Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА-Российский технологический университет»

РТУ МИРЭА

Кафедра КБ-1 «Защита информации»

ПРАКТИЧЕСКАЯ РАБОТА № 6

по дисциплине «Криптографические методы защиты информации»

Тайные многосторонние вычисления и разделение секрета

РТУ МИРЭА – 2020 г.

Протокол конфиденциального вычисления (также безопасное, защищенное или тайное многостороннее вычисление) — криптографический протокол, позволяющий нескольким участникам произвести вычисление, зависящее от тайных входных данных каждого из них, таким образом, чтобы ни один участник не смог получить никакой информации о чужих тайных входных данных. Впервые задача конфиденциального вычисления была поднята Эндрю Яо в 1982 году в статье «Protocols for Secure Computations». Два миллионера, Алиса и Боб, хотят выяснить, кто же из них богаче, при этом они не хотят разглашать точную сумму своего благосостояния. Яо предложил в своей статье оригинальный способ решения этой задачи, получившей впоследствии название проблема миллионеров. Гораздо позже, в 2004 году Йехуда Линделл и Бенни Пинкас предоставили математически строгое доказательство корректности протокола Яо в статье «A Proof of Yao's Protocol for Secure Two-Party Computation». Задача конфиденциального вычисления тесно связана с задачей разделения секрета.

Задача, решаемая с помощью тайных многосторонних вычислений состоит в следующим: в конфиденциальном вычислении участвуют N участников p_1, p_2, …, p_N. У каждого участника есть тайные входные данные d_1, d_2, …, d_N соответственно. Участники хотят найти значение $F(d_1, d_2, …, d_N)$, где F — известная всем участникам вычислимая функция от N аргументов. Допускается, что среди участников будут получестные нарушители, то есть те, которые верно следуют протоколу, но пытаются получить дополнительную информацию из любых промежуточных данных.

К безопасности протоколов конфиденциального вычисления обычно предъявляются различные требования в зависимости от ситуации. Приведём основные требования.

- Конфиденциальность. Никто из участников не должен иметь возможности получить больше информации, чем им предписано.
- Корректность. Каждый участник должен гарантировано получить верные данные.
- Гарантия получения информации. У участников не должно быть возможности помешать другим участников получить выходные данные.

Практическое применение протоколов конфиденциального вычисления:

- Электронное голосование. Например, каждый участник может проголосовать за или против, тогда результатом голосования n участников будет функция $F(x_1, …,x_n)$, где x_i может принимать значения 0 (против) и 1 (за).
- Электронные аукционы. Каждый участник предлагает цену x_i, и функция $F(x_1, …,x_n)$ возвращает номер максимального x_i.
- Статистика. Допустим, студенты хотят узнать лучшую или среднюю оценку, не показывая оценки друг другу.
- Базы данных. Например, пусть пользователь хочет выполнить запрос к базе данных и получить ответ, не раскрывая запроса. Владелец сервера с базой данных хочет, чтобы при запросах никакая информация, кроме ответа на запрос, не попадала к пользователю. В этом случае участниками протокола конфиденциального вычисления будет как пользователь, так и сервер.
- Распределённый центр сертификации. Допустим нужно создать центр сертификации, который будет выдавать сертификаты пользователям, подписывая их каким-нибудь секретным ключом. Для защиты ключа ключ можно поделить между несколькими серверами таким образом, чтобы каждый сервер хранил свою часть ключа. Тогда возникнет проблема: как выполнить криптографическую операцию (в данном примере выдачу подписи), не передавая все части ключа на один компьютер.

Эта проблема решается с помощью протокола конфиденциального вычисления, где входными данными для функции конфиденциального вычисления являются части ключа и подписываемое сообщение, а выходные данные представляют собой подписанное сообщение.

Пример протокола.

Задача – определение средней заработной платы трех сотрудников: Директора (Д), Секретаря (С) и Уборщицы (У). Заработная плата, которую сотрудники не хотят раскрывать друг другу:

- Директор – 10 у.е.;

- Секретарь – 5 у.е.;

- Уборщица – 2 у.е.

Пары ключей асимметричного шифрования (RSA) для обмена информацией между собой:

- Директор: открытый ключ – $e_Д = 5$ и $n_Д = 91$; закрытый ключ - $d_Д = 29$;

- Секретарь: открытый ключ – $e_С = 7$ и $n_С = 91$; закрытый ключ - $d_С = 31$;

- Уборщица: открытый ключ – $e_У = 17$ и $n_У = 91$; закрытый ключ - $d_У = 17$.

В рассмотренном примере подбор ключей некорректен, т.к. выбор простых чисел для определения модуля должен выполняться каждым индивидуально. Данное упрощение принято в целях рассмотрения работы протокола.

Таблица 1. Протокол тайных многосторонних вычислений

№ п/п	Описание операции	Пример
1	**У** прибавляет случайное секретное число **x** к сумме своей зарплаты, шифрует результат с помощью открытого ключа **С** и отсылает его **С**.	x = 3 $(2 + 3)^7 \bmod 91 = 47$
2	**С** расшифровывает результат, добавляет к нему свою зарплату, шифрует результат с помощью открытого ключа **Д** и отсылает его **Д**.	$47^{31} \bmod 91 = 5$ $(5 + 5)^5 \bmod 91 = 82$
3	**Д** расшифровывает результат, добавляет к нему свою зарплату, шифрует результат с помощью открытого ключа **У** и отсылает его **У**.	$82^{29} \bmod 91 = 10$ $(10 + 10)^{17} \bmod 91 = 76$
4	**У** расшифровывает результат, отнимает **x** и объявляет среднюю зарплату.	$76^{17} \bmod 91 = 20$ СЗ = (20 - 3)/3 = 5.(6)

В данной схеме поочередное шифрование/дешифрование необходимо для предотвращения вычисления мошенником информации, которой владеют участники протокола. Если пересылаемую информацию не шифровать, то мошенник, зная функцию преобразования и перехватив информацию, направленную одному из участников и высланную им следующему, может легко вычислить скрываемые исходные данные. Например, противник или недобросовестный участник протокола, перехватив информацию, высланную уборщицей секретарю (5) и секретарем директору (10), определит зарплату секретаря 10 – 5 = 5 у.е. Шифрование предотвращает подобную атаку.

Разделение секрета - термин в криптографии, под которым понимают любой из способов распределения секрета среди группы участников, каждому из которых достаётся своя некая доля. Секрет может воссоздать только коалиция участников из первоначальной группы, причём входить в коалицию должно не менее некоторого изначально известного их числа.

Схемы разделения секрета применяются в случаях, когда существует значимая вероятность компрометации одного или нескольких хранителей секрета, но вероятность недобросовестного сговора значительной части участников считается пренебрежимо малой.

Существующие схемы имеют две составляющие: разделение и восстановление секрета. К разделению относится формирование частей секрета и распределение их между членами группы, что позволяет разделить ответственность за секрет между её участниками. Обратная схема должна обеспечить его восстановление при условии доступности его хранителей в некотором необходимом количестве.

Пример использования: протокол тайного голосования на основе разделения секрета.

Сущность данных протоколов заключается в том, что владелец секрета распределяет его части (доли) между несколькими людьми (субъектами). Каждая часть сама по себе ничего не значит и не дает информации о секрете. Для восстановления секрета требуется собрать все или определенное количество его долей. В первом случае говорят о разбиении (англ. splitting), а во втором о разделении (англ. sharing) секрета.

Второе отличие протоколов разбиения от протоколов разделения заключается в распределении долей. При разбиении разные доли передаются разным людям, при разделении – один человек может владеть сразу несколькими долями.

Разбиения секрета с использование гаммирования.

Простую и в то же время эффективную схему разбиения секрета можно построить на базе гаммирования по модулю 2. В этом случае секрет вначале кодируется в двоичном виде. Для его разбиения владелец генерирует несколько битовых строк (гамм), которые отдельно передает каждому из участников протокола. Кроме этого он складывает по модулю 2 битовое представление секрета со всеми гаммами и результат (шифрограмму) выкладывает в доступное для участников место. Для восстановления секрета необходимо сложить шифрограмму со всеми выданными гаммами, при чем не важно, в каком порядке.

В следующей таблице представлен пример разбиения секрета между тремя участниками.

Таблица 2. Протокол разбиения секрета на трех участников

<table>
<tr><th>№ п/п</th><th>Описание операции</th><th colspan="5">Пример</th></tr>
<tr><td rowspan="2">1</td><td rowspan="2">Кодирование секрета – слово «КОД».</td><td rowspan="2">Секрет</td><td>Буква</td><td>К</td><td>О</td><td>Д</td></tr>
<tr><td>Bin-код</td><td>1100 1010</td><td>1100 1110</td><td>1100 0100</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">Генерация случайных гамм и передача их участникам.</td><td rowspan="2">Гамма$_1$</td><td>Буква</td><td>Ю</td><td>Л</td><td>Я</td></tr>
<tr><td>Bin-код</td><td>1101 1110</td><td>1100 1011</td><td>1101 1111</td></tr>
</table>

<table>
<tr><td rowspan="4"></td><td rowspan="4"></td><td rowspan="2">Гамма$_2$</td><td>Буква</td><td>Ш</td><td>А</td><td>Р</td></tr>
<tr><td>Bin-код</td><td>1101
1000</td><td>1100
0000</td><td>1101
0000</td></tr>
<tr><td rowspan="2">Гамма$_3$</td><td>Буква</td><td>С</td><td>У</td><td>К</td></tr>
<tr><td>Bin-код</td><td>1101
0001</td><td>1101
0011</td><td>1100
1010</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">Получение шифрограммы и выкладывание её в доступное для участников место.</td><td>Секрет
Гамма$_1$
Гамма$_2$
Гамма$_3$</td><td>$\oplus$</td><td>1100
1010
1101
1110
1101
1000
1101
0001</td><td>1100
1110
1100
1011
1100
0000
1101
0011</td><td>1100
0100
1101
1111
1101
0000
1100
1010</td></tr>
<tr><td>Шифрограмма</td><td>Bin-код</td><td>0001
1101</td><td>0001
0110</td><td>0000
0001</td></tr>
<tr><td rowspan="3">4</td><td rowspan="3">Восстановление секрета.</td><td>Шифрограмма
Гамма$_2$
Гамма$_1$
Гамма$_3$</td><td>$\oplus$</td><td>0001
1101
1101
1000
1101
1110
1101
0001</td><td>0001
0110
1100
0000
1100
1011
1101
0011</td><td>0000
0001
1101
0000
1101
1111
1100
1010</td></tr>
<tr><td rowspan="2">Секрет</td><td>Bin-код</td><td>1100
1010</td><td>1100
1110</td><td>1100
0100</td></tr>
<tr><td>Буква</td><td>К</td><td>О</td><td>Д</td></tr>
</table>

Примечание. Бинарное представление символов в соответствии с кодировкой Windows 1251.

Для восстановления секрета участники протокола, которым выданы гаммы, должны собраться вместе и в любой последовательности сложить свои гаммы с шифрограммой. В том случае, если гаммирование выполняется поочередно и обмен информации между участниками выполняется по открытым каналам связи (например, первый участник складывает шифрограмму со своей гаммой и отсылает результат второму, второй складывает полученный результат со своей гаммой и отсылает третьему и т.д.), то пересылаемую между ними информацию необходимо шифровать, как при тайных многосторонних вычислениях. В противном случае мошенник может определить гаммы участников протокола.

В общем случае, в основе протокола разбиения секрета лежит шифрование с разными ключами (например, как в рассмотренном примере или тройном DES) или последовательное применение разных методов шифрования (например, как в комбинированных шифрах).

Разделения секрета по схеме Шамира.

В отличие от разбиения секрета участнику (субъекту) может передаваться сразу несколько равных долей и для восстановления секрета необязательно иметь все доли. Например, код запуска баллистической ракеты разбивается на пять долей, которые передаются трем полковникам (по одной доле) и одному генералу (две доли). Если для восстановления кода запуска (секрета) необходимо собрать три доли, то это могут сделать три полковника или генерал с одним полковником. Такая схема, где секрет делится на n долей, а для его восстановления необходимо собрать не менее чем m долей, где m < n, называется (m, n)–пороговой схемой.

В 1979 г. Ади Шамир (один из авторов RSA) предложил протокол разделения секрета с использованием полиномов (многочленов), максимальная степень которых равна m-1. Для восстановления секрета используются формулы интерполяционного полинома Лагранжа.

Интерполяционный полином Лагранжа.

Пусть имеется некоторая исходная функция f(x), с помощью которой определены m точек – пар (xi, yi). Тогда можно подобрать полином степени m-1, который будет проходить через все точки и максимально близко описывать исходную функцию.

Интерполяционный полином L(x) определяется формулой

$$f(x) \approx L(x) = a_{m-1}x^{m-1} + \ a_{m-2}x^{m-2} + \cdots + a_2x^2 + a_1x + a_0 = \sum_{i=0}^{m-1} y_i l_i(x)$$

где a_i - коэффициенты интерполяционного полинома Лагранжа;
y_i - значения исходной функции в i-ой точке;
$l_i(x)$ - базисные полиномы, определяемые по формуле

$$l_i(x) = \prod_{j=0,\, j\neq i}^{m-1} \frac{x - x_j}{x_i - x_j}$$

где x_i, x_j - значения аргумента функции в i-ой и j-ой точках.

Пример подбора интерполяционного полинома Лагранжа.

Исходная функция f(x) = Sin(x^2).

Точки исходной функции:

x_0 = -2, f(x_0) = -0.7568;
x_1 = -1, f(x_1) = -0.8415;
x_2 = 0, f(x_2) = 0;
x_3 = 1, f(x_3) = 0.8415;
x_4 = 2, f(x_4) = 0.7568.

Определение базисных полиномов:

$$l_0(x) = \prod_{j=1}^{4} \frac{x - x_j}{x_0 - x_j} = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} \cdot \frac{x - x_3}{x_0 - x_3} \cdot \frac{x - x_4}{x_0 - x_4} = \frac{x + 1}{-2 + 1} \cdot \frac{x - 0}{-2 - 0} \cdot \frac{x - 1}{-2 - 1} \cdot \frac{x - 2}{-2 - 2} = \frac{x + 1}{-1} \cdot \frac{x}{-2} \cdot \frac{x - 1}{-3} \cdot \frac{x - 2}{-4} = \frac{1}{24} \cdot (x^4 - 2x^3 - x^2 + 2x)$$

$$l_1(x) = \prod_{j=0, j\neq 1}^{4} \frac{x - x_j}{x_1 - x_j} = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} \cdot \frac{x - x_3}{x_1 - x_3} \cdot \frac{x - x_4}{x_1 - x_4} = \frac{x + 2}{-1 + 2} \cdot \frac{x - 0}{-1 - 0} \cdot \frac{x - 1}{-1 - 1} \cdot \frac{x - 2}{-1 - 2} = \frac{x + 2}{1} \cdot \frac{x}{-1} \cdot \frac{x - 1}{-2} \cdot \frac{x - 2}{-3} = \frac{1}{-6} \cdot (x^4 - x^3 - 4x^2 + 4x)$$

$$l_2(x) = \prod_{j=0, j\neq 2}^{4} \frac{x - x_j}{x_2 - x_j} = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} \cdot \frac{x - x_3}{x_2 - x_3} \cdot \frac{x - x_4}{x_2 - x_4} = \frac{x + 2}{0 + 2} \cdot \frac{x + 1}{0 + 1} \cdot \frac{x - 1}{0 - 1} \cdot \frac{x - 2}{0 - 2} = \frac{x + 2}{2} \cdot \frac{x + 1}{1} \cdot \frac{x - 1}{-1} \cdot \frac{x - 2}{-2} = \frac{1}{-4} \cdot (x^4 - 5x^2 + 4)$$

$$l_3(x) = \prod_{j=0, j\neq 3}^{4} \frac{x - x_j}{x_3 - x_j} = \frac{x - x_0}{x_3 - x_0} \cdot \frac{x - x_1}{x_3 - x_1} \cdot \frac{x - x_2}{x_3 - x_2} \cdot \frac{x - x_4}{x_3 - x_4} = \frac{x + 2}{1 + 2} \cdot \frac{x + 1}{1 + 1} \cdot \frac{x - 0}{1 - 0} \cdot \frac{x - 2}{1 - 2} = \frac{x + 2}{3} \cdot \frac{x + 1}{2} \cdot \frac{x}{1} \cdot \frac{x - 2}{-1} = \frac{1}{-6} \cdot (x^4 + x^3 - 4x^2 - 4x)$$

$$l_4(x) = \prod_{j=0}^{3} \frac{x - x_j}{x_4 - x_j} = \frac{x - x_0}{x_4 - x_0} \cdot \frac{x - x_1}{x_4 - x_1} \cdot \frac{x - x_2}{x_4 - x_2} \cdot \frac{x - x_3}{x_4 - x_3} = \frac{x + 2}{2 + 2} \cdot \frac{x + 1}{2 + 1} \cdot \frac{x - 0}{2 - 0} \cdot \frac{x - 1}{2 - 1} = \frac{x + 2}{4} \cdot \frac{x + 1}{3} \cdot \frac{x}{2} \cdot \frac{x - 1}{1} = \frac{1}{24} \cdot (x^4 + 2x^3 - x^2 - 2x)$$

Определение интерполяционного полинома Лагранжа:

$$L(x) = \sum_{i=0}^{m-1} y_i l_i(x) = \frac{y_0}{24} \cdot (x^4 - 2x^3 - x^2 + 2x) + \frac{y_1}{-6} \cdot (x^4 - x^3 - 4x^2 + 4x) + \frac{y_2}{-4} \cdot (x^4 - 5x^2 + 4) + \frac{y_3}{-6} \cdot (x^4 + x^3 - 4x^2 - 4x) + \frac{y_4}{24} \cdot (x^4 + 2x^3 - x^2 - 2x) =$$
$$\frac{-0.7568}{24} \cdot (x^4 - 2x^3 - x^2 + 2x) + \frac{0.8415}{-6} \cdot (x^4 - x^3 - 4x^2 + 4x) + \frac{0}{-4} \cdot (x^4 - 5x^2 + 4) + \frac{0.8415}{-6} \cdot (x^4 + x^3 - 4x^2 - 4x) + \frac{-0.7568}{24} \cdot (x^4 + 2x^3 - x^2 - 2x) = -0.3436x^4 + 1.1851x^2$$

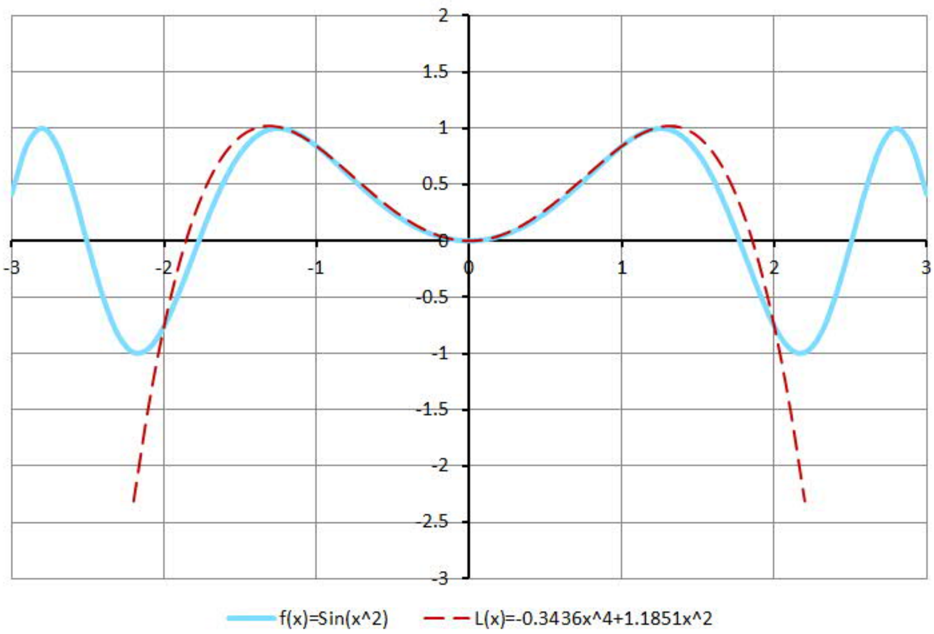

Рис.1. Графики исходной функции и интерполяционного полинома

Как видно на рисунке, интерполяционный полином довольно хорошо аппроксимирует исходную функцию в диапазоне x ∈ [-2; 2].

Протокол разделения секрета на основе интерполяционных полиномов Лагранжа.

Для разделения секрета S, восстанавливаемого с помощью m долей, используется полином степени m-1 по модулю p

$$f(x) = L(x) = (a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_2x^2 + a_1x + S)\ mod\ p$$

где f(x) = L(x) - исходная функция и интерполяционный полином Лагранжа;
a_i - целочисленные коэффициенты полинома;
$S = a_0$ - разделяемый секрет, закодированный в виде числа;
p - простое число.

Коэффициенты полинома a_i выбираются произвольно, за исключением $a_0 = S$. Модуль p должен быть простым числом, большим секрета S и общего количества долей n. Владелец секрета для $x_i = 1..n$ определяет значения полинома $y_i = f(x_i)$ и передает пары (x_i, y_i) участникам согласно определенному для каждого количеству долей. Для восстановления секрета необходимо собрать m долей (пар (x_i, y_i)) и найти значения коэффициентов интерполяционного полинома, включая секрет $S = a_0$.

Т.к. исходная функция и интерполяционный полином выражаются одинаковой формулой, то определенные по известным точкам (долям) коэффициенты интерполяционного полинома совпадут с коэффициентами исходной функции.

Пример протокола (по схеме Шамира).

Секрет S = 11. Количество долей, необходимых для восстановления секрета, m = 3. Общее количество долей n = 5.

Таблица 3. Процедура определения и распределения долей (выполняет владелец)

№ п/п	Описание операции	Пример
1	Выбор простого числа **p**, которое больше количества долей **n** и секрета **S**.	p = 59
2	Выбор произвольного многочлена степени **m-1** : **f(x)** = $(a_2x^2 + a_1x + S)$ mod p, где значения $\mathbf{a_2}$ и $\mathbf{a_1}$ выбираются случайным образом, хранятся в тайне и отбрасываются после распределения долей.	$a_2 = 10$, $a_1 = 23$ $f(x) = (10x^2 + 23x + 11)$ mod 59
3	Определение долей $(\mathbf{x_i}, \mathbf{y_i})$, где $\mathbf{y_i} = f(x_i)$ и $\mathbf{x_i} = i + 1$.	$y_0 = (10*1^2 + 23*1 + 11)$ mod 59 = 44 $y_1 = (10*2^2 + 23*2 + 11)$ mod 59 = 38 $y_2 = (10*3^2 + 23*3 + 11)$ mod 59 = 52 $y_3 = (10*4^2 + 23*4 + 11)$ mod 59 = 27 $y_4 = (10*5^2 + 23*5 + 11)$ mod 59 = 22

4	Публикация **p** и распределение долей (**x_i**, **y_i**) между участниками.	p = 59 $(x_0, y_0) = (1, 44)$ $(x_1, y_1) = (2, 38)$ $(x_2, y_2) = (3, 52)$ $(x_3, y_3) = (4, 27)$ $(x_4, y_4) = (5, 22)$

Таблица 4. Процедура восстановления секрета (выполняют участники)

№ п/п	Описание операции	Пример
1	Сбор **m** долей.	$(x_1, y_1) = (2, 38)$ $(x_2, y_2) = (3, 52)$ $(x_4, y_4) = (5, 22)$
2	Определение базисных полиномов.	$l_1(x) = \frac{x-3}{2-3} \cdot \frac{x-5}{2-5} = \frac{x-3}{-1} \cdot \frac{x-5}{-3} = \frac{1}{3} \cdot (x^2 - 8x + 15)$ $l_2(x) = \frac{x-2}{3-2} \cdot \frac{x-5}{3-5} = \frac{x-2}{1} \cdot \frac{x-5}{-2} = \frac{1}{-2} \cdot (x^2 - 7x + 10)$ $l_4(x) = \frac{x-2}{5-2} \cdot \frac{x-3}{5-3} = \frac{x-2}{3} \cdot \frac{x-3}{2} = \frac{1}{6} \cdot (x^2 - 5x + 6)$
3	Определение интерполяционного полинома Лагранжа.	$L(x) = \left[\frac{38}{3} \cdot (x^2 - 8x + 15) + \frac{52}{-2} \cdot (x^2 - 7x + 10) + \frac{22}{6} \cdot (x^2 - 5x + 6)\right]$ $L(x) = \left[\frac{76}{6} \cdot (x^2 - 8x + 15) - \frac{156}{6} \cdot (x^2 - 7x + 10) + \frac{22}{6} \cdot (x^2 - 5x + 6)\right]$ $L(x) = \left[\frac{1}{6} \cdot (-58x^2 + 374x - 288)\right] \mathit{mod}\ 59$
4	Определение обратного числа по модулю **b^{-1}** для дробного множителя полинома **1 / b**.	$\frac{1}{b} = \frac{1}{6}$ $b^{-1} = 10$ [(6 * 10) mod 59 = 1]
5	Замена дробного множителя **1 / b** и умножение коэффициентов полинома на множитель **b^{-1}**.	$L(x) = [10 * (-58x^2 + 374x – 288)] \bmod 59 = (-580x^2 + 3740x – 2880) \bmod 59$
6	Приведение коэффициентов полинома и определение секрета **S**.	$a_2 = -580 \bmod 59 = -49 \bmod 59 = 10$ $a_1 = 3740 \bmod 59 = 23$ $S = a_0 = -2880 \bmod 59 = -48 \bmod 59 = 11$ $L(x) = (10x^2 + 23x + 11) \bmod 59$

Примечание. Обратное число по модулю определяется из выражения ($b * b^{-1}$) mod p = 1 (например, с помощью расширенного алгоритма Евклида).

Разделения секрета по схеме Асмута-Блума.

В (m, n)-пороговой схеме Асмута-Блума для распределения долей используются простые (натуральное число, большее единицы и не имеющее других натуральных делителей, кроме самого себя и единицы) и взаимно простые числа (числа, не имеющие общих делителей, кроме 1, т.е. наибольший общий делитель которых равен 1), а для восстановления - китайская теорема об остатках.

Схема и пример протокола.

Секрет S = 11. Количество долей, необходимых для восстановления секрета, m = 3. Общее количество долей n = 5.

Таблица 5. Процедура определения и распределения долей (выполняет владелец)

№ п/п	Описание операции	Пример
1	Выбор простого числа **p**, которое больше секрета **S**.	p = 13
2	Выбор **n** взаимно простых чисел $\mathbf{d_i}$, удовлетворяющих условиям: - $d_i > p$; - $d_i < d_{i+1}$; - $d_1 * d_2 * \ldots * d_m < p * d_{n-m+2} * d_{n-m+3} * \ldots * d_n$.	$d_i \in \{17, 20, 23, 29, 37\}$ 17 * 20 * 23 < 13 * 29 * 37 7820 < 13949
3	Выбор произвольного числа **r**, удовлетворяющего условию $r < \frac{\prod_{i=1}^{m} d_i - S}{p}$. Вычисление **S’** = S + r p.	r = 30 $\left[30 < 600.7 = \frac{17 \cdot 20 \cdot 23 - 11}{13}\right]$ S’ = 11 + 30 * 13 = 401
4	Определение долей ($\mathbf{d_i}$, $\mathbf{k_i}$), где $\mathbf{k_i}$ = S’ mod d_i.	k_1 = 401 mod 17 = 10 k_2 = 401 mod 20 = 1 k_3 = 401 mod 23 = 10 k_4 = 401 mod 29 = 24 k_5 = 401 mod 37 = 31
5	Публикация **p** и распределение долей ($\mathbf{d_i}$, $\mathbf{k_i}$) между участниками.	p = 13 (d_1, k_1) = (17, 10) (d_2, k_2) = (20, 1) (d_3, k_3) = (23, 10) (d_4, k_4) = (29, 24) (d_5, k_5) = (37, 31)

Сущность **китайской теоремы об остатках** заключается в определении некоторого числа S’ по набору его остатков k_i от деления на некоторые заданные взаимно простые числа d_i.

$$\begin{cases} S' \, mod \, d_1 = k_1 \\ S' \, mod \, d_2 = k_2 \\ \ldots \\ S' \, mod \, d_m = k_m \end{cases}.$$

Например, для трех пар (d_i, k_i) – (3, 1), (5, 3) и (8, 3) – таким числом является S' = 43.

$$\begin{cases} 43 \; mod \; 3 = 1 \\ 43 \; mod \; 5 = 3 \\ 43 \; mod \; 8 = 3 \end{cases}.$$

В следующей таблице, наряду с процедурой восстановления секрета, приведен алгоритм определения числа S' (китайской теоремы об остатках) в пп. 2-5.

Таблица 6. Процедура восстановления секрета (выполняют участники)

№ п/п	Описание операции	Пример
1	Сбор **m** долей.	(d_2, k_2) = (20, 1) (d_3, k_3) = (23, 10) (d_5, k_5) = (37, 31)
2	Вычисление произведения **D** взаимно простых чисел $\mathbf{d_j}$.	D = 20 * 23 * 37 = 17020
3	Вычисление сомножителей $\mathbf{D_j}$ = D / d_j.	D_1 = 17020 / 20 = 851 D_2 = 17020 / 23 = 740 D_3 = 17020 / 37 = 460
4	Определение обратных чисел $\mathbf{D_j^{-1}}$ по модулям $\mathbf{d_j}$.	D_1^{-1} = 11 [(851 * 11) mod 20 = 1] D_2^{-1} = 6 [(740 * 6) mod 23 = 1] D_3^{-1} = 7 [(460 * 7) mod 37 = 1]
5	Вычисление **S'** = (Σ k_j D_j D_j^{-1}) mod D.	S' = (1*851*11 + 10*740*6 + 31*460*7) mod 17020 = 153581 mod 17020 = 401
6	Определение секрета **S** = S' mod p.	S = 401 mod 13 = 11

*Примечание. Обратное число по модулю определяется из выражения (b * b-1) mod p = 1 (например, с помощью расширенного алгоритма Евклида).*

Кроме классической пороговой схемы разделения секрета (владелец раздает доли и при восстановлении участники раскрывают свои доли) существуют и другие схемы.

1. Разделение секрета без владельца. Участники могут создать секрет и разделить его на доли так, что никто из них не узнает секрета, пока они совместно его не восстановят.

2. Разделение секрета без раскрытия долей при восстановлении. В этом смысле протокол представляет собой нечто среднее между разделением секрета и тайными многосторонними вычислениями.

3. Разделение секрета с возможностью проверки корректности отдельных долей. Каждый из участников независимо от других может проверить корректность своей доли без восстановления секрета.

4. Разделение секрета с возможностью блокирования восстановления секрета. Каждый из участников получает две доли: «да» и «нет». Если при восстановлении секрета число долей «нет» превышает некоторое пороговое значение, то его восстановление невозможно, даже, если количества долей «да» достаточно.

5. Разделение секрета с возможностью блокирования долей. Если после распределения долей, некоторые из участников теряют доверие, то можно блокировать их доли.

6. Разделение секрета с возможностью выявления фальшивых долей. При восстановлении секрета возможно выявление участников, предоставивших фальшивые доли.

7. Групповое разделение секрета. Секрет распределяется среди участников, объединенных в k групп. Для восстановления секрета необходимо собрать в каждой группе определенное количество долей. Т.е. имеет место ((m1, n1), (m2, n2), ..., (mk, nk))-пороговая схема.

Задание на практическую работу.

Составить отчет о проделанной практической работе. В отчете **должны** содержаться **выполненные задания**, указанные ниже.

1) Ответить на контрольные вопросы

1. Для чего необходимо применение шифрования с открытым ключом в тайных многосторонних вычислениях?

2. Что означает (m, n) - пороговая схема разделения секрета.

3. Назначение интерполяционного полинома Лагранжа.

4. Сущность китайской теоремы об остатках.

2) Привести последовательность выполнения следующих протоколов:

- **тайных многосторонних вычислений для расчета средней величины трех чисел**. В качестве исходных данных принять коды 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите;

- **разбиения секрета с использование гаммирования для трех участников**. В качестве секрета принять первые 3 буквы фамилии, для гамм - любые трехбуквенные сочетания;

- **разделения секрета по схеме Шамира для (3, 5)-пороговой схемы**. В качестве секрета **S** принять модуль суммы разниц кодов 1-ой и последней, 2-ой и предпоследней букв своей фамилии согласно ее положению в алфавите;

- **разделения секрета по схеме Асмута-Блума для (3, 5)-пороговой схемы**. В качестве секрета **S** принять модуль суммы разниц кодов 1-ой и последней, 2-ой и предпоследней букв своей фамилии согласно ее положению в алфавите.

При оформлении отчета необходимо привести данные и таблицы, содержащие последовательность выполнения протоколов.