2}$ в цепную дробь. Однако, известно (см., например, , [2], стр. 45, п. 2.19.3), что всего подходящих дробей не более $2\log_2 N^m = 2m\log_2 N$ и все они эффективно вычислимы. Подставляя поочередно знаменатели подходящих дробей в выражение

$$\left(M^{e^m}\right)^{d_m} = M^{(e^m d_m) mod \varphi(N)}$$

с некоторым случайным числом $M$, мы в случае равенства находим расшифровывающую экспоненту $d_m$, которая является новым ключом в системе RSA. Теорема доказана.

Хотелось бы высказать мнение теоретико-числовика, что "лазейка" любой односторонней функции с секретом в принципе должна позволять раскрыть содержащийся в этой функции ее секрет.

В заключении мы благодарим выпускников Самарского госуниверситета С.В. Минюшова и А.В. Яшнева, просчитавших в своих студенческих работах ряд конкретных примеров, иллюстрирующих некоторые из изложенных здесь результатов.

**Литература**

1. Соловьев Ю.П., Садовничий В.А., Шавгулидзе Е.Т., Белокуров В.В. Эллиптические кривые и современные алгоритмы теории чисел.- М.-Иж.: Институт комп. исследований, 2003.
2. Математические и компьютерные основы криптологии: Учебн. пособие/ Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн: Новое знание, 2003.
3. Смарт Н. Криптография. – М.: Техносфера, 2005.
4. Wiener M/ Cryptanalysis of chort RSA secret exponents. – IEEE Trans. Int. Theory, 1989. V. 35. P.54 – 58.
5. Boneh D. Twenty years of attacks of the RSA cryptosystem. – Notes of the Americ. Math. Soc.,1999. V. 46.P.203-213.
6. Бронштейн И.Н., Семендяев К.А. Справочник по математике для инженеров и студентов втузов.- Изд. перераб. Пер. с нем. – М.:Наука, 1980.
7. Виноградов И.М. Основы теории чисел. – М.: Наука, 1965.

И.В. Федоров

## МОДЕЛИРОВАНИЕ ИНДИКАТРИСЫ РАССЕЯНИЯ АНСАМБЛЯ ЧАСТИЦ

(Самарский университет)

При испытаниях качества распыливания топлива в газотурбинном двигателе летательного аппарата наблюдению доступна индикатриса рассеяния лазерного излучения, прошедшего через струю распыла. Задачей является оценивание распределения капель по размеру на основе зарегистрированной индикатрисы рассеяния. В работе решаются как прямая задача моделирования индикатрисы рассеяния по заданному распределению ансамбля частиц на основе теории дифракции Фраунгофера, так и обратная задача восстановления гистограммы распределения ансамбля частиц по размерам.

При распыливании форсунками жидкого вещества в струе одновременно могут находиться разнородные по размерам капли, и общее их число чрезвычайно велико. Для измерения размеров капель используется метод малоуглового дифракционного рассеяния света [3].

Главным недостатком метода малоуглового рассеяния [2] является ограничение по пространственной плотности расположения капель в связи с трудностью учета в методах математической обработки влияния эффектов вторичного рассеяния.

Качество работы форсунок оценивается по форме и дальнобойности струй, по обеспечению требуемого закона распределения в пространстве, по величине неравномерности этого распределения, а также по величине диаметров образующихся капель и по количеству капель того или иного диаметра.