Лабораторная работа №3

Изучение циклических алгоритмов, операторов цикла, программирование циклического вычислительного процесса

Цели и задачи работы: изучение циклических алгоритмов, операторов цикла, программирование циклического вычислительного процесса.

Задание к работе: Реализовать циклический вычислительный процесс. Самостоятельно решить задачи в соответствии с индивидуальным вариантом.

Задание 1. Вычислить и вывести на экран или в файл в виде таблицы значения функции, заданной графически, на интервале от *Хнач* до *Хкон* с шагом *dx*. Интервал и шаг задать таким образом, чтобы проверить все ветви программы. Таблица должна иметь заголовком и шапку.

Задание 2. Реализовать $a^x \bmod p$ Сравнения по модулю простого числа через теорему Ферма и свойства сравнений.

Задание 3. Реализовать обобщенный алгоритм Евклида для вычисления c*d mod m=1.

Задание 4. Реализовать расширенный алгоритм Евклида для вычисления взаимообратного числа $c^{-1} \bmod m=d$.

Задание 5. Написать программу, использующую алгоритм шифрования данных для преобразования исходного текста.

Задание 6*. Тесты на простоту.

Задание 7. Найти последнюю цифру «трехэтажного числа». Например,

$$3^{7^8}$$

Литература для реализации заданий 3 – 5 (есть в курсе на диспейс):

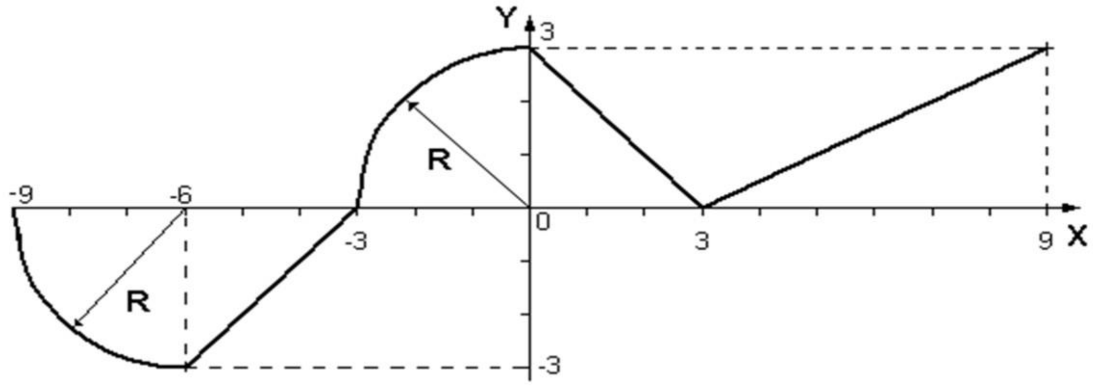
Рябко, Б. Я. Основы современной криптографии и стеганографии [Текст] : монография / Б. Я. Рябко, А. Н. Фионов. - Москва : Горячая линия-Телеком, 2010. - 232 с.

(или другие годы издания)

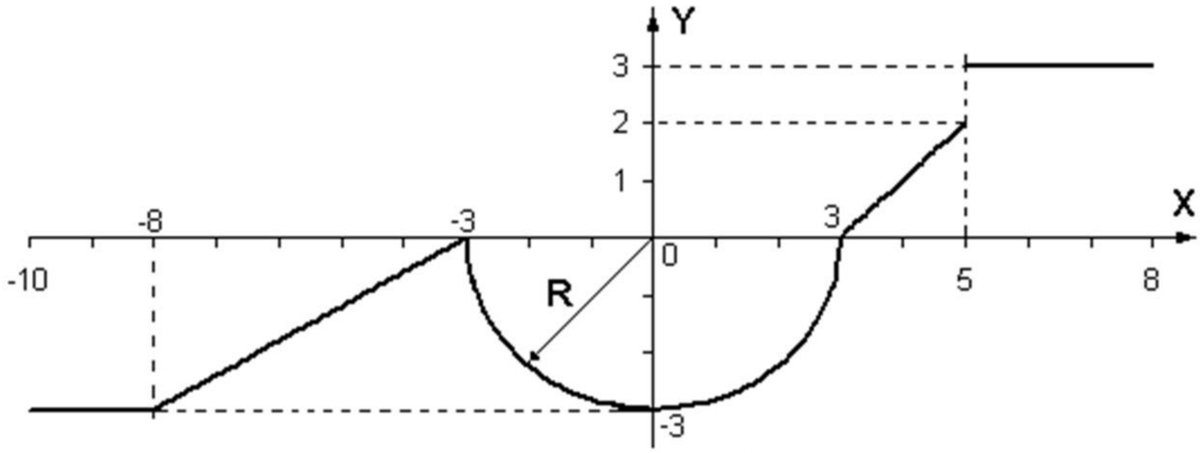
Задание №3.1

Параметры, необходимые для решения задания следует получить из графика и определить в программе.

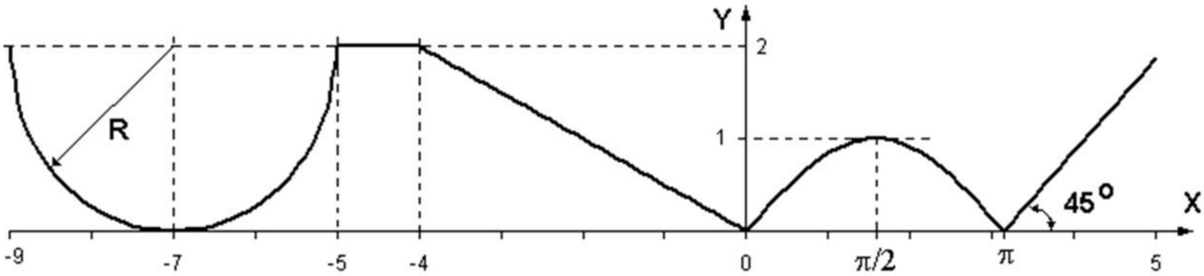
1)



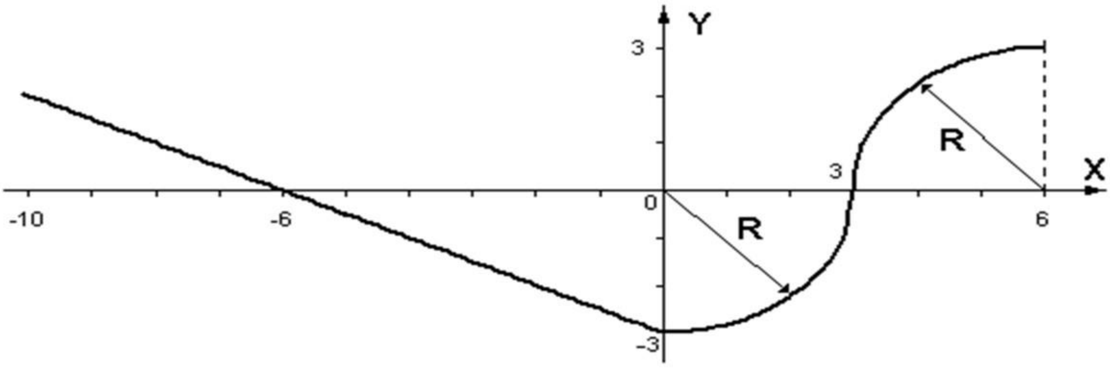
2)



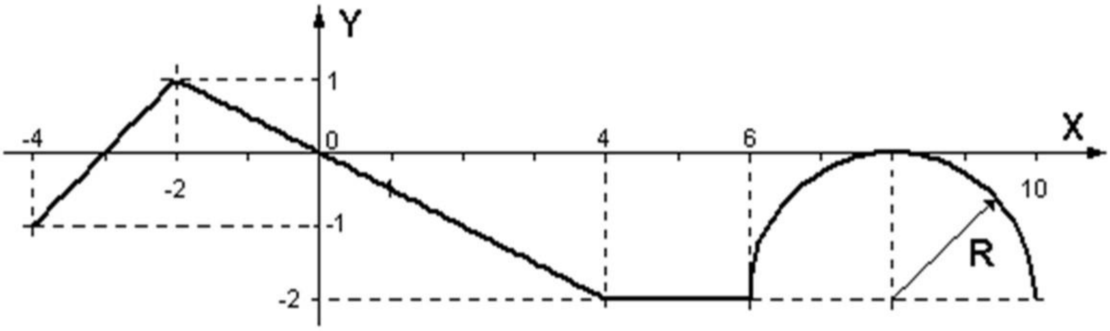
3)



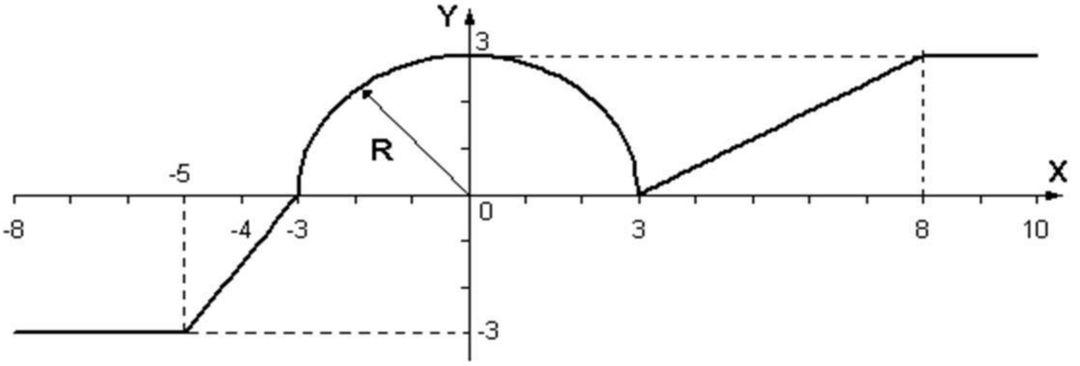
4)



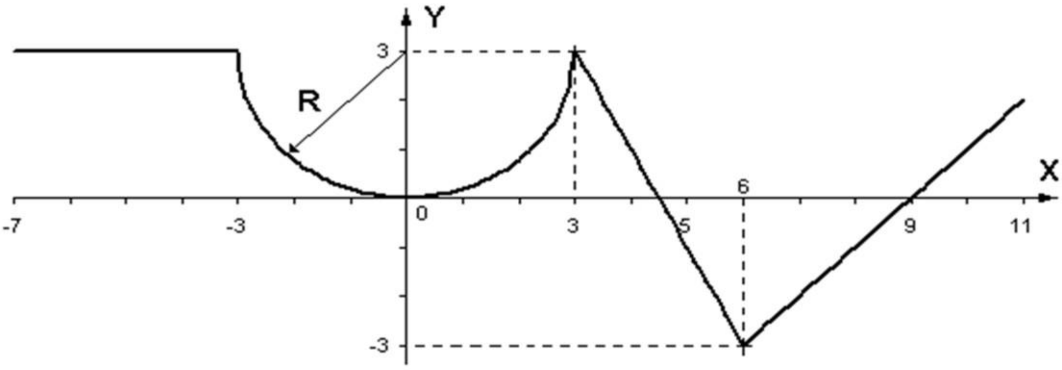
5)


Y
X
1
-1
-2
-4
-2
0
4
6
10
R

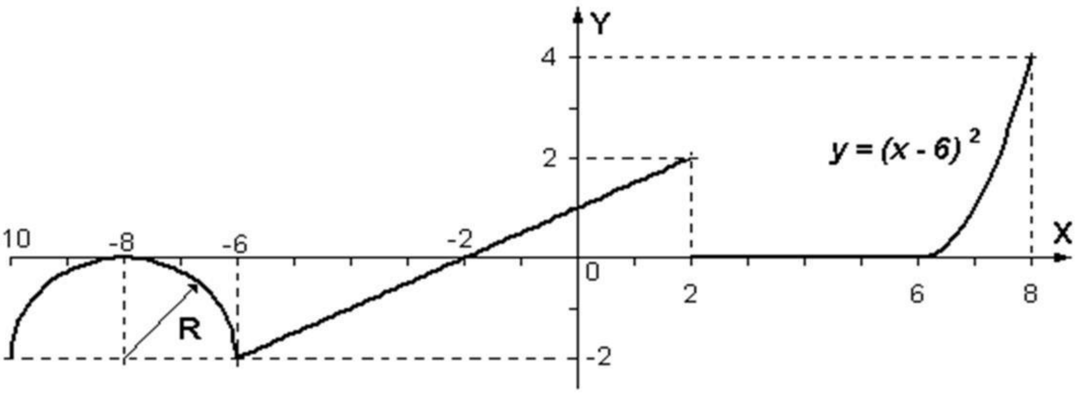
6)


Y
X
3
-3
-5
-8
-4
-3
0
3
8
10
R

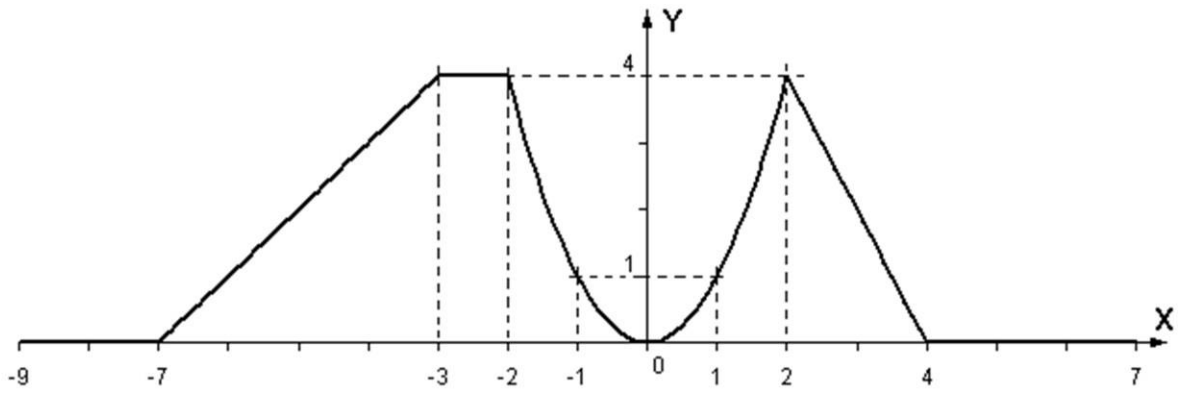
7)


Y
X
3
-3
-7
-3
0
3
5
6
9
11
R

8)

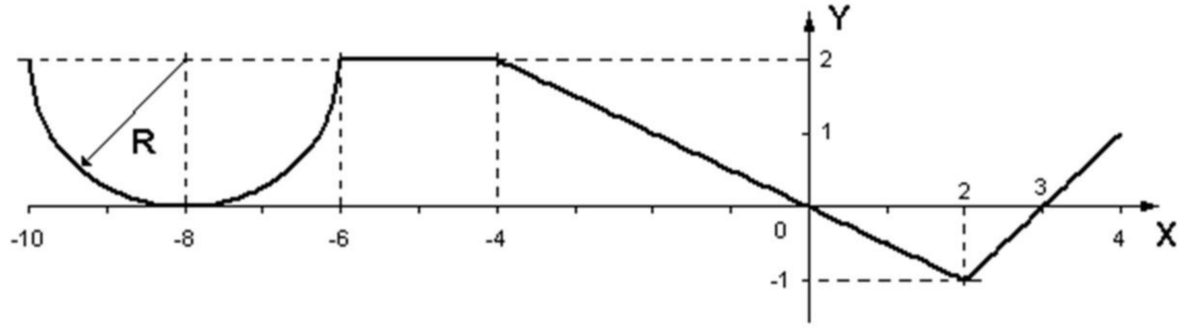

Y
X
4
2
-2
-10
-8
-6
-2
0
2
6
8
R
y = (x - 6) 2

9)



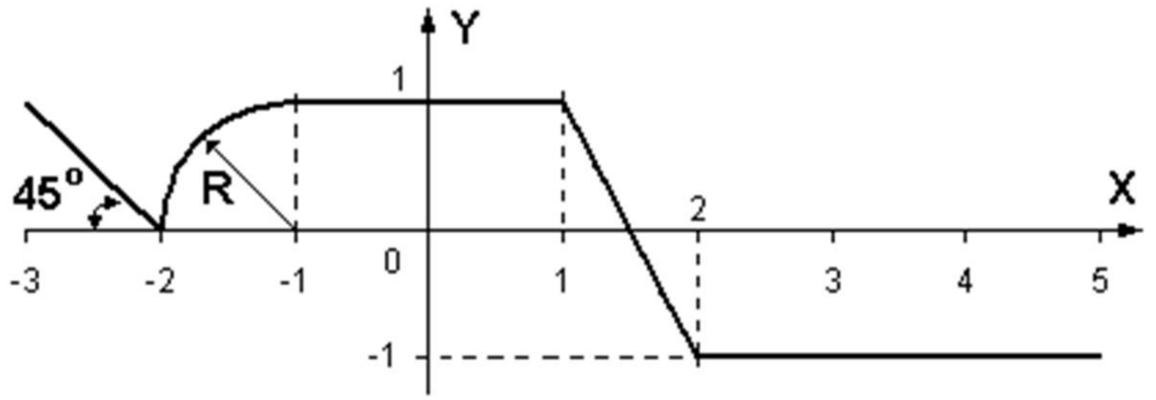
Y
4
1
X
-9
-7
-3
-2
-1
0
1
2
4
7

10)



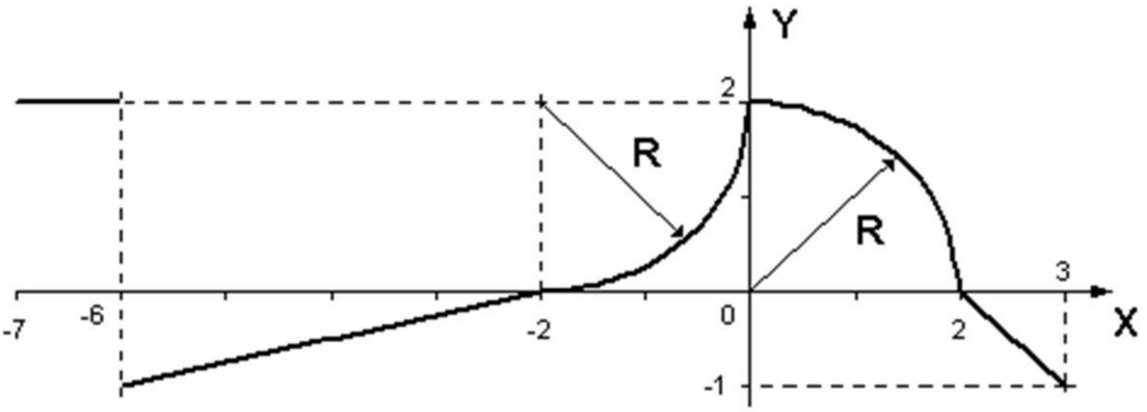
Y
2
1
R
2
3
-10
-8
-6
-4
0
4
X
-1

11)



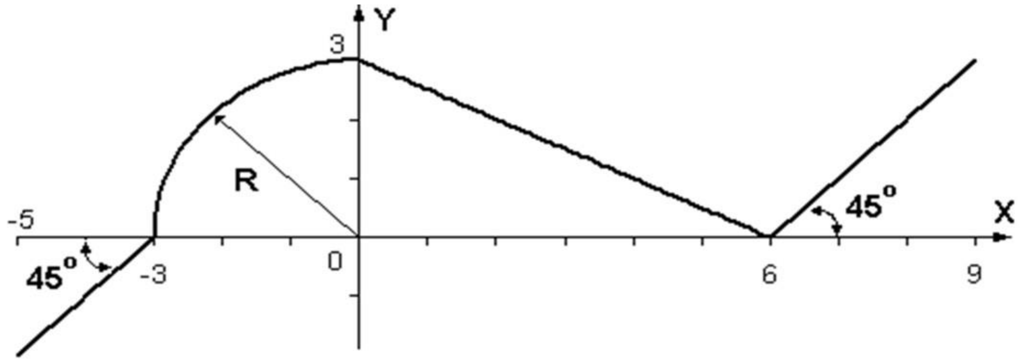
Y
1
45°
R
X
2
-3
-2
-1
0
1
3
4
5
-1

12)

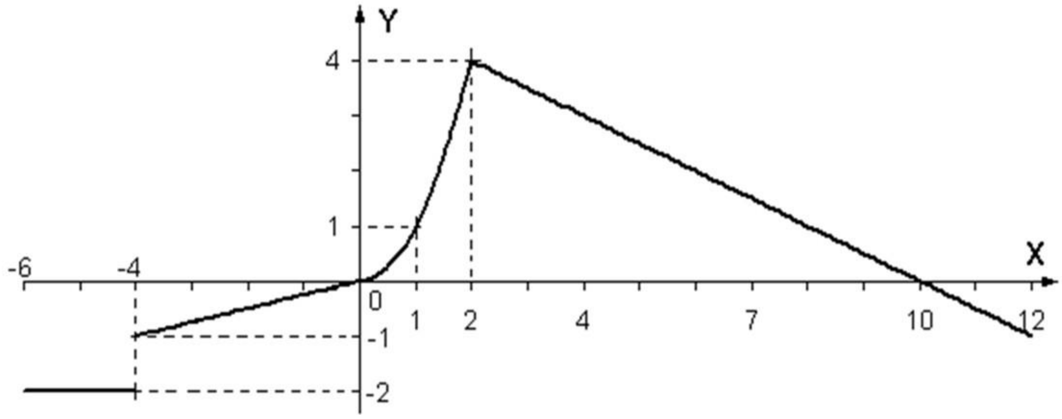


Y
2
R
R
3
-7
-6
-2
0
2
X
-1

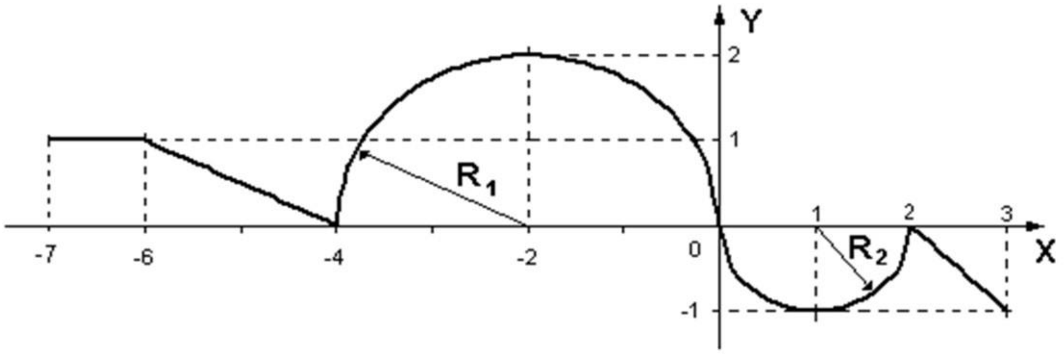
13)


Y
3
R
-5
45°
X
45°
0
-3
6
9

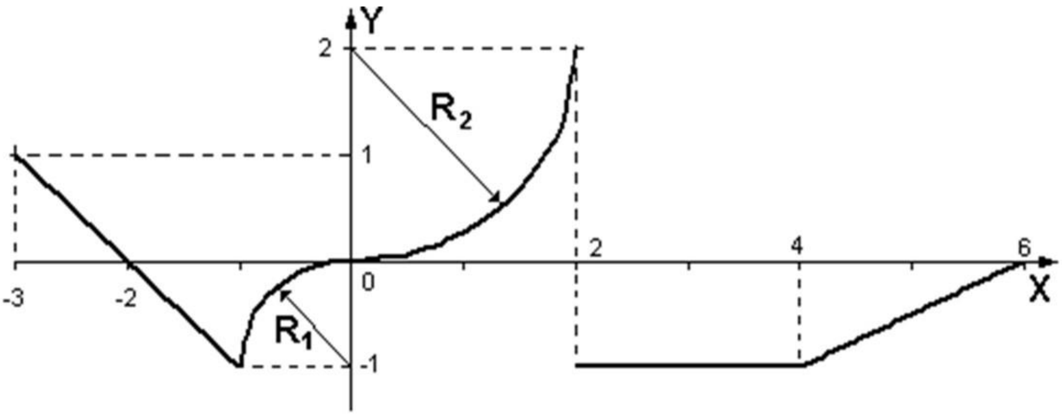
14)


Y
4
1
-6
-4
X
0
1
2
4
7
10
12
-1
-2

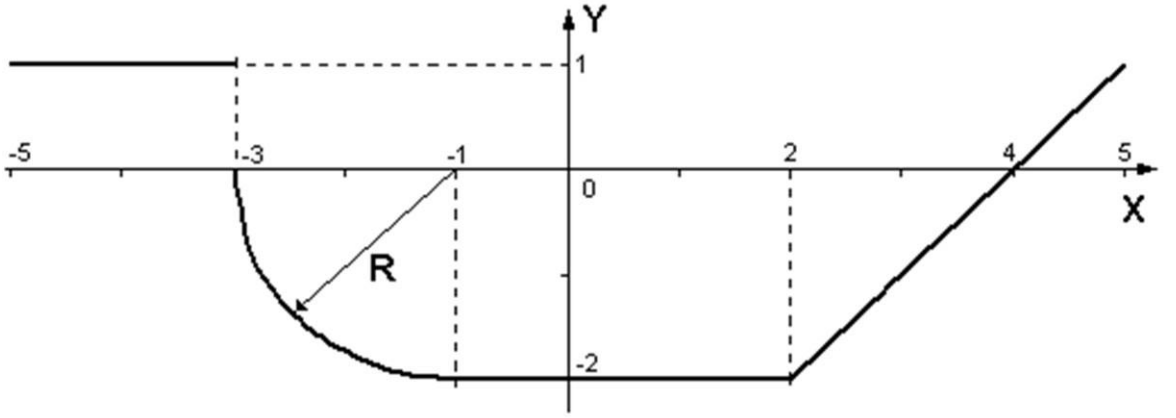
15)


Y
2
1
R_1
1
2
3
R_2
X
-7
-6
-4
-2
0
-1

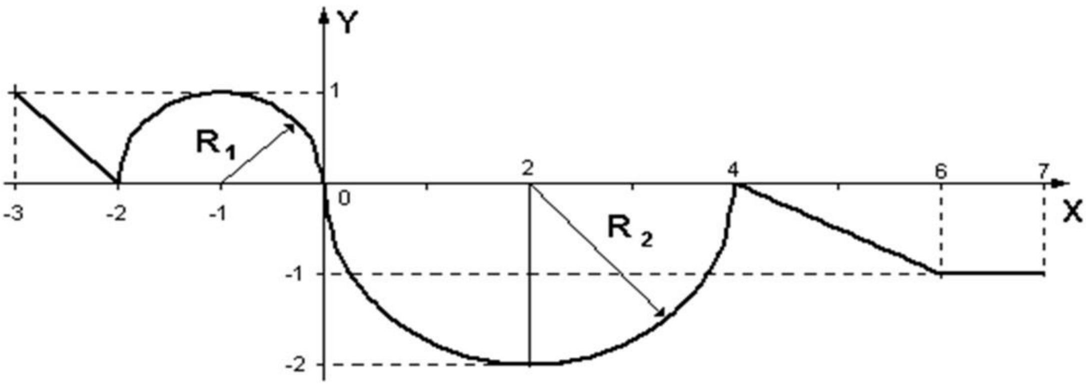
16)


Y
2
R_2
1
2
4
6
X
-3
-2
0
R_1
-1

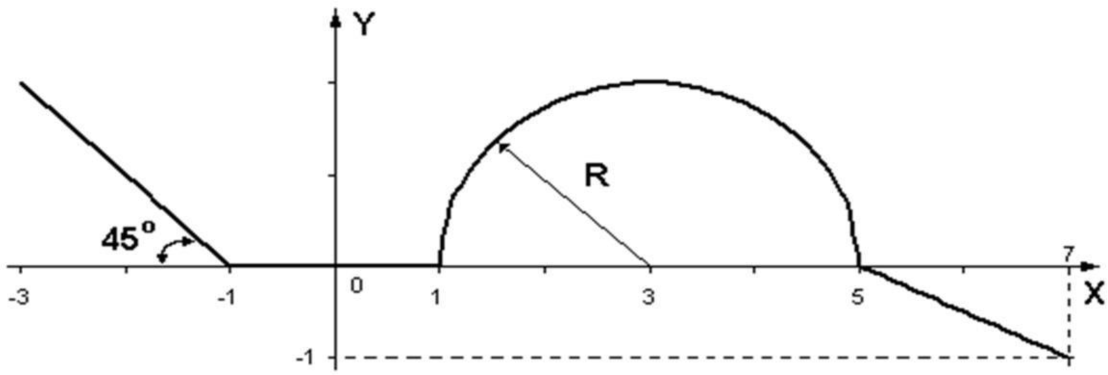
17)


Y
1
-5
-3
-1
2
4
5
0
X
R
-2

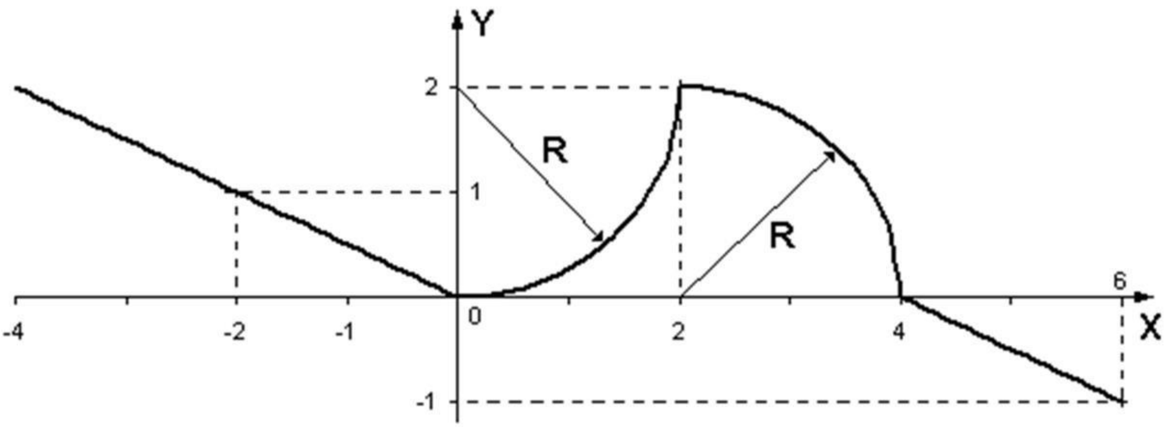
18)


Y
1
R1
-3
-2
-1
0
2
4
6
7
X
R2
-1
-2

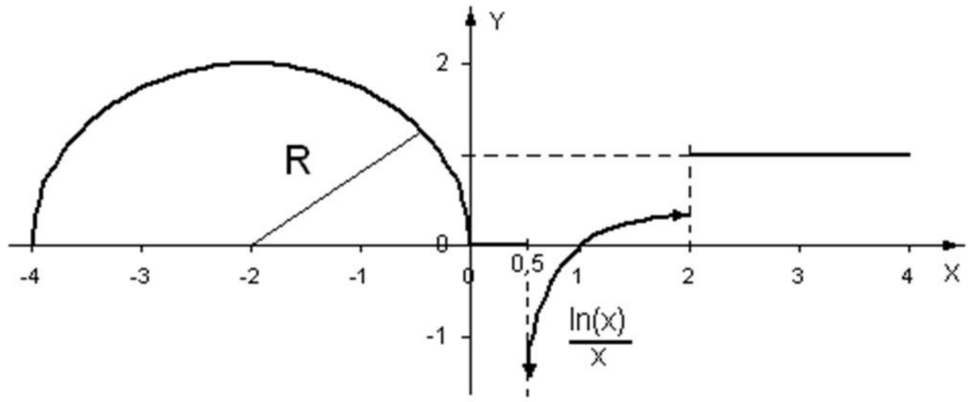
19)


Y
R
45°
-3
-1
0
1
3
5
7
X
-1

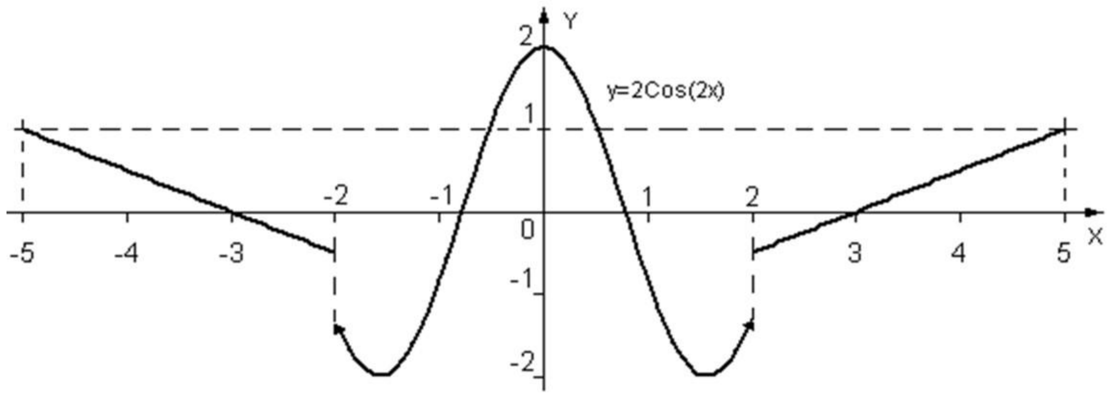
20)


Y
2
R
1
R
-4
-2
-1
0
2
4
6
X
-1

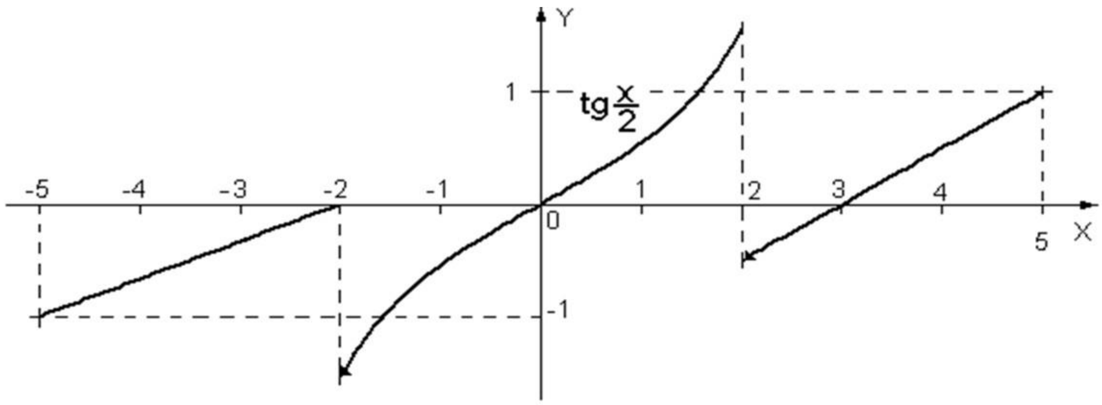
21)


Y
2
R
0
0,5
-4
-3
-2
-1
0
1
2
3
4
X
-1
ln(x)
x

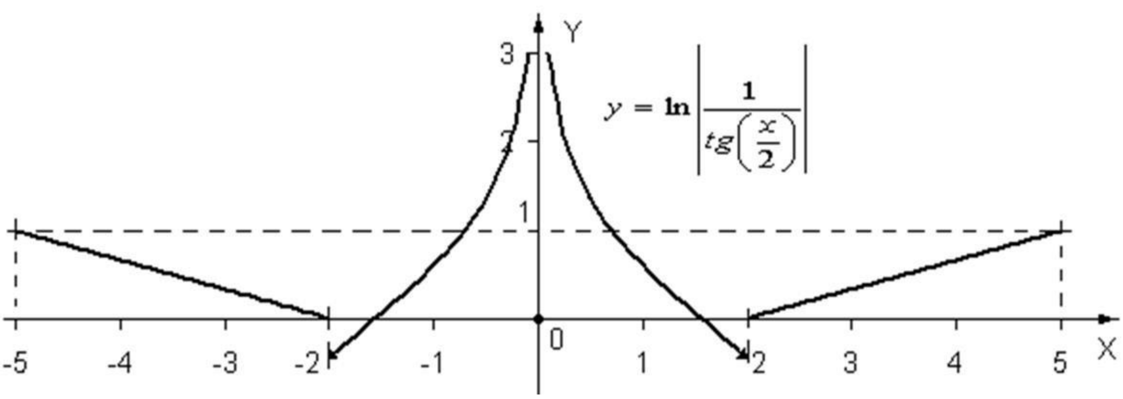
22)


Y
2
y=2Cos(2x)
1
-2
-1
1
2
0
-5
-4
-3
3
4
5
X
-1
-2

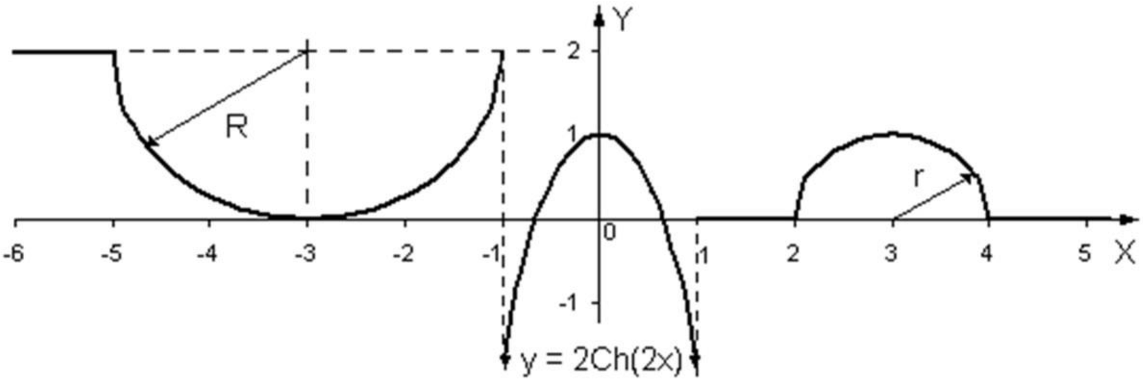
23)


Y
1
tg x/2
-5
-4
-3
-2
-1
1
2
3
4
0
5
X
-1

24)

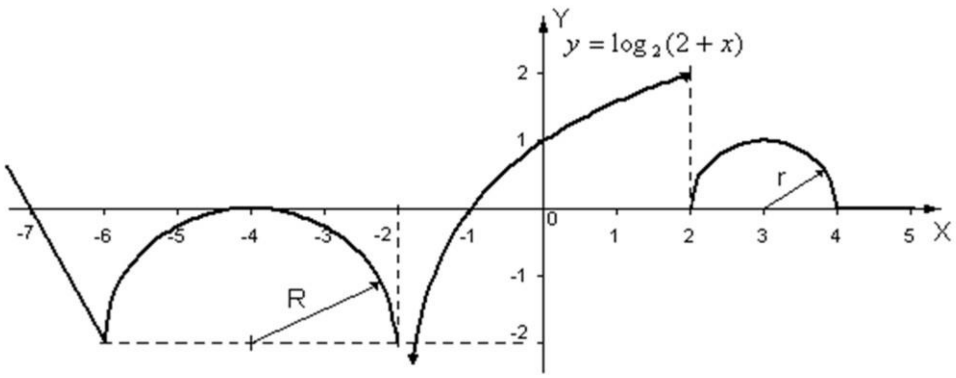

Y
3
$y = \ln\left|\frac{1}{tg\left(\frac{x}{2}\right)}\right|$
2
1
0
-5
-4
-3
-2
-1
1
2
3
4
5
X

25)

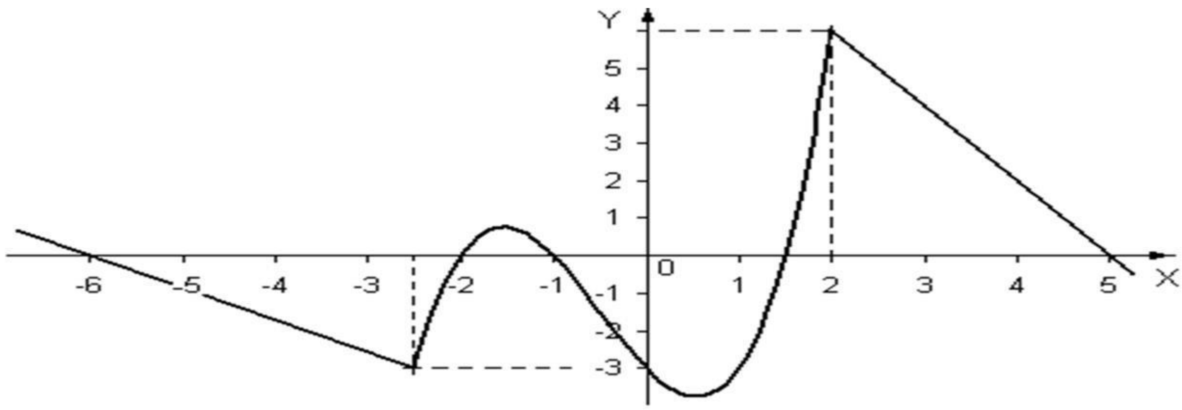


Гиперболический косинус может быть вычислен по формуле: $Ch(x) = \frac{1}{2}\left(e^{x} + e^{-x}\right)$.

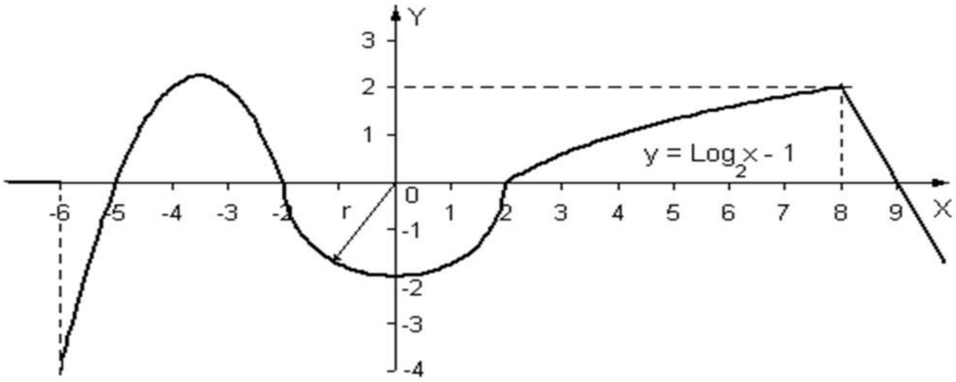
26)



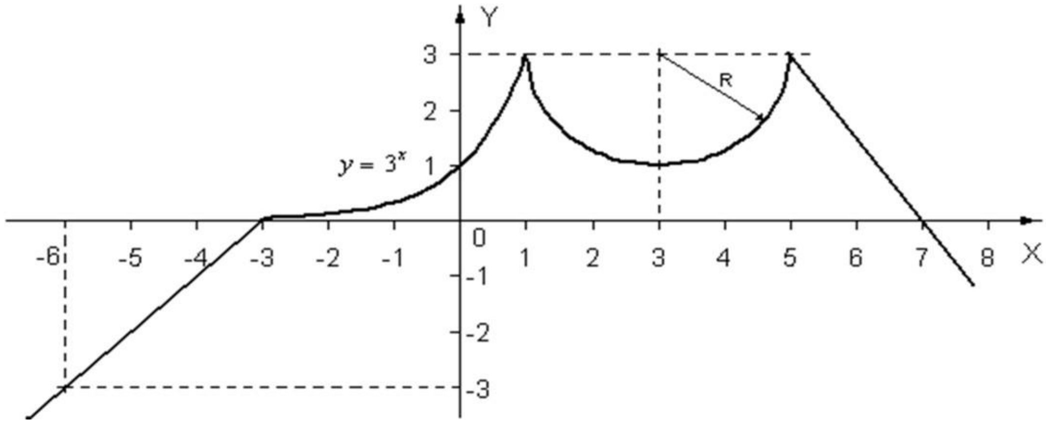
27)



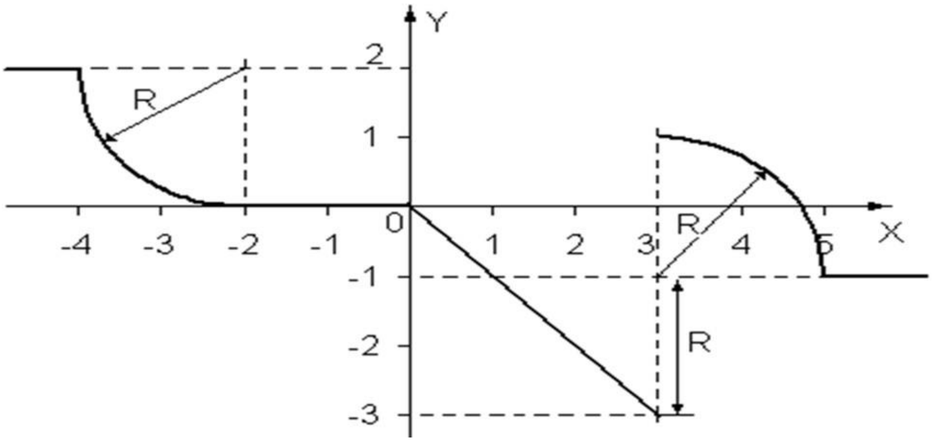
28)



29



30)



Задание №3.5

Написать программу, использующую криптопротоколы вида.
Вариант 1 - Диффи-Хеллмана
Вариант 2 - Шамира
Вариант 3 - Эль-Гамаля
Вариант 4 – RSA
Вариант 5 - Хьюза (Hughes)

Выбор варианта по модулю 5.

Задание №3.6*

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Доказуемо простые числа, как правило, используются в качестве модулей криптосистем, основанных на проблеме дискретного логарифмирования, таких как шифр Шамира, криптосистема Эль-Гамаля и связанные с ней стандарты цифровой подписи ГОСТ Р 34.11-94, ГОСТ Р 34.11-2001, DSA и ECDSA. Рассмотрим тесты на простоту Миллера, Поклингтона, ГОСТ.

1 Тест Миллера на простоту

Тест Миллера основан на теореме Сэлфриджа.

Алгоритм построения простого числа с помощью теста Миллера следующий:

1. Строится таблица малых простых чисел q_i (или используется готовая таблица);

2. Строится число $m=q_1^{\alpha 1}q_2^{\alpha 2}\ldots q_k^{\alpha k}$ (где q_i—различные случайные простые числа из таблицы, α_i – случайные целые числа), размер которого на 1 бит меньше требуемого размера для простого числа;

3. Вычисляется значение $n=2m+1$;

4. Построенное число n испытывается тестом Миллера с заданным параметром надежности. Если результат проверки отрицательный, то следует вернуться на шаг 2 и построить новое число m.

Тест Миллера:

Вход: n – число для проверки, $n—1=q_1^{\alpha 1}q_2^{\alpha 2}\ldots q_k^{\alpha k}$ - каноническое разложение, t – параметр надежности.

1. Выбрать t различных целых случайных чисел a_j: $1<a_j<n$.

2. Для каждого a_j вычислить $a_j^{n—1} \bmod n$. Если какой-либо из результатов не равен «1», то идти на Выход с сообщением «n – составное число».

3. Для каждого q_i выполнить:

3.1. Для каждого a_j вычислить $a_j^{\frac{n-1}{q_i}} \bmod n$. Если какой-либо из результатов не равен единице, то идти на шаг 3, взять следующее q_i. Если все результаты равны «1», то идти на Выход с сообщением «вероятно, n – составное число».

4. Идти на Выход с сообщением «n – простое число».

Выход.

Если число n было предварительно проверено на простоту вероятностным тестом Миллера-Рабина, то в тесте Миллера достаточно перебрать 4-6 значений a_j.

Если n – нечетное простое число, то вероятность того, что n по случайно выбранному основанию $1<a<n$ пройдет проверку на шаге 3.1, есть φ(n-1)/(n-1).

https://en.wikipedia.org/wiki/Miller–Rabin_primality_test - Миллер-Рабин Википедия (анг).
http://compoasso.free.fr/primelistweb/page/prime/liste_online_en.php - Сайты, для поиска простых чисел.

2 Тест Поклингтона

Тест Поклингтона основан на теореме Поклингтона и позволяет проверять простоту числа n, если каноническое разложение числа (n-1) известно лишь частично.

Алгоритм построения простого числа с помощью теста Поклингтона следующий:

1. Строится таблица малых простых чисел q_i (или используется готовая таблица);

2. Строится число $F=q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_k^{\alpha_k}$ (где q_i—различные случайные простые числа из таблицы, α_i – случайные целые числа), размер которого на 1 бит больше половины требуемого размера для простого числа;

3. Вычисляется значение n=RF+1, где R – случайное четное число, размер которого на 1 бит меньше размера F;

4. Построенное число n испытывается тестом Поклингтона с заданным параметром надежности. Если результат проверки отрицательный, то следует вернуться на шаг 2.

Тест Поклингтона (данные представлены в Приложении):

Вход: n – число для проверки: n—1=RF, F>R, $F=q_1^{\alpha 1}q_2^{\alpha 2}...q_k^{\alpha k}$ - каноническое разложение; t – параметр надежности.

1. Выбрать t различных целых случайных чисел a_j: $1<a_j<n$.

2. Для каждого a_j вычислить (a_j^{n-1} mod n. Если какой-либо из результатов не равен «1», то идти на Выход с сообщением «n – составное число».

3. Для каждого a_i выполнить:

3.1. Для каждого q_j вычислить $(a_i^{\frac{n-1}{q_j}})$ mod n. Если какой-либо из результатов равен единице, то идти на шаг 3, взять следующее a_i. Если все результаты не равны «1», то идти на Выход с сообщением «n – простое число».

4. Идти на Выход с сообщением «вероятно, n – составное число».

Выход.

Если n=RF+1 – нечетное простое число, $F>\sqrt{n}—1$, $F=q_1^{\alpha_1}q_2^{\alpha_2}...q_k^{\alpha_k}$, НОД(R,F)=1, то вероятность того, что случайно выбранное $1<a<n$ будет удовлетворять условиям теоремы Поклингтона, есть $\prod_{i=1}^{k}(1-\frac{1}{q_i})$.

Если известно полное разложение n—1, то в качестве F следует брать число, составленное из наибольших делителей n—1 для того, чтобы:

1) сократить число проверок для каждого a;

2) уменьшить степени, в которые возводится a на этапе проверки;

3) повысить вероятность того, что случайно выбранное a будет удовлетворять условиям теоремы Поклингтона, а значит уменьшить количество перебираемых a.

Пример

Вход: n=4021. $\sqrt{n}—1<63$.

n—1=4020=$2^2 \cdot 3 \cdot 5 \cdot 67$. F=67, R=$2^2 \cdot 3 \cdot 5$=60.

Проверка условий:

a=2.

1) $2^{4020} \bmod 4021=1$.

2)$2^{4020/67} \bmod 4021 = 2^{60} \bmod 4021=1452$.

Выход: n=4021 – простое число.

(Заметим, что вероятность того, что наугад выбранное a будет удовлетворять условиям теоремы Поклингтона для данного примера, есть (1—1/67)≈0,985).

3 Процедура генерации простых чисел ГОСТ Р 34.10-94

В отечественном стандарте на цифровую подпись ГОСТ Р34.10-94 рекомендована процедура генерации доказуемо простых чисел заданного размера. ГОСТ Р 34.10-2001 также предписывает использование этой процедуры. Данная процедура основана на теореме Диемитко.

Теорема Диемитко

Пусть $n=qR+1$, где q – простое число, R – четное, $R<4(q+1)$.

Если найдется $a<n$: 1) $a^{n-1}\equiv 1 \pmod n$; 2) $a^{\frac{n-1}{q}} \not\equiv 1 \pmod n$, то n – простое число.

Итак, если имеем простое число q, то, перебирая четные числа R, строим числа $n=qR+1$ и испытываем их на простоту согласно теореме Диемитко, пока не получим простое число. По полученному числу можно построить еще одно простое число и т.д., пока не будет достигнут требуемый размер числа.

Приведем алгоритм перехода от меньшего простого числа q: $|q|=\left\lceil \frac{t}{2} \right\rceil$ к большему p: $|p|=t$, использующийся в ГОСТе. Фигурирующая в процедуре ξ есть равномерно распределенная на (0,1) случайная величина, получаемая с помощью линейного конгруэнтного генератора. Каждый раз на шаге 1 получают новое значение ξ.

Алгоритм перехода от меньшего простого числа к большему:

Вход: t – требуемая размерность простого числа, q – простое число : $|q|=\left\lceil \frac{t}{2} \right\rceil$

.

1. Вычисляем $N=\left\lceil \frac{2^{t-1}}{q} \right\rceil+\left\lceil \frac{2^{t-1}\xi}{q} \right\rceil$. Если N – нечетное, то N=N+1.

2. u=0.

3. Вычисляем $p=(N+u)q+1$ – кандидат в простые.

4. Если $p>2^t$, возвращаемся на шаг 1.

5. Если $2^{p-1}\equiv 1(\mathrm{mod}\ p)$ и $2^{N+u}\not\equiv 1(\mathrm{mod}\ p)$, то идем на Выход.

6. Вычисляем $u=u+2$. Возвращаемся на шаг 3.

Выход: p – простое число.

Первое слагаемое в построении числа N на шаге 1 обеспечивает минимальный требуемый размер числа p, а второе вносит в процедуру поиска новых простых чисел необходимый элемент случайности.

Проверка на шаге 4 необходима, чтобы число p не превышало своей верхней границы, а проверка на Шаге 5 есть проверка условия теоремы Диемитко при a=2.

Пример

Вход: $t=4$, $q=3=[11]_2$

1. $N=\left\lceil \frac{8}{3} \right\rceil+\left\lceil \frac{8\cdot 0{,}1}{3} \right\rceil=4$. 4 – четное число.

2. $u=0$.

3. $p=4\cdot 3+1=13$.

4. $13<2^4=16$.

5. $2^{12}\ \mathrm{mod}\ 13=1$, $2^4\ \mathrm{mod}\ 13 = 3$.

Выход. $p=13=[1011]_2$

Поскольку на Шаге 5 условие теоремы Диемитко проверяется не для всех $a<p$, а только для a=2, то некоторые простые числа, сгенерированных этим алгоритмом, не опознаются как простые. Но вероятность того, что для

простого числа n наугад выбранное число a будет удовлетворять условиям теоремы Диемитко, есть $(1—1/q)$, а q – достаточно большое число. Таким образом, проверки при a=2 вполне достаточно, чтобы не отсеивать слишком много простых чисел.

Расширенные данные представлены в Приложении.

Задания для самостоятельного решения:

1) Построить таблицу простых чисел, меньших 500, с помощью решета Эратосфена. С использованием этой таблицы:

а) реализовать процедуру получения простых чисел заданной длины на основе теста Миллера;

б) реализовать процедуру получения простых чисел заданной длины на основе теста Поклингтона;

в) реализовать процедуру генерации простых чисел заданной длины ГОСТ Р 34.10-94.

2) Построить 10 простых чисел с помощью полученной процедуры.

3) Каждое построенное число проверить на простоту вероятностным тестом, реализованным в задании к разделу 2. Количество итераций вероятностного теста должно быть таково, чтобы вероятность ошибки не превышала 0,1.

4) Каждое отвергнутое тестом из пункта 1 число проверить вероятностным тестом. Подсчитать k – количество отвергнутых чисел, определенных вероятностным тестом как простые.

5) Результат оформить в виде таблицы:

№	1	2	…	10
P	101		…	
Результат проверки вероятностным тестом	+	-	…	
K	2		…	

Здесь № - номер эксперимента, p – построенное простое число, в третьей строке результат проверки построенного числа вероятностным тестом (+ или -), k – количество отвергнутых чисел, определенных вероятностным тестом как простые.

Количество итераций вероятностного теста должно быть таково, чтобы вероятность ошибки не превышала 0,1.

Приложение А

Данные для проверки на простоту

Для тестов Миллера и Поклингтона

Требования к реализации:

1) реализованный тест следует проверить таблицей составных чисел. В качестве входных параметров реализованного теста следует подставить числа из колонки «Числа для проверки» если в результате тест выдаст сообщение о том, что данное число отвергается, то следует перейти к следующему этапу проверки. Если хотя бы одно из этих чисел опознается тестом как простое, то тест реализован с ошибками.

2) следует воспользоваться таблицами согласно реализованному тесту. Для проверки этими таблицами следует подставить в качестве входных параметров данные из таблиц (для теста Миллера проверяемое простое число p и каноническое разложение числа (p-1), для теста Поклингтона – проверяемое простое число p, число R и каноническое разложение числа F). Установить количество итераций теста t=1. Проверить число p этим тестом несколько раз (30-100). Затем рассчитать частоту события, когда проверяемое простое число будет принято за составное, и сравнить это значение с данными из колонки «Вероятность ошибки». Если эти данные приблизительно равны рассчитанному значению частоты, то тест реализован верно.

Для процедуры генерации чисел ГОСТ 31.10-94

Следует выставить параметр $\xi = 0$ (то есть избавиться от случайности). Затем следует подставить в качестве входных параметров данные из таблицы (q и t). Результат должен совпадать со значением из колонки «Построенное число».

Таблица составных чисел

Числа для проверки (p)	**Разложение p-1**	**Разложение F**	**R**	**Результат теста**
335	$2 \cdot 167$	167	2	

437	$2^2 \cdot 109$	109	4	**Всегда отвергаются**
657	$2^4 \cdot 41$	41	16	
779	$2 \cdot 389$	389	2	
1189	$2^2 \cdot 3^3 \cdot 11$	$3^3 \cdot 11$	4	
1191	$2 \cdot 5 \cdot 7 \cdot 17$	$7 \cdot 17$	10	
1533	$2^2 \cdot 383$	383	4	
1785	$2^3 \cdot 223$	223	8	
2071	$2 \cdot 3^2 \cdot 5 \cdot 23$	$5 \cdot 23$	18	
2327	$2 \cdot 1163$	1163	2	
2249	$2^3 \cdot 281$	281	8	
3057	$2^4 \cdot 191$	191	16	
3379	$2 \cdot 3 \cdot 563$	563	6	
3701	$2^2 \cdot 5^2 \cdot 37$	$2^2 \cdot 37$	25	
4009	$2^3 \cdot 3 \cdot 167$	167	24	
4647	$2 \cdot 23 \cdot 101$	101	46	
5007	$2 \cdot 2503$	2503	2	
5211	$2 \cdot 5 \cdot 521$	521	10	
8891	$2 \cdot 5 \cdot 7 \cdot 127$	127	70	
9451	$2 \cdot 3^3 \cdot 5^2 \cdot 7$	$5^2 \cdot 7$	54	
9837	$2^2 \cdot 2459$	2459	4	
9943	$2 \cdot 3 \cdot 1657$	1657	6	
6141	$2^2 \cdot 5 \cdot 307$	307	20	
6259	$2 \cdot 3 \cdot 7 \cdot 149$	149	42	
6951	$2 \cdot 5^2 \cdot 139$	139	50	
7157	$2^2 \cdot 1789$	1789	4	
7483	$2 \cdot 3 \cdot 29 \cdot 43$	$29 \cdot 43$	6	

Таблица простых чисел для теста Миллера

Простое число *p*	**Разложение (*p*-1)**	**Вероятность ошибки**
13	$2^2 \cdot 3$	0,66666
29	$2^2 \cdot 7$	0,57142
61	$2^2 \cdot 3 \cdot 5$	0,73333
97	$2^5 \cdot 3$	0,66666
157	$2^3 \cdot 13$	0,53846
173	$2^2 \cdot 43$	0,51162
179	$2 \cdot 89$	0,02325
353	$2^5 \cdot 11$	0,54545
419	$2 \cdot 11 \cdot 19$	0,56937
461	$2^2 \cdot 5 \cdot 23$	0,61739
617	$2^3 \cdot 7 \cdot 11$	0,61038
821	$2^2 \cdot 5 \cdot 41$	0,60975
1069	$2^2 \cdot 3 \cdot 89$	0,67041
5953	$2^6 \cdot 3 \cdot 31$	0,67741
6121	$2^3 \cdot 3^2 \cdot 5 \cdot 17$	0,74901
6197	$2^2 \cdot 1549$	0,5
6373	$2^2 \cdot 3^3 \cdot 59$	0,67231

Таблица простых чисел для теста Поклингтона

Простое число *p*	**Разложение F**	**R**	**Вероятность ошибки**
13	2^2	3	0,5
29	7	4	0,14285
61	$3 \cdot 5$	4	0,46666
97	$3 \cdot 2^2$	8	0,66666
157	13	8	0,125
173	43	4	0,02325
179	89	2	0,01123
353	$2 \cdot 11$	16	0,54545
419	$11 \cdot 19$	2	0,13875
461	23	20	0,04347
617	$7 \cdot 11$	8	0,09604
821	41	20	0,02439
1069	89	12	0,01123
5953	$3 \cdot 31$	64	0,35483
6121	$5 \cdot 17$	72	0,24705
6197	1549	4	0,00064
6373	$3 \cdot 59$	36	0,33333

Данные для ГОСТ 31.10-94 при ξ=0

q	t	**Построенное число p**
3	4	13
5	6	41
7	5	29
5	5	31
11	7	67
11	8	199
13	7	79
13	8	131
17	9	307
17	10	613
19	9	419
23	9	277
29	9	349
31	9	311
37	11	2221
41	11	2297
19	10	571
23	10	599

Приложение Б. Таблица простых чисел

Таблица Б.1 − Таблица простых чисел, не превосходящих 6000

2	167	389	631	883	1153	1447	1709	2011	2309	2621
3	173	397	641	887	1163	1451	1721	2017	2311	2633
5	179	401	643	907	1171	1453	1723	2027	2333	2647
7	181	409	647	911	1181	1459	1733	2029	2339	2657
11	191	419	653	919	1187	1471	1741	2039	2341	2659
13	193	421	659	929	1193	1481	1747	2053	2347	2663
17	197	431	661	937	1201	1483	1753	2063	2351	2671
19	199	433	673	941	1213	1487	1759	2069	2357	2677
23	211	439	677	947	1217	1489	1777	2081	2371	2683
29	223	443	683	953	1223	1493	1783	2083	2377	2687
31	227	449	691	967	1229	1499	1787	2087	2381	2689
37	229	457	701	971	1231	1511	1789	2089	2383	2693
41	233	461	709	977	1237	1523	1801	2099	2389	2699
43	239	463	719	983	1249	1531	1811	2111	2393	2707
47	241	467	727	991	1259	1543	1823	2113	2399	2711
53	251	479	733	997	1277	1549	1831	2129	2411	2713
59	257	487	739	1009	1279	1553	1847	2131	2417	2719
61	263	491	743	1013	1283	1559	1861	2137	2423	2729
67	269	499	751	1019	1289	1567	1867	2141	2437	2731
71	271	503	757	1021	1291	1571	1871	2143	2441	2741
73	277	509	761	1031	1297	1579	1873	2153	2447	2749
79	281	521	769	1033	1301	1583	1877	2161	2459	2753
83	283	523	773	1039	1303	1597	1879	2179	2467	2767
89	293	541	787	1049	1307	1601	1889	2203	2473	2777
97	307	547	797	1051	1319	1607	1901	2207	2477	2789
101	311	557	809	1061	1321	1609	1907	2213	2503	2791
103	313	563	811	1063	1327	1613	1913	2221	2521	2797
107	317	569	821	1069	1361	1619	1931	2237	2531	2801
109	331	571	823	1087	1367	1621	1933	2239	2539	2803
113	337	577	827	1091	1373	1627	1949	2243	2543	2819
127	347	587	829	1093	1381	1637	1951	2251	2549	2833
131	349	593	839	1097	1399	1657	1973	2267	2551	2837
137	353	599	853	1103	1409	1663	1979	2269	2557	2843
139	359	601	857	1109	1423	1667	1987	2273	2579	2851
149	367	607	859	1117	1427	1669	1993	2281	2591	2857
151	373	613	863	1123	1429	1693	1997	2287	2593	2861
157	379	617	877	1129	1433	1697	1999	2293	2609	2879
163	383	619	881	1151	1439	1699	2003	2297	2617	2887

2897	3221	3529	3821	4127	4447	4751	5051	5399	5683
2903	3229	3533	3823	4129	4451	4759	5059	5407	5689
2909	3251	3539	3833	4133	4457	4783	5077	5413	5693
2917	3253	3541	3847	4139	4463	4787	5081	5417	5701
2927	3257	3547	3851	4153	4481	4789	5087	5419	5711
2939	3259	3557	3853	4157	4483	4793	5099	5431	5717
3001	3323	3613	3917	4229	4547	4871	5167	5479	5791
3011	3329	3617	3919	4231	4549	4877	5171	5483	5801
3019	3331	3623	3923	4241	4561	4889	5179	5501	5807
3023	3343	3631	3929	4243	4567	4903	5189	5503	5813
3037	3347	3637	3931	4253	4583	4909	5197	5507	5821
3041	3359	3643	3943	4259	4591	4919	5209	5519	5827
3049	3361	3659	3947	4261	4597	4931	5227	5521	5839
3061	3371	3671	3967	4271	4603	4933	5231	5527	5843
3067	3373	3673	3989	4273	4621	4937	5233	5531	5849
3079	3389	3677	4001	4283	4637	4943	5237	5557	5851
3083	3391	3691	4003	4289	4639	4951	5261	5563	5857
3089	3407	3697	4007	4297	4643	4957	5273	5569	5861
3109	3413	3701	4013	4327	4649	4967	5279	5573	5867
3119	3433	3709	4019	4337	4651	4969	5281	5581	5869
3121	3449	3719	4021	4339	4657	4973	5297	5591	5879
3137	3457	3727	4027	4349	4663	4987	5303	5623	5881
3163	3461	3733	4049	4357	4673	4993	5309	5639	5897
3167	3463	3739	4051	4363	4679	4999	5323	5641	5903
3169	3467	3761	4057	4373	4691	5003	5333	5647	5923
3181	3469	3767	4073	4391	4703	5009	5347	5651	5927
3187	3491	3769	4079	4397	4721	5011	5351	5653	5939
3191	3499	3779	4091	4409	4723	5021	5381	5657	5953
3203	3511	3793	4093	4421	4729	5023	6387	5659	5981
3209	3517	3797	4099	4423	4733	5039	5393	5669	5987
3217	3527	3803	4111	4441					