УДК 512. 5/8

# ОБ ОДНОМ RSA-ПОДОБНОМ КРИПТОАЛГОРИТМЕ

*В.А.Фильштинский, доц.; Л.А.Фильштинский, проф.; С.В.Фильштинский*

## 1 ВВЕДЕНИЕ

Замечательным достижением науки о защите информации явилось изобретение криптографии с открытым ключом, серьезно изменившим представления о возможностях криптографических применений, в особенности распространения социальных и экономических механизмов на современный мир, обладающий всеохватывающими сетями телекоммуникаций [1-3]. Несколько ранее W.Diffie и M.E.Hellman [4] предложили систему открытого обмена сеансовыми ключами, внеся основополагающий вклад в криптографию с открытым ключом. Сущность метода состоит в следующем: двое пользователей $A$ и $B$ ( Алиса и Боб - их общепринятые "обозначения" в научных работах ) выбирают достаточно большое простое число $P>1$ и такое $1<\alpha<p-1$, что отображение

$$\begin{cases}(0,1,...,P-2)\to(1,2,...,P-1)\\ x\quad\to\alpha^x\pmod P\end{cases}$$

есть биекция (подобное $\alpha$ для простого $P$ всегда существует [5]), выбирают (каждый свой) секретные ключи $X_A$, $X_B$, $(1<X_A,X_B<P)$. Наконец, они публикуют значение модуля $P$ и свои открытые ключи $Y_A\equiv\alpha^{X_A}$, $Y_B\equiv\alpha^{X_B}\pmod P$.

Чтобы найти общий сеансовый ключ $K$, т.е. значение, с помощью которого можно принятым ими способом шифровать свои сообщения для передачи друг другу, Алиса и Боб вычисляют $K_A\equiv Y_B^{X_A}$, $K_B\equiv Y_A^{X_B}\pmod P$. Но $\left(\alpha^{X_B}\right)^{X_A}=\left(\alpha^{X_A}\right)^{X_B}$, т.е. $K_A\equiv K_B\pmod P$. Попытка раскрыть секретные ключи $X_A,X_B$ "упирается" в задачу о дискретном логарифме: по заданному $y\equiv x^\alpha\pmod P$ найти $x:0\le x\le P-r$. В этой задаче не найден алгоритм вычисления $x$ за удовлетворительное время.

Если мы желаем открыто передавать криптограммы, которые достаточно легко может расшифровать законный получатель, а за достаточно обозримое время не может расшифровать незаконный получатель, то следует так выбрать функцию зашифрования $y=f(x)$, $x\in X$, где $y$ - множество открытых сообщений, чтобы

(i1) можно было легко найти $y$ по известному $x$;

(i2) практически невозможно найти $x\in X$ по известному $y\in X$ (предположено, что $X$ есть также множество криптограмм).

Функцию расшифрования $x=g(y), y\in X$ следует выбрать так, чтобы

(j1) можно было легко найти $x$ по известному $y \in X$;

(j2) функция $g$ практически не могла быть вычислительно найдена из функции $f$;

(j3) функция $g$ легко вычисляема законным получателем и только им;

(j4) выполнялось условие частичной обратимости функции $f$

$g(f(x)) = x \ \forall x \in X$.

Именно такую пару функций указали R.Rivest, A.Shamir, L.Adleman [3]

$$f(x) \equiv x^{\alpha} \pmod{m}, \quad g(y) \equiv y^{\beta} \pmod{m},$$

где модуль $m = p \cdot q, p \neq q$ - простые нечетные числа. Условие (i2) требует, чтобы значения $p,q$ были очень большие. Это объясняется тем, что задача разложения числа $m(= p \cdot q)$ на простые множители $p$ и $q$ не имеет удовлетворительного алгоритмического решения. Значение $f(x)$ достаточно просто вычисляется с помощью двоичного представления показателя $\alpha$.

Вместе с тем отыскание значения $x$ по известному $y \equiv x^{\alpha} \pmod{m}$ столь же трудно, как и вычисление дискретного логарифма. Условия (i1), (i2) удовлетворены. Условие (j4) и вид функций $f,g$ приводят к налагаемому на $\beta$ условию

$$x^{\alpha\beta} \equiv x \pmod{m}.$$

Вместе с тем по известной теореме Эйлера

$$x^{\gamma} \equiv x \pmod{m}.$$

Здесь $\gamma \equiv 1(\bmod \varphi(m))$, $(x,m) = 1$, где $\varphi(m) = (p-1)(q-1)$ – функция Эйлера, равная количеству чисел из ряда $1,2,...,m-1$, взаимно простых с $m$, а $(x,m)$ - общий наибольший делитель чисел $x$ и $m$. Алиса находит $\beta$ так, чтобы

$$\alpha\beta \equiv 1 \pmod{(p-1)(q-1)}, \qquad (1.1)$$

и выбирает это значение в качестве своего секретного ключа. Значение $\alpha$ найти несложно. Оно служит открытым ключом Алисы и публикуется вместе со значением $m$ в открытом справочнике. Условие (j2) выполняется уже потому, что неизвестен модуль $(p-1)(q-1)$ в сравнении (1.1). Заметим, что в (1.1) модуль можно уменьшить до значения $\langle p-1, q-1 \rangle$, равного наименьшему общему кратному чисел $p-1, q-1$. Кроме того, условие $(x,m) = 1$ излишне (в рассматриваемой ситуации). Итак, желая получить зашифрованное сообщение в свой адрес, Алиса публикует открытый ключ $\alpha$, знает секретный ключ $\beta$ и параметры $p,q$. Отправитель открытого сообщения $x, 1 < x < p$ в виде криптограммы $y = f(x) \equiv x^{\alpha} \pmod{m}$ не знает, как и все остальные, ни $p$, ни $q$, ни $\beta$. Значение секретного ключа $\beta$ находится среди чисел, взаимно простых с $N = \langle p-1, q-1 \rangle$ и меньших $N$. Одна из возможностей "усилить" криптоалгоритм, т.е. сделать его более сложным для несанкционированного дешифрования, состоит в увеличении чисел $p,q$. Другая возможность состоит в том, чтобы, не увеличивая $p$ и $q$, сделать

интервал для выбора $\beta$ более широким и затруднить тем самым поиск секретного ключа.

Некоторой реализации этой цели посвящена предлагаемая работа. Для этого мы предлагаем использовать некоторые свойства многочленов П.Л.Чебышева (см., например, [6]), введенные им при решении одной экстремальной задачи теории аппроксимации. Более известна система многочленов Чебышева в связи с теорией ортогональных многочленов.

## ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

Элементарные факты относительно многочленов Чебышева $T_n(x)$ можно найти в [6]. Многочлены $T_n$ и многочлены Чебышева второго рода $U_n$ определяются (в частности) соотношениями:

$$T_0(x)=1,\ \ T_1(x)=x,\ \ T_n(x)=2xT_{n-1}(x)-T_{n-2}(x),\ n=2,3,\ldots, \qquad (2.1)$$

$$U_0(x)=1,\ \ U_1(x)=2x,\ \ U_n(x)=2xU_{n-1}(x)-U_{n-2}(x),\ n=2,3,\ldots \qquad (2.2)$$

Многочлены $T_n$, $U_n$ имеют целые коэффициенты при степенях переменной; являются четными функциями при четных $n$ и нечетными при нечетных $n$. Кроме того, если

$$T_n(x)=\sum_{k=0}^{n} t_{nk}x^k,\ U_n(x)=\sum_{k=0}^{n} u_{nk}x^k,$$

то

$$t_{2n,0}=(-1)^n,\ u_{2n,0}=(-1)^n,\ t_{2n+1,1}=(-1)^n\cdot(2n+1),\ u_{2n+1,1}=(-1)^n\ \ (2n+2), \qquad (2.3)$$

$$t_{n,n}=2^{n-1},\ \ u_{n,n}=2^n.$$

Кроме того,
$$T_n(x)=\sum_{k=0}^{\left[\frac{n}{2}\right]}\binom{n}{2k}x^{n-2k}\left(x^2-1\right)^k,\ n=0,1,\ldots, \qquad (2.4)$$

$$T_n(x)=\frac{n}{2}\sum_{k=0}^{\left[\frac{n}{2}\right]}\frac{(-1)^k}{n-k}\binom{n-k}{k}(2x)^{n-2k},\ n=1,2,\ldots, \qquad (2.5)$$

$$U_n(x)=\sum_{k=0}^{\left[\frac{n}{2}\right]}(-1)^k\binom{n-k}{k}(2x)^{n-2k},\ n=0,1,\ldots, \qquad (2.6)$$

где $[s]$ - целая часть числа $s\ge 0$, а $\binom{n}{m}=\frac{n!}{m!(n-m)!}$,

$$T_n(x)=\frac{1}{2}\left[\left(x+\sqrt{x^2-1}\right)^n+\left(x-\sqrt{x^2-1}\right)^n\right],\ n=0,1,\ldots,\ |x|>1, \qquad (2.7)$$

$$U_n(x)=\frac{1}{2}\left[\left(x+\sqrt{x^2-1}\right)^{n+1}-\left(x-\sqrt{x^2-1}\right)^{n+1}\right]/\sqrt{x^2-1},\ n=0,1,\ldots,\ |x|>1. \qquad (2.8)$$

Ниже приведены формулы, связывающие многочлены Чебышева разных степеней:

$$T_n(x)T_m(x)=\frac{1}{2}\left[T_{n-m}(x)+T_{n+m}(x)\right],\ n,m=0,\pm1,\ldots, \tag{2.9}$$

$$U_m(x)T_n(x)=\frac{1}{2}\left[U_{m-n}(x)+U_{m+n}(x)\right],\ n,m=0,\pm1,\ldots, \tag{2.10}$$

$$U_n(x)=\frac{xT_{n+1}(x)-T_n(x)}{x^2-1},\ x\neq\pm1,\ n=0,\pm1,\ldots, \tag{2.11}$$

$$T_n(T_m(x))=T_{nm}(x),\ n,m=0,\pm1,\ldots \tag{2.12}$$

Докажем весьма важное свойство (2.12). Для $n=1$ и любого $m$ утверждение очевидно. Для $n=2$ и любого $m$

$$T_2(T_m(x))=2T_m^2(x)-1=\left[T_0(x)+T_{2m}(x)\right]-1=T_{2m}(x)$$

по формуле (2.9). Пусть утверждение доказано для $n\le n_0$ и любого $m$. Тогда из (2.1), (2.9) и предположения индукции

$$T_{n_0+1}(T_m(x))=2T_{n_0}(x)T_{n_0}(T_m(x))-T_{n_0-1}(T_m(x))=$$
$$=2T_m(x)\cdot T_{n_0m}(x)-T_{m(n_0-1)}(x)=T_{(n_0+1)m}(x),$$

что и требовалось.

Заметим, что (2.12) прямо следует из определения $T_n(x)=\cos(n\arccos x)$ при $|x|\le1$ и аналогичного при $|x|>1$. Многочлены $T_n,U_n$ определены при $n\ge0$. Меняя местами $T_n$ и $T_{n-2}$, $U_n$ и $U_{n-2}$, легко распространить определения $T_n,U_n$ на отрицательные номера:

$$T_{-n}(x):=T_n(x),\ U_n(x):=-U_{(n-2)}(x) \tag{2.13}$$

с сохранением всех ранее упомянутых свойств.

## ОСНОВНЫЕ СООТНОШЕНИЯ

В этом разделе будут доказаны утверждения относительно функций

$$T_n(x)\pmod p,\ U_n(x)\pmod p,$$

где $p=2q+1$ – простое число; $q\ge1$, а $x\in\mathbf{Z}$.

Лемма 1

$$T_p(x)\equiv T_1(x)\pmod p. \tag{3.1}$$

Действительно,

$$\binom{p}{2k}\equiv0\pmod p,\ k>0.$$

Поэтому (формула (2.4) и малая теорема Ферма [5])

$$T_p(x)\equiv\binom{p}{0}x^p\equiv x=T_1(x)\pmod p.$$

Следствие 1

$$T_{\nu p}(x)\equiv T_\nu(x)\pmod p,\ \nu=1,2,\ldots \tag{3.2}$$

В самом деле, из (2.12) следует, что $T_{\nu p}(x)=T_\nu(T_p(x))\equiv T_\nu(x)$.

Лемма 2

$$T_n(x) \equiv U_\nu(x)T_{n-\nu p}(x) - U_{\nu-1}(x)T_{n-(\nu+1)p}(x) \pmod p. \qquad (3.3)$$

Доказательство

Пусть $\nu = 1$, тогда (используем (2.9) и лемму 1)

$$T_n(x) + T_{n-2p}(x) = 2T_{n-p}(x)T_p(x) \equiv U_1(x)T_{n-p}(x) \pmod p,$$

т.е. (3.3) доказано для $\nu = 1$. Далее

$$T_n(x) \equiv U_1(x)\left[2xT_{n-2p}(x) - T_{n-3p}(x)\right] - T_{n-2p}(x) = \left[2xU_1(x) - U_0(x)\right]T_{n-2p}(x) -$$

$$- U_1(x)T_{n-3p}(x) = U_2(x)T_{n-2p}(x) - U_1(x)T_{n-3p}(x) = \ldots$$

Лемма 3

Положим $N_p := \dfrac{p^2-1}{2}$, тогда $T_{N_p}(x) \equiv 1 \pmod p$.

Доказательство

Так как $N_p = pq + q$, то из леммы 2 при $n = N_p$, $\nu = q$ и (2.3) следует, что

$$T_{N_p}(x) \equiv U_q(x)T_q(x) - U_{q-1}(x)T_{q+1}(x) \pmod p. \qquad (3.4)$$

Пусть $x \equiv 0, \pm 1 \pmod p$. Подставим (2.11) в (3.4) и получим

$$T_{N_p}(x) \equiv \left(x^2-1\right)^{-1}\left[T_q(x)\left(xT_{q+1}(x) - T_q(x)\right) - T_{q+1}(x)\left(xT_q(x) - T_{q-1}(x)\right)\right] =$$

$$= \left(x^2-1\right)^{-1}\left[T_{q+1}(x)T_{q-1}(x) - T_q^2(x)\right] = 1.$$

Последнее равенство есть прямое следствие (2.7). Значение $\left(x^2-1\right)^{-1}$ есть обратный элемент к $x^2-1$ в поле вычетов по модулю $P$. Если $x \equiv 0 \pmod p$, то из (2.4) получаем

$$T_{N_p}(0) \equiv (-1)^{q(q+1)} = 1.$$

Наконец, при $x \equiv \pm 1$ многочлен $T_n(x)$ с четным $n$ всегда равен 1 (см. (2.7)).

Следствие 2

$$T_{\nu N_p}(x) \equiv 1 \pmod p, \pm\nu = 0,1,2,\ldots$$

Действительно, $T_{\nu N_p}(x) = T_\nu\left(T_{N_p}(x)\right) \equiv T_\nu(1) = 1$.

Лемма 4

$$T_{N_p - j}(x) \equiv T_j(x) \pmod p, \pm j = 0,1,\ldots.$$

Доказательство состоит в прямой проверке утверждения при $j = \pm 1$ и дальнейшем применении индукции по $j$.

Следствие 3

$$1\ T_{N_p - \frac{N_p+1}{2} + j}(x) \equiv T_{N_p - \frac{N_p-1}{2} - j}(x) \pmod p.$$

$$2\ T_{\nu N_p + 1}(x) \equiv T_1(x) \pmod p.$$

Теорема 1

Сравнение $T_n(x) \equiv x \pmod p$, $p$ – простое число, справедливо тогда и только тогда, когда выполнено одно из сравнений:

$$nn_1 = \nu N_p + 1,$$

откуда уже следует

$$T_n\left(T_{n_1}(x)\right) \equiv x \pmod p. \qquad (5.1)$$

Действительно, (следствие 2 и лемма 4)

$$T_{nn_1}(x) = T_{\nu N_p + 1}(x) \equiv x \pmod p.$$

Из (5.1) следует, что отображение

$$T_n : x \to T_n(x) \pmod p$$

является биекцией.

2 Пусть отображение, заданное функцией $T_n(x) \pmod p$, есть биекция и порождает некоторую перестановку $\sigma$. В таком случае найдется целая степень $k$ такая, что $\sigma^k$ - тождественная перестановка, т.е.

$$T_n\left(T_n\left(\ldots\left(T_n(x)\right)\ldots\right)\right) = T_{n^k}(x) \equiv x \pmod p.$$

По теореме 1 $n^k \equiv \pm 1 \pmod{N_p}$, либо $n^k \equiv \pm p \pmod{N_p}$. Но взаимная простота $n^k$ и $N_p$ влечет взаимную простоту $n$ и $N_p$, т.е.

$$n^k \equiv \pm 1 \pmod{N_p} \Rightarrow (n, N_p) = 1.$$

Если же $n^k \equiv \pm p \pmod{N_p}$, то $pn^k \equiv \pm 1 \pmod{N_p}$ и, следовательно, $(n^k, N_p) = 1$, т.е. и $(n, N_p) = 1$. Теорема доказана.

## ЗАКЛЮЧЕНИЕ

Системы с открытыми ключами позволили решить сразу несколько задач: задачу открытого распространения ключей, задачу открытого распространения сообщений, задачу получения достоверной подписи. Точные постановки и решения можно найти, например, в [7,8]. Привлекая многочлены Чебышева, можно формулировать и обосновывать новые схемы электронных подписей, решать некоторые примыкающие сюда задачи.

## ПРИЛОЖЕНИЕ

Доказательство теоремы 1

Положим $p = 2q + 1 > 3, p$ - простое число, $N_p = \frac{1}{2}(p^2 - 1)$,

$$\gamma_1 = 1, \gamma_2 = p, \gamma_3 = \frac{p^2 - 2p - 1}{2}, \gamma_4 = \frac{p^2 - 3}{2}.$$

Достаточность установить легко. Действительно,

$$T_1(x) = x, T_p(x) = x \quad \text{(лемма 1)},$$

$$T_{\frac{p^2-2p-1}{2}}(x) = T_{N_p - p}(x) \equiv T_p(x) \equiv x \quad \text{(лемма 4)},$$

$$T_{\frac{p^2-3}{2}}(x) = T_{N_p - 1}(x) \equiv T_1(x) = x \quad \text{(лемма 4)}.$$

Пусть теперь

$$T_n(x) \equiv x \pmod p$$

и $$n = sp + r,\ s \geq 0,\ 0 \leq r < p-1.$$

1) Нам понадобится отношение

$$T_{sp+r}(x) \equiv Q(x) := U_s(x)T_r(x) - U_{s-1}(x)T_{p-r}(x) \pmod p,$$

которое следует из (2.13) и леммы 2.

2) Достаточно доказать, что из $n \leq N_p/2, T_n(x) \equiv x \pmod p$ следует $n = 1$ или $n = p$. Действительно,

$$T_{N_p - n}(x) \equiv T_n(x) \quad \text{(лемма 6)}.$$

3) Пусть $n = sp + r, 0 \leq r < p$. Благодаря неравенству $n \leq \frac{1}{2}N_p$, можно считать, что $s < \frac{1}{2}q$. В самом деле,

$$\max_{0 \leq r < p}(sp + r) \leq q^2 + q,$$

и потому

$$s \leq \frac{q^2 - q}{2q+1} < \frac{q}{2}.$$

4) Можно считать, что числа $r$ и $s$ имеют разную четность: $(-1)^{r+s} = -1$. Если $r$ и $s$ оба четные или нечетные, то $Q(x)$ является четной функцией и сравнение $T_n(x) \equiv x \pmod p$ невозможно (см. а) ).

Найдем степени многочленов в (П1):

$\deg U_s T_r = s + r$, $\deg U_{s-1}T_{p-r} = p + s - r - 1$.

Вообще говоря, возможны четыре случая:

$$\text{(i)} \quad \begin{cases} r + s < p, \\ p + s - r - 1 < p, \end{cases} \qquad \text{(ii)} \quad \begin{cases} r + s \geq p, \\ p + s - r - 1 < p, \end{cases}$$

$$\text{(iii)} \quad \begin{cases} r + s < p, \\ p + s - r - 1 \geq p, \end{cases} \qquad \text{(iv)} \quad \begin{cases} r + s \geq p, \\ p + s - r - 1 \geq p. \end{cases}$$

Сразу можно отбросить (iv), так как тогда $p - s \leq r \leq s - 1$, и поэтому $p \leq 2s - 1 < q$ (см. (c)), что невозможно. В случае (i) $s - 1 < r < p - s$, т.е. $r = s, s+1, \ldots, p - s - 1$. В случае (ii) $r \geq p - s, r > s - 1$, т.е. $r = p - s, p - s + 1, \ldots, p - 1$. В случае (iii) $r < p - s, r \leq s - 1$, т.е. $r = 0, 1, \ldots, s - 1$.

Поочередно изучим ситуации (П2 - П4). Если верно (П2), то $\deg Q < p$. Если $s + r = p + s - r - 1$, т.е. $r = q$, то

$$Q(x) = U_s(x)T_q(x) - U_{s-1}(x)T_{q+1}(x) = T_{q-s}.$$

Последнее равенство следует из леммы 6.

Лемма 6

$$T_{m+k}(x) = U_k(x)T_m(x) - U_{k-1}(x)T_{m-1}(x), \qquad \text{(П5)}$$

$$T_{m-k}(x) = U_k(x)T_m(x) - U_{k-1}(x)T_{m+1}(x). \qquad \text{(П6)}$$

Доказательство

При $k=1$ обе формулы следуют из (2.1) и (2.2). Зафиксируем в (П5) номер $m$. Если (П5) верно для некоторого $k \geq 1$, то

$$T_{m+k+1}(x) = 2xT_{m+k}(x) - T_{m+k-1}(x) = 2x[U_k(x)T_m(x) - U_{k-1}T_{m-1}(x)] -$$
$$-[U_{k-1}(x)T_m(x) - U_{k-2}(x)T_{m-1}(x)] = T_m(x)[2xU_k(x) - U_{k-1}(x)] -$$
$$-T_{m-1}(x)[2xU_{k-1}(x) - U_{k-2}(x)] = U_{k+1}(x)T_m(x) - U_k(x)T_{m-1}(x).$$

Соотношение (П6) получается из (П5) заменой $m$ на $-m$ с учетом (2.13). Лемма доказана. Нам еще понадобится следующее простое утверждение [5].

Лемма 7

Если сравнение по простому модулю $P$

$$R(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv (\mathrm{mod}\, p),\ n < p$$

имеет более, чем $n$ решений $x_1, x_2, \ldots, x_m$, то

$$a_k \equiv 0\ (\mathrm{mod}\, p),\ k = 0,1\ldots,n.$$

Справедливость леммы немедленно вытекает из представления

$$R(x) = b_0 + b_1(x - x_1) + b_2(x - x_1)(x - x_2) + \ldots + b_n(x - x_1)\cdot\ldots\cdot(x - x_n).$$

Продолжим доказательство теоремы. Из леммы 7 следует, что все коэффициенты многочлена $Q(x) - x$ кратны $P$, т.к. сравнение $Q(x) - x \equiv 0\ (\mathrm{mod}\, p)$ верно при $x = 0,1,\ldots, p-1$. Но

$$Q(x) - x = T_{q-s}(x) - x = (2^{q-s-1}x^{q-s} + \ldots) - x,$$

и $q - s > 1$, т.е. многочлен $Q(x) - x$ содержит некратный модулю $P$ коэффициент $2^{q-s-1}$, что невозможно. Напомним, что был рассмотрен случай $s + r = p + s - r - 1$. Если же $s + r \neq p + s - r - 1$, то либо

$$Q(x) = 2^{s+r-1}x^{s+r} + \ldots, \text{ либо } Q(x) = 2^{p+s-r-2}x^{p+s-r-1} + \ldots$$

В любом случае старшая степень многочлена $Q(x)$ больше, чем 1, а коэффициент при ней не кратен $P$, что невозможно ввиду леммы 7.

Итак, в ситуации (i1) сравнение $T_n(x) \equiv x\ (\mathrm{mod}\, p)\ \forall x$ невозможно, если $n > 1$.

Рассмотрим случай (i2). Преобразуем произведение $U_s T_r$ в сумму. Это необходимо для вычисления коэффициента при $x^n$ многочлена $U_s T_r$ (а следовательно, и $Q$). Итак (см. (2.9)),

$$U_s T_r = \frac{1}{2}(U_{s-r} + U_{s+r}),$$

и $s - r < 0$. По формуле (2.13) $U_{s-r} = -U_{r-s-2}$, и потому

$$U_s T_r = \frac{1}{2}(U_{s+r} - U_{r-s-2}),$$

где $r - s - 2 \geq 0$. Действительно, неравенство $r - s - 2 < 0$ вместе с неравенством $s - r < 0$ приводит к равенству $r = s + 1$, выводя тем самым число $r$ из условия (i2). Итак,

$$Q=\frac{1}{2}U_{s+r}-\frac{1}{2}U_{r-s-2}-U_{s-1}T_{p-r}.$$

Слагаемое $ax^p$ содержит только многочлен $\frac{1}{2}U_{s+r}$. Положим $r+s=2t+1$, $r-s=2\tau+1$.

По формуле (2.6) $a=\frac{1}{2}(-1)^k\binom{s+r-k}{k}\cdot 2^{r+s-2k}$, где $r+s-2k=p$, т.е. $k=t-q$.

Следовательно,

$$a=(-1)^{t-q}2^{p-1}\frac{(t+q+1)(t+q)\cdot\ldots\cdot(t+q+1-t+q+1)}{(t-q)!}=$$

$$=(-1)^{t-q}2^{p-1}\frac{(p+1)(p+2)\cdot\ldots\cdot(p+t-q)}{(t-q)!}\equiv(-1)^{t-q}.$$

После приведения по mod $P$ $x^p\equiv x$, $x^{p+1}\equiv x^2$, ... многочлен $Q(x)$ переходит в многочлен $Q_1(x)\equiv Q(x)\pmod p$, $\deg Q_1<p$. Найдем коэффициент при $x^1$ многочлена $Q_1(x)$:

$$b\equiv(-1)^{t-q}+\frac{1}{2}(-1)^{(s+r-1)/2}(s+r+1)-\frac{1}{2}(-1)^{(r-s-1)/2}(r-s-1)-$$

$$-\begin{cases}(-1)^{(p-r)/2+(s-r)/2}\cdot s, & s-\text{четное}\\ (-1)^{(s-1)/2+(p-r-1)/2}\cdot(p-r), & s-\text{нечетное}\end{cases}=$$

$$=(-1)^{t+q}+\frac{1}{2}(-1)^t(r+s+1)+\frac{1}{2}(-1)^\tau(r-s-1)+\begin{cases}(-1)^{\tau}\cdot s, & s-\text{четное},\\ (-1)^{\tau}\cdot(p-r), & s-\text{нечетное}.\end{cases}$$

Пусть $s$ четное. Тогда $r$ нечетное, а так как $r=t+\tau+1$, $s=t-\tau$, то $t$ и $\tau$ либо оба четные, либо оба нечетные. В таком случае

$$b\equiv(-1)^t\left[(-1)^\tau(s+1)+r\right].$$

Если $t$ и $q$ - четные, то $b\equiv s+r+1$. Требование $b\equiv 1$ влечет равенство $r=p-s$. Тем самым $Q=U_sT_{p-s}-U_{s-1}T_s$.

Найдем коэффициент $d$ при $x^{p-2}$ многочлена $Q$. Пусть

$$U_s(x)=a_0x^s+a_1x^{s-2}+\ldots,\quad T_{p-s}(x)=b_0x^{p-s}+b_1x^{p-s-2}+\ldots$$

Значит,

$$d=a_0b_1+a_1b_0=-\frac{2^{s-1}(p-s)}{p-s-1}\binom{p-s-1}{1}\cdot 2^{p-s-2}-2^{s-1}\binom{s-1}{1}\cdot 2^{s-2}=$$

$$=-2^{p-3}(p-1)\equiv 2^{p-3}\equiv 1\pmod p.$$

и сравнение $T_n(x)\equiv x\pmod p$ невозможно.

Пусть $t$ - четное, $q$ - нечетное. Тогда сравнение $(b\equiv)\,r-s-1\equiv 1$ равносильно равенству $r=s+2$. Это невозможно из-за разной четности $r$ и $s$. Если $t$ -

нечетное, $q$ - четное, то $b\equiv -(r+s+1)$. Сравнение $r=p-s-2$ приводит к равенству $r=p-s-2$, а по условию $r\geq p-s$.

Пусть, наконец, $q$, $t$ - нечетные. Тогда $b\equiv 1$ эквивалентно равенству $r=s$, а по условию $r>s$. Чтобы завершить изучение (i2) будем считать $s$ нечетным. В этом случае $t$ и $\tau$ имеют разные четности, а $b\equiv (-1)^{t}\left[(-1)^{q}(1+r)+s+1\right]$.

Могут представиться случаи:

1 $q$, $t$ - четные. Из $b\equiv 1$ следует, что $r+s=p-1$, т.е. $r$ и $s$ одной четности, что невозможно.

2 $t$ - четное, $q$ - нечетное. Тогда из $b\equiv 1$ следует, что $s-r\equiv 1$. Так как $0<s<r<p$, то $r-s=p-1$, и вновь $r$ и $s$ оказываются числами одной четности.

3 $t$ - нечетное, $q$ - четное. Тогда из $b\equiv 1$ следует $r+s=p-s$, что невозможно по тем же причинам.

4 $t$, $q$ - нечетные. Тогда $r=s+1$ вопреки неравенству $r>s+1$.

Итак, в ситуации (i2) сравнение $T_n(x)\equiv x \pmod p$ невозможно. Изучим (i3). Преобразуем в сумму выражение $U_{s-1}T_{p-r}$:

$$U_{s-1}T_{p-r}=\frac{1}{2}\left[U_{s-1-p+r}+U_{p+s-r-1}\right]=\frac{1}{2}\left[U_{p+s-r-1}-U_{p-s-r-1}\right].$$

Здесь $p-r-s-1\geq 0$, ибо в противном случае $p<r+s+1\leq 2s$, что невозможно.

Положим $r+s=2t+1$, $s-r=2\tau+1$. Далее

$$Q=U_sT_r+\frac{1}{2}U_{p-s-r-1}-\frac{1}{2}U_{p+s-r-1},$$

и только многочлен $U_{p+s-r-1}$ содержит $x^{\tau}$. Коэффициент при $x^{\tau}$ в нем равен

$$(-1)^{r}\binom{p+\tau}{\tau}\cdot 2^{\tau}=(-1)^{r}\cdot 2^{\tau}\frac{(p+\tau)(p+\tau-1)\cdot\ldots\cdot(p+1)}{1\cdot 2\cdot\ldots\cdot\tau}\equiv 2\cdot(-1)^{r}\pmod p.$$

Значение коэффициента при $x^1$ многочлена $Q$ после преобразований по $\bmod p$ таков

$$b\equiv(-1)^{r+1}-\frac{1}{2}\cdot(-1)^{q+\tau}\cdot(p+s-r)+\frac{1}{2}(-1)^{q-1-1}(p-s-r)+\begin{cases}(-1)^{(s+\tau-1)/2}\cdot r, & s-\text{четное},\\ (-1)^{(s+\tau-1)/2}\cdot(s+1), & s-\text{нечетное}.\end{cases}$$

Пусть $s$ четное. Тогда $t$, $\tau$ имеют разную четность, и

$$b\equiv(-1)^{t}\left[r+1+(-1)^{q}s\right]\pmod p.$$

Если $t$, $q$ - четные, то условие $r+s+1\equiv 1 \pmod p$ влечет равенство $r=p-s$, что невозможно. Если $t$ - четное , $q$ -нечетное, то условие $r+s-1\equiv 1\pmod p$ влечет равенство $r=s$, что невозможно. Если $t$ - нечетное , $q$ - четное, то

условие $-r-s-1\equiv 1 \pmod p$ влечет равенство $r=p-s-2$, что невозможно, так как даже $\max r=s-1<p-s-2$. Если $t$, $q$ - нечетные, то условие $-r-1+s\equiv 1 \pmod p$ влечет равенство $s-r=2$, что невозможно, так как $s$ и $r$ имеют разную четность.

Пусть теперь $s$ нечетное. В этом случае $t$, $\tau$ имеют одну четность, и

$$b\equiv (-1)^t\left[s+(-1)^t\cdot r\right].$$

Если $t$, $q$ - четные, то условие $s+r\equiv 1 \pmod p$ влечет $s=1, r=0$, т.е. $n=p$, и тогда, действительно, $T_p(x)\equiv x \pmod p$.

Если $t$ - четное , $q$ -нечетное, то условие $s-r\equiv 1 \pmod p$ влечет равенство $r=s-1$. В этом случае

$$Q=U_sT_{s-1}-U_{s-1}T_{p-s+1}.$$

Найдем коэффициент при $x^{p-2}$ многочлена $Q$. Слагаемое, содержащее $x^{p-2}$, имеется только у многочлена $-U_{s-1}T_{p-s+1}$.

Пусть

$$U_{s-1}(x)=a_0x^{s-1}+a_1x^{s-3}+\ldots,\ T_{p-s+1}(x)=b_0x^{p-s+1}+b_1x^{p-s-1}+\ldots$$

Коэффициент при $x^{p-2}$ равен

$$a_0b_1+b_0a_1=2^{p-3}(p-1)\equiv 2^{p-3}\equiv 0 \pmod p$$

и потому $$Q(x)\equiv x \pmod p.$$

Если $t$ - нечетное, $q$ - четное, то условие $-s-r\equiv 1 \pmod p$ влечет равенство $s+r=p-1$, что невозможно. Если $t$, $q$ - оба нечетные, то условие $-s+r\equiv 1 \pmod p$ влечет равенство $r=s+1$, что невозможно. Все ситуации (i1) - (i3) рассмотрены. Теорема доказана.


## SUMMARY

*New procedure of building cryptoalgorithm with using some extremum properties of Chebyshev polynomials is proposed. Examples are shown.*


## СПИСОК ЛИТЕРАТУРЫ


1. James L.Massey. An Introduction to Contemporary Cryptology. Proceedings of the IEEE, 1988, Vol.76. - №.5. - P.24-42.
2. Манин Ю.И., Панчишкин А.А. Введение в теорию чисел, серия Итоги науки и техники. Современные проблемы математики, ВИНИТИ, Москва,т.49, 1990, С.1 - 348.
3. R.Rivest, A.Shamir, L.Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems, CACM, vol.22,No.11, February 1978, pp.120 - 126.
4. W.Diffie, M.E.Hellman. New Directions in Cryptography, IEEE Trans. Informat.Theory, Vol.IT22,1976. - P.644-654.
5. А.К.Сушкевич. Теория чисел. - Харьков: ХГУ, 1956. - 204 с.
6. С.Пашковский. Вычислительные применения многочленов и рядов Чебышева. - М.: Наука, 1983. - 384 с.
7. T.El Gamal "A public-key cryptosystem and a signature scheme based on discrete logarithms" Advances in Cryptology: Proceedings of CRYPTO'84, volume 196 of Lecture Notes in Computer Science, Springer-Verlag, 1985.- P.10-18.
8. P.Horster, M.Michels and H.Petersen "Generalized ElGamal signatures for one message block" Technical Report TR-94-3 University of Technolodgy Chemnitz-Zwickau, May 1994.



*Поступила в редколлегию 29 декабря 1999 г.*