УДК 003.26

Богуш В. В.; **Мухачов В. А.,** к.т.н.
(Державний університет інформаційно-комунікаційних технологій)

АЛГОРИТМІЧНІ АСПЕКТИ ПОБУДОВИ ПРОСТИХ ЧИСЕЛ ЗА ПРОЦЕДУРОЮ ГОСТ Р 34.10 – 94 РФ

Богуш В. В., Мухачов В. А. Алгоритмічні аспекти побудови простих чисел за процедурою ГОСТ Р 34.10 – 94 РФ. Проведено аналіз алгоритму побудови спеціальних простих чисел великої розрядності та структури відповідних проміжних даних. З'ясовано достатні умови для вибору **параметрів**, за яких простоту згенерованих чисел може бути доведено строго.

Ключові слова: КРИПТОГРАФІЯ, ПРОСТЕ ЧИСЛО, СТАНДАРТ Р 34.10-94, ЦИФРОВИЙ ПІДПИС

Богуш В. В., Мухачёв В. А. Алгоритмические аспекты построения простых чисел в соответствии с процедурой ГОСТ Р 34.10 – 94 РФ. Проведен анализ алгоритма построения специальных простых чисел большой разрядности и структуры соответствующих промежуточных данных. Выяснены достаточные условия для выбора параметров, при которых простота сгенерированных чисел может быть доказана строго.

Ключевые слова:КРИПТОГРАФИЯ, ПРОСТОЕ ЧИСЛО, СТАНДАРТ Р34.10-94, ЦИФРОВАЯ ПОДПИСЬ

Bogush V. V., Mukhachov V. A. Algorithmic aspects of GOST 34.10 − 94 RF recommended procedure for generating prime numbers. An analysis of the algorithm for finding special large prime numbers and of appropriate intermediate data structure was fulfilled. Sufficient conditions for the choice of parameters for which the generated numbers primality was proved rigorously were clarified.

Key words:CRYPTOGRAPHY, PRIME NUMBERS, STANDARD R 34.10-94, DIGITAL SIGNATURE

Вступ. Система стандартизації у галузі криптографічного захисту інформації є, по суті, єдиною ланкою, що, з точки зору довіри користувачів, пов'язує математичні моделі з діючими реалізаціями криптосистем,

Разом з тим, вибір параметрів для процедур, що встановлені стандартами, користувачі мають здійснювати самостійно, незважаючи на те, що параметри можуть бути нерівноцінними, а обґрунтування їх вибору не є очевидним.

Стаття Бессалова А. В. та Третьякова Д. Б. [1], у який запропоновано оптимізацію представлення даних у якобіані гіпереліптичної кривої, створює прецедент щодо аналізу складових криптографічних механізмів з алгоритмічної точки зору.

Стаття, що пропонується, має на меті підтримати такий підхід, який є важливим як для свідомого вибору надійних параметрів реалізації, так і для надання висновків щодо безпечної сфери застосування окремих процедур поза межами відповідного стандарту.

Ціллю статті є знаходження параметрів алгоритму базової «процедури А» стандарту ГОСТ Р 34.10 – 94 за яких простоту чисел, побудованих для реалізації механізму цифрового підпису типу Ель Гамаля, можна строго довести.

Схема цифрового підпису основана на складності дискретного логарифму у циклічній підгрупі великого порядку q простого поля $GF(p)$.

1. Процедура А побудови параметрів *p,q.* У стандарті [2] процедури A, A', B, B' застосовуються для побудови великих простих чисел p, q у різних діапазонах значень. Процедури B та B' використовують процедури A та A', як допоміжні**.**

Вимоги схеми цифрового підпису щодо чисел p, q наступні: $p = Rq + 1-$ просте число, $2^{509} < p < 2^{512}$, або $2^{1020} < p < 2^{1024}$; $q-$ просте число, $2^{254} < q < 2^{256}$ (дільник $p-1$).

Процедуру A можна вважати базовою щодо організації пошуку простого числа p та застосування відповідного критерію простоти.

У процедурах стандарту для побудови чисел p, q використовуються повноциклові конгруентні генератори псевдовипадкових чисел, що задаються рекурентними співвідношеннями виду $x_n = bx_{n-1} + c(\mathrm{mod}\, n)$, при $n = 2^{16}$ та $n = 2^{32}$, при рекомендованих значеннях b, c.

Такі генератори мають добрі псевдовипадкові властивості, але є криптографічно слабкими. Це не впливає на надійність стандарту, оскільки параметри p, q мають бути загальнодоступні.

При звернені до процедури користувачі задають розмір $t_0 = t(p)$ (тобто розрядність) шуканого числа $p_0 = p$ у двійковій системі числення, початковий стан генератора x_0 та відповідний параметр c.За стандартом, процедура A дозволяє отримувати прості числа p довжини $t \geq 17_{10}$ бітів з простим дільником q довжини $\lfloor t/2 \rfloor$ числа $p-1$.

У процедурі застосовується генератор ПВЧ виду $x_n = 13981x_{n-1} + c(\mathrm{mod}2^{16})$.

Числа c і x_0 мають задовольняти умови $0 < c,\ x_0 < 2^{16}$, крім того, число c має бути непарним (умови повноцикловості).

Ми будемо проводити аналіз процедури у процесі її викладення, що надає нам змогу вчасно надавати пояснення та використовувати допоміжні формули.Позначимо розмір числа a через $|a| = \lfloor \log_2 a \rfloor + 1$. Зауважимо для подальшого, що якщо слово a довжиною $|a| = t$, розглядати як двійкове число, то $a = 2^{t-1} + \alpha_{t-2}2^{t-2} + \ldots + \alpha_1 2 + \alpha_0$; навпаки, якщо $a = 2^{t-1} + \eta$ і $0 \leq \eta < 2^{t-1}$, то $|a| = t$.

1.1. Опис процедури генерації простих чисел. Розглянемо процедуру A по кроках.

1. $y_0 := x_0$.

2. Покласти $t_0 := t(p)$. Обчислити (спадаючу) послідовність чисел $(t_0, t_1, \ldots, t_s)$, що складається з довжин $(t_1, \ldots, t_s)$ майбутніх проміжних простих чисел $(p_1, \ldots, p_s)$ і довжини $t_0 = t$ шуканого простого числа p_0 за наступним правилом.

Для $i := 0,1,2,\ldots$ перевіряти умову $t_i \geq 17$. Якщо умова виконується, то $t_{i+1} := \lfloor t_i/2 \rfloor$. Якщо умова не виконується, то покласти $s := i$ та перейти на п.3.

Зауваження. Числа p_m будуватимуться послідовно, у вигляді $p_m = Np_{m+1} + 1$, де N – парне.

3. Знайти найменше просте число p_s довжини t_s бітів.

4. $m := s - 1$. Значення змінної m тепер дорівнює індексу чергового (справа наліво) елемента в послідовності $(t_0, t_1, \ldots, t_s)$.

5. Обчислити $r_m = \lceil t_m/16 \rceil$. Змінна r_m дорівнює мінімальній кількості шістнадцятибітових блоків, в яких можна розмістити послідовність довжини t_m бітів.

6. На основі конгруентного генератора з початковим станом y_0 обчислити послідовність $y_1, \ldots, y_{r_m}$. Послідовність $y_{r_m-1}, \ldots, y_1, y_0$, відіграватиме роль цифр деякого числа Y_m що надано у системі за основою 2^{16}. Число y_{r_m} використаємо далі.

7. Обчислити $Y_m = \sum_{i=0}^{r_m-1} y_i \cdot 2^{16i}$.

8. $y_0 = y_{r_m}$. Готуємо новий (наступний) початковий стан генератора, щоб при переходах на п. 6 отримувати чергову послідовність виду $y_1, \ldots, y_{r_m}$ для побудови Y_m.

9. Обчислити $N = \left\lceil \frac{2^{t_m-1}}{p_{m+1}} \right\rceil + \left\lfloor \frac{2^{t_m-1} Y_m}{p_{m+1} 2^{16r_m}} \right\rfloor$. Якщо N непарне, то $N := N + 1$.

Число N – парне псевдовипадкове число, за допомогою якого буде здійснюватися побудова чергового проміжного простого числа p_m, виходячи з попереднього p_{m+1}.

Задля зручності, пояснення щодо кроків 9-13 надамо після закінчення опису процедури.

10. $k := 0$. Число k потрібне для модифікації фіксованого N у ході пошуку p_m, виходячи з p_{m+1}. У цьому процесі число k завжди буде парним: $k = 2i, i = 0,1,\ldots$(п. 13).

11. Обчислити $p_m = p_{m+1}(N+k)+1$.

12. Якщо $p_m > 2^{t_m}$, перейти на п. 6.

Для переходу на п.13 вимагається $p_m \le 2^{t_m}$, але p_m – непарне, тобто, $p_m < 2^{t_m}$. Це означає, що $p_m \le 2^{t_m-1}+\eta$, $\eta < 2^{t_m-1}$, тобто, $|p_m| \le t_m$. Насправді, виявляється, що випадок $|p_m| < t_m$ неможливий (див. далі). Таким чином, у п. 13 оброблятимуться лише числа p_m розміром в t_m бітів.

13. Перевірити умови:

а) $2^{p_{m+1}(N+k)} = 1 \pmod{p_m}$; б) $2^{(N+k)} \ne 1 \pmod{p_m}$.

Якщо хоч одна з умов не виконується, то $k := k+2$ і перейти до кроку 11. Якщо виконуються обидві умови, то число p_m вважається простим. Змінюємо $m := m-1$.

14. Якщо $m \ge 0$, перейти на крок 5 для пошуку наступного простого p_m більшого розміру. Якщо $m < 0$, то $p := p_0$, $q := p_1$ – кінець процедури.

1.2. Аналіз алгоритму. У виразі $p_m = p_{m+1}(N+k)+1$ (п. 11) значення N нарощується, якщо p_m не є простим, але необхідно враховувати обмеження $|p_m| = t_m$.

У кроці 12 можливість $p_m > 2^{t_m}$ блокується переходом на побудову нового значення N. Покажемо спочатку, що випадок $|p_m| < t_m$ неможливий.

Позначимо у виразі $N = \left\lceil \frac{2^{t_m-1}}{p_{m+1}} \right\rceil + \left\lfloor \frac{2^{t_m-1} Y_m}{p_{m+1} 2^{16 r_m}} \right\rfloor$ (п. 9) перший доданок через n_1, а другий доданок – через n_2. Оцінимо розмір числа $p_{m+1}n_1$.

Поділимо 2^{t_m-1} на p_{m+1} з остачею. Це можна записати як $2^{t_m-1} = r_1 + \lambda p_{m+1}$, де $\lambda > 0$ та r_1 – цілі, $0 < r_1 < p_{m+1}$. Тому $2^{t_m-1} + p_{m+1} - r_1 = (\lambda+1)p_{m+1}$.

Число $x = \frac{2^{t_m-1}}{p_{m+1}} > 0$ не є цілим, тому $\lceil x \rceil = \lfloor x \rfloor + 1$. Але $\lambda = \lfloor x \rfloor$, звідки $n_1 = \lambda + 1$, тобто,

$$p_{m+1}n_1 = 2^{t_m-1} + p_{m+1} - r_1 . \qquad (1)$$

Разом з тим, $p_{m+1} - r_1 > 0$, а $t_m = |2^{t_m-1}| = |p_m| \ge 2|p_{m+1}|$ за побудовою, тому $|p_{m+1}n_1| = t_m$. Крім того, $|2p_{m+1} - r_1| \le t_{m+1} + 1$ і, очевидно, $|p_{m+1}(n_1+1)| = |2^{t_m-1} + 2p_{m+1} - r_1| = t_m$. Це виправдовує присвоєння $N := N+1$ у кроці 9 і дозволяє вважати далі N парним.

Таким чином, двійковий запис (1) числа $p_{m+1}n_1$ має вигляд $100\ldots00{*}{*}\ldots{*}$, де кількість символів $*$ не перевищує $t_{m+1}+1$ та містить серію нулів, довжина якої не менше $t_m - t_{m+1} - 2$, а саме: $\frac{t_m}{2} - 2$, при $t_m = 0 \pmod 2$, або $\frac{t_m+1}{2} - 2$, якщо $t_m = 1 \pmod 2$. (2)

Зі структури числа (1) випливає, що випадок $|p_m| < t_m$ неможливий.

Аналогічно, для оцінки розміру числа $p_{m+1}n_2$ запишемо $2^{t_m-1}Y_m = r_2 + \mu p_{m+1} 2^{16 r_m}$, де μ та r_2 – цілі, $0 \le r_2 < p_{m+1}2^{16 r_m}$. Оскільки $n_2 = \mu$, то

$$p_{m+1}n_2 = \frac{2^{t_m-1}Y_m - r_2}{2^{16 r_m}} . \qquad (3)$$

Кількість двійкових розрядів числа Y_m знаходиться у межах від $16r_m-15$ до $16r_m$. Якщо навіть всі вони – одиниці, то відповідне значення $Y_m = 2^{16r_m}-1$ є максимальним, тобто завжди $\frac{Y_m}{2^{16r_m}}<1$. Тому $p_{m+1}n_2 < 2^{t_m-1} - \frac{r_2}{2^{16r_m}}$, звідки: $|p_{m+1}n_2| \le t_m - 1$.

Оскільки ділення двійкових чисел на два є зсувом на розряд управо від коми, то з (3) випливає, що $p_{m+1}n_2$ являє собою деяке число виду $u-\gamma p_{m+1}$, де u створено старшими розрядами числа Y_m, $0 \le \gamma < 1$. Розмір u може дорівнювати t_m-1, або бути менше, за рахунок перших нулів у старшій цифрі числа Y_m.

Розглянемо тепер вираз з п. 11 у вигляді двох доданків:

$$p_m = p_{m+1}(N+k)+1 = [p_{m+1}(n_1+k)+1] + p_{m+1}n_2. \qquad (4)$$

З (1) випливає, що $t(k) \overset{df}{=} |p_{m+1}(n_1+k)+1| = |2^{t_m-1} + (k+1)p_{m+1} + 1 - r_1| \le |2^{t_m-1} + (k+2)p_{m+1}|$, крім того, $t(0) = t_m$. Для якої кількості випадків виконується $t(k) = t_m$?

Вимога $|2^{t_m-1} + (k+2)p_{m+1}| = t_m$ є еквівалентною умові $|(k+2)p_{m+1}| < t_m$, яка при $k=0$, очевидно, виконується.

Далі. Для цілих x, y, $x>0$, $y>0$, має місце

$$|xy| = |x|+|y|, \text{ або } |xy| = |x|+|y|-1, \qquad (5)$$

тому $|(k+2)p_{m+1}| = |k+2|+|p_{m+1}|-v < t_m$, де $0 \le v \le 1$, тобто $|k+2| < t_m - |p_{m+1}| + v$.

Звідки $|k+2| < \frac{t_m}{2}$, при $t_m = 0(\mathrm{mod}2)$, або $|k+2| < \frac{t_m+1}{2}$, якщо $t_m = 1(\mathrm{mod}2)$. (6)

Умови (2) і (6) можна узгодити, якщо прийняти $|k+2| \le \frac{t_m}{2} - 2$.

Таким чином, у першому доданку з (4), принаймні, для довільних значень $k = 2j = 0,2,4,\ldots$, де $\max j = \max \frac{k+2}{2} \le 2^{\left(t_m/2\right)-3}$, переносу зі старшого розряду не виникає внаслідок серії нулів, тому за рахунок цього числа перехід у п. 12 на побудову нового Y_m не відбувається.

Виходячи зі структури $2^{t_m-1}+\delta$ першого доданку (4), при додаванні його до числа $p_{m+1}n_2$ в останньому задіяні $|\delta| \le t_{m+1}+1$ молодших розрядів, тобто, приблизно, половина $|p_{m+1}n_2|$.

Нехай, при додаванні виникає перенос одиниці поза старший розряд числа δ.

Тільки у випадку, коли $p_{m+1}n_2$ має максимально допустимий розмір t_m-1 і перенос розповсюдиться аж до старшого розряду числа $p_{m+1}n_2$, розмір суми (4) дорівнюватиме t_m+1 і випадковий пошук p_m при фіксованому N виявиться невдалим та здійсниться перехід на обчислення нового значення N. У подібних випадках старші розряди Y_m повинні мати спеціальний вид, оскільки за визначенням числа Y_m число $p_{m+1}n_2$ є псевдовипадковим і його старші розряди суттєво залежать від Y_m.

Ймовірність таких ситуацій зменшується за рахунок того, що r_m послідовних шістнадцятибітових цифр, які утворюють числа Y_m вибираються з орбіти конгруентного генератора послідовно, без перетину, більш того, внаслідок повноцикловості генератора, у числах Y_m цифри не повторюються.

З цього випливає, що зміна N відбувається частіше при малих $|p_m|$, а при великих значеннях $|p_m|$ можливостей для пошуку при фіксованому N стає суттєво більше.

Для $|p_m|=1024$ $r_m=64$, тому мінімальна кількість варіантів Y_m дорівнює 1023.

Враховуючи (2), (6), можна вважати, що чисел, які підлягають перевірці у п.13, тобто мають розрядність t_m, достатньо багато.

1.3. Перевірка на простоту. Перепозначимо $p_m = Rp_{m+1}+1$, де $R=N+k$.

Покажемо, що при $|p_m|=t_m=0(2)$ виконується нерівність $R<4(p_{m+1}+1)$.

Дійсно, якщо це не так, то $R\ge 4(p_{m+1}+1)$ і $p_m\ge(2p_{m+1}+1)^2$. З (5) випливає, що $|p_m|\ge 2(|p_{m+1}|+1)-1=2|p_{m+1}|+1$, але $|p_m|=2|p_{m+1}|$ – протиріччя.

Для подальшого зауважимо, що при $|p_m|=1(\mathrm{mod}\,2)$ з попереднього випливає $|p_m|=2|p_{m+1}|+1$, тому не виключається, що $p_m=(2p_{m+1}+1)^2$.

Тепер ми можемо довести наступне твердження.

Теорема. Якщо $|p_m|=0(\mathrm{mod}\,2)$ і виконуються умови а), б) п. 13, то p_m – просте.

Дійсно, згадані умови і нерівність $R<4(p_{m+1}+1)$ складають умови наступної теореми Демитко при $n=p_m$, $q=p_{m+1}$, $a=2$.

Теорема Демитко [3]. Нехай $n=qR+1$, де q –просте, R –парне і $R<4(q+1)$. Якщо існує ціле a таке, що $a^{n-1}=1(\mathrm{mod}\,n)$ і $a^{(n-1)/q}\ne 1(\mathrm{mod}\,n)$, то число n – просте.

Наявність простих чисел серед чисел p_m, що генеруються можна обгрунтувати, якщо розглянути послідовність $p_m=p_{m+1}N+1+2jp_{m+1}$, $j=0,1,2\ldots$ як арифметичну прогресію $l_j=l_0+jd$ виду $l_0=p_{m+1}N+1$, $d=2p_{m+1}$, НСД$(l_0,d)=1$.

Позначимо через $\pi(x,d,l)$ кількість простих чисел p, що належать до прогресії $\{l_j\}$ і не перевищують x. Відомо [4. ст.157], що має місце хороше наближення $\pi(x,d,l)\sim\dfrac{x}{\varphi(d)\ln x}$, де $\varphi(x)$– функція Ейлера.

Оскільки $\pi(2^t,d_1,l_1)\sim\dfrac{2^t}{(p_{m+1}-1)\ln 2^t}=\dfrac{2^t\log_2 e}{(p_{m+1}-1)t}\approx\dfrac{2^{t/2}\log_2 e}{t}$, а $\pi(2^{t/2},d_2,l_2)\approx\dfrac{2^{t/4}\log_2 e}{t/2}$,

то $\pi(x,d_1,l_1)-\pi(x,d_2,l_2)\approx\dfrac{\log_2 e}{t}2^{t/4+1}(2^{t/4-1}-1)$.

Зауважимо, що зі зміною N нова прогресія матиме ту саму властивість, оскільки оцінка від l_0 не залежить. Таким чином, при переході від p_{m+1} до p_m простих чисел перевіряється достатньо багато.

Повернемося до випадку$|p_m|=1(\mathrm{mod}\,2)$. Припустимо, що критерій п.13 проходить, але число p_m складене. Щоб з'ясувати його структуру, застосуємо підхід, який використовується при доведенні теореми Демитко [6, ст.185], виходячи з наступної леми.

Лема. Нехай $n=q^kQ+1>1$, де q – просте. Якщо існує натуральне число a, таке, що $a^{n-1}=1(\mathrm{mod}\,n)$ і $a^{(n-1)/q}\ne 1(\mathrm{mod}\,n)$, то число n має простий дільник p виду $p=q^kr+1$, при деякому $r=r(p)$.

Таким чином, у нас $n=p_m=\prod p_i^{d_i}$ – непарне, $i>1$, $r=0(2)$, $k=1$, $q=p_{m+1}$, $Q=R$, $a=2$. За лемою, існує i, таке, що $q\,|\,(p_i-1)$. Запишемо $n=wp_i$. Оскільки $n=1(q)$ і $p_i=1(q)$, то і $w=1(q)$, звідки $w=1+Kq$, $p_i=1+Sq$, де K і S парні, тому що n непарне.

Насправді, $K, S \geq 2$. Дійсно, якщо $K = 0$, то $n = p_i$ – просте, що невірно за припущенням. Якщо $S = 0$, то $p_i = 1$ і це суперечить тому, що p_i просте. Звідси випливає $w \geq 2q+1$, $p_i \geq 2q+1$ і $n \geq (2q+1)^2$, тобто $p_i \geq 2p_{m+1}+1$, $wp_i = p_m \geq (2p_{m+1}+1)^2$.

Легко бачити, що при $K = 2, S = 4$ (або навпаки) в останній формулі строга нерівність порушується за рахунок перевищення $|p_m|$, тому $K = S = 2$.

Як наслідок маємо $p_m = (2p_{m+1}+1)^2$, тобто $p_m = u^2$, де $u = 2p_{m+1}+1$ – просте число.

Таким чином, строго обґрунтувати критерій перевірки на простоту не вдається.

З цього приводу, припустимо, що результатом пошуку є складене значення $p_m = u^2$.

Тоді $\varphi(u^2) = u^2 - u$, $2^{p_m - 1} = 1 (\mathrm{mod}\ p_m) \Rightarrow 2^{u^2 - 1 - \varphi(u^2)} = 1 (\mathrm{mod}\, u^2) \Rightarrow 2^{u-1} = 1 (\mathrm{mod}\, u^2)$.

Прості числа u, які задовольняють останнє порівняння, називаються числами Віфериха за основою 2. Серед чисел до $6 \cdot 10^9$ [5], це тільки 1093, 3511. Інші подібні числа авторам невідомі. Крім того, питання, чи нескінченна множина простих чисел виду $2p+1$, де p просте, є невирішеною проблемою.

Цікаво, що числа Віфериха виникли у спробах доведення Великої теореми Ферма.

Зокрема, перший випадок цієї теореми справедливий, якщо показник у гіпотетичній рівності $x^u + y^u = z^u$ є числом Віфериха за основою $w \leq 43$. Зауважимо також те, що числа 1093 та 3511 не належать до чисел виду $2p+1$.

Висновки. Алгоритм генерації спеціальних простих чисел ГОСТ Р 34.10 – 94 за процедурою *A* реалізує випадковий пошук з критерієм перевірки на простоту, який можна строго обґрунтувати, виходячи з теореми Демитко, при побудові чисел, розмір яких є степенем двійки (у перевірочних прикладах стандарту інші числа не розглядаються).

Якщо послідовність зростаючих розмірів чисел, виходячи з якої будується шукане число, містить непарне значення, строго довести достатність критерію не вдається.

Оскільки критерій простоти, сам по собі, не є строгим детермінованим критерієм, то суттєву роль мають відігравати статистичні особливості структури проміжних псевдовипадкових чисел, що генеруються. Це, принаймні потенційно, може призводити до збільшення часу роботи алгоритму при побудові чисел з непарним розміром.

Щодо можливості застосування процедури А для побудови параметрів криптосистеми RSA, то алгоритм використовувати недоцільно, оскільки початкові значення генератора ПВЧ знаходяться перебором і дільник RSA-модуля отримується менше ніж за 2^{32} випробувань.

Література

1. Бессалов А. В. Представление элементов якобиана гиперэллиптической кривой рода два / А. В Бессалов, Д. Б. Третьяков // Сучасний захист інформації. – 2010. – № 4. – С.122-126.

2. Информационная технология. Криптографическая защита информации. Цифровая подпись на базе асимметричного криптографического алгоритма // ГОСТ Р 34.10-94. – М.: Изд-во стандартов, 1994.

3. Demytko N. Generating multiprecision integers with guaranteed primality / N. Demytko // Computer Age of Information. – 1989. – P. 1-8.

4. Прахар К. Распределение простых чисел / К. Прахар – М.: Мир, 1967. – 511с.

5. Lehmer D. On Fermat's Quotient base two / Lehmer D. // Mathematics of Computation. – 1981. – V.36. – P. 289-290.

6. Мухачов В. А. Методы практической криптографии / В. А. Мухачов, В. А. Хорошко. – К.: ООО «ПолиграфКонсалтинг» , 2005. – 215с.