ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

УПРАВЛЕНИЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Кафедра «Кибербезопасность информационных систем»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к проведению практических занятий
по дисциплине

«Криптографические методы защиты информации»

на тему

«Алгоритмы гомоморфного шифрования»

Авторы
Короченцев Д. А.,
Дроздова И.

Ростов-на-Дону, 2018

Аннотация

Методические указания предназначены для студентов очной формы обучения по направлению подготовки 10.05.01 «Компьютерная безопасность» и преподавателей, ведущих практические занятия по курсу «Криптографические методы защиты информации»; в них содержатся краткие теоретические сведения о понятии гомоморфного шифрования, некоторых гомоморфных алгоритмах и принципах их работы, а также индивидуальные задания для студентов.

Авторы

кандидат технических наук,
доцент кафедры «Кибербезопасность информационных систем»
Короченцев Д.А.

студентка кафедры «Кибербезопасность информационных систем»
Дроздова И.

Оглавление

1. ВВЕДЕНИЕ

1.1 Цель преподавания дисциплины

Целью преподавания дисциплины «Криптографические методы защиты информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

1.2 Связь с предшествующими дисциплинами и последующими дисциплинами

Материал курса «Криптографические методы защиты информации» связан с предшествующими дисциплинами: «Языки программирования», «Теория информации», «Теория кодирования, сжатия и восстановления информации», «Дискретная математика».

Материал курса «Криптографические методы защиты информации» связан с последующими дисциплинами: «Теоретико-числовые методы в криптографии», «Криптографические протоколы», «Методы алгебраической геометрии в криптографии».

1.3 Компетенции обучающегося, формируемые в результате освоения дисциплины

В соответствии с ФГОС ВПО в результате изучения дисциплины студенты должны обладать следующими компетенциями:

- способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.
- способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

2. ПРАКТИЧЕСКОЕ ЗАНЯТИЕ НА ТЕМУ «АЛГОРИТМЫ ГОМОМОРФНОГО ШИФРОВАНИЯ»

2.1 Цель занятия

Целью практического занятия на тему «Алгоритмы гомоморфного шифрования» является получение студентами практических навыков по расчёту криптосистем Пэйе и Бенало.

2.2 Краткие теоретические сведения

В [1] даётся следующее определение гомоморфного шифрования – это криптографический примитив, представляющий собой функцию шифрования, удовлетворяющую дополнительному требованию гомоморфности относительно каких-либо алгебраических операций над открытыми текстами.

Рассмотрим принцип гомоморфного шифрования более подробно, для этого введём следующие обозначения:

E – функция шифрования;
m – открытый текст;
k – ключ шифрования;
op – операция над открытыми текстами.

В данном случае функция E гомоморфна относительно op, если существует какой-либо эффективный алгоритм M, который при поступлении на вход пары криптограмм вида $E\,(k, m_1)$, $E\,(k, m_2)$ на выходе будет иметь криптограмму C такую, что при дешифровании открытый текст будет равен результату операции $m_1\ op\ m_2$.

Различают полностью гомоморфные и частично гомоморфные криптосистемы. Частично гомоморфные криптосистемы [1] – это такие криптосистемы, которые гомоморфны относительно только одной операции (или сложения, или умножения). Такие криптосистемы как RSA, Эль-Гамаль, Гольдвассер-Микали, Пэйе, Бенало, Окамото-Учияма и Шмидт-Самоа-Такаги являются примерами гомоморфных систем. В данном методическом указании представлены две из них: криптосистема Пэйе [2] и криптосистема Бенало [3].

2.3 Алгоритм работы криптосистемы Пэйе

Криптосистема Пэйе – является вероятностной криптосистемой с открытым ключом [2]. Криптосистема Пэйе основана на сложности факторизации большого числа, являющегося произведением двух простых чисел.

Расшифровка шифротекста в данной криптосистеме требует использования функции логарифма L. Кроме того, криптосистема Пэйе использует задачу о трудности определения вычета высокого порядка по модулю n^2, где $n = p * q$.

Первым этапом работы криптосистемы Пэйе является генерация ключей.

Вход: большие простые числа p и q.

Выход: значения n, g, λ, μ.

Шаг 1. Необходимо выбрать два больших простых числа p и q, удовлетворяющие следующему условию $\text{НОД}\,(pq, (p-1)(q-1)) = 1$.

Шаг 2. Вычисляем $n = p * q$ и $\lambda = \text{НОК}\,(p-1, q-1)$.

Шаг 3. Выбираем случайное целое число $g \in Z^*_{n^2}$.

Шаг 4. Необходимо вычислить μ по следующей формуле

$$\mu = \left(L\left(g^{\lambda}\ mod\ n^2\right)\right)^{-1} mod\ n,$$

где $L(u) = \frac{u-1}{n}$.

Шаг 5. Открытым ключом является пара (n, g), а закрытым – (λ, μ).

Для выполнения корректного шифрования необходимо придерживаться следующего алгоритма.

Шаг 1. Определяем открытый текст $m \in Z^*_n$.

Шаг 2. Выбираем случайное число $r \in Z^*_n$.

Шаг 3. Вычисляем шифротекст c по следующей формуле

$$c = g^m * r^n\ mod\ n^2.$$

Расшифрование полученного сообщения выполняется по формуле, приведённой ниже

$$m = L\left(c^{\lambda} \, mod \, n^2\right) * \mu \, mod \, n.$$

Приведём пример генерации ключей для конкретных чисел.

Шаг 1. Определим p и q следующим образом, $p = 19, q = 5$.

Шаг 2. Исходя из выбранных p и q, параметры равны $n = 95, \lambda = 36$.

Шаг 3. Пусть $g = 1594$.

Шаг 4. Следующим шагом вычисляем μ

$$\mu = \left(\frac{1594^{36} \, mod \, 9025 - 1}{95}\right)^{-1} mod \, 95 = 94.$$

Шаг 5. Для выбранных параметров открытым ключом является пара $(95, 1594)$, а закрытым – $(36, 94)$.

Рассмотрим процесс шифрования более подробно.

Шаг 1. Определяем открытый текст $m = 12$.

Шаг 2. Пусть случайный параметр r равен $r = 7$.

Шаг 3. Согласно формуле, вычисляем шифротекст

$$c = 1594^{12} * 7^{95} \, mod \, 9025 = 6448.$$

После получения шифротекста, принимающей стороне необходимо выполнить расшифрование.

$$m = \left(\frac{6448^{36} \, mod \, 9025 - 1}{95}\right) * 94 \, mod \, 95 = 12.$$

Покажем гомоморфность данной криптосистемы. Пусть $m_1 = 12, r_1 = 7, c_1 = 6448$, тогда $m_2 = 22, r_2 = 17, c_2 = 3573$.

$$m_1 + m_2 = c_1 * c_2 \, mod \, n^2,$$
$$m_1 + m_2 = 6448 * 7575 \, mod \, 9025 = 300,$$
$$m_1 + m_2 = \left(\frac{6904^{36} \, mod \, 9025 - 1}{95}\right) * 94 \, mod \, 95 = 34 = 12 + 22.$$

Вычислим сумму по второй формуле

$$m_1 + m_2 = c_1 \; * \; g^{m_2} \, mod \, n^2,$$
$$m_1 + m_2 = 6448 * 1594^{22} \, mod \, 9025 = 8928,$$
$$m_1 + m_2 = \left(\frac{8928^{36} \, mod \, 9025 - 1}{95}\right) * 94 \, mod \, 95 = 34 = 12 + 22.$$

Вычислим произведение отрытых текстов $m_1 = 12$ и $m_2 = 22$

$$m_1 * m_2 \, mod \, n = {c_1}^{m_2} \, mod \, n^2,$$

$$m_1 * m_2 \, mod \, n = \; 6448^{22} \, mod \, 9025 = 2154,$$
$$m_1 * m_2 \, mod \, n = \left(\frac{2154^{36} \, mod \, 9025 - 1}{95}\right) * 94 \, mod \, 95 = 74,$$
$$12 * 22 \, mod \, 95 = 74.$$

Упражнение. Разберитесь в алгоритме работы данной криптосистемы. Для большего понимания принципа работы возьмите иной открытый текст, а затем проведите процедуру шифрования и расшифрования.

2.4 Алгоритм работы криптосистемы Бенало

Данная система [3] позволяет шифровать входную последовательность блоками данных.

Генерация ключа в данной криптосистеме является одной из наиболее трудоёмких задач. Необходимо корректно подобрать ключевые значения таких параметров как p, q, r.

Вход: большие простые числа p, q и блок r.

Выход: значения y, r, n, φ.

Шаг 1. Необходимо выбрать блок r и два больших простых числа p и q, которые должны удовлетворять следующим условиям:

- $r \mid (p-1)$ – r делит $(p-1)$;
- r и $(q-1)$ – взаимно простые.

Шаг 2. Вычисляем $n = p * q$ и $\varphi = (p-1) * (q-1)$.

Шаг 3. Выбираем $y \in Z_n^*$ такой, что $y^{\varphi/r} \not\equiv 1 \, mod \, n$.

Шаг 4. Открытым ключом системы является (y, r, n), а закрытым – (p, q).

Шифрование представляется собой достаточно простой процесс, по сравнению с процессом расшифрования криптограммы.

Шаг 1. Выбираем сообщение $m \in Z_r$ и $u \in Z_n^*$.

Шаг 2. Вычисляем $E_r(m) = y^m * u^r \, mod \, n$.

В данном алгоритме расшифрование является не менее трудоёмкой задачей, нежели генерация ключа. Если параметр m имеет большое значение, то нахождение необходимой величины может занять большое количество времени.

Шаг 1. Вычисляем следующие значения, где $m \in Z_r$

$$T_m = y^{m*\varphi/r} \; mod \; n.$$

Шаг 2. По формуле, которая представлена ниже, вычисляем величину T и ищем совпадение в ранее вычисленном массиве T_m, когда совпадение найдено, то $m = i$

$$T = c^{\varphi/r} \, mod \, n.$$

Стоит отметить, что если r принимает большие значения, то для нахождения m можно воспользоваться алгоритмом Гельфонда-Шенкса, если значения r малы, то можно использовать метод перебора.

Данная криптосистема гомоморфна относительно операции сложения и вычитания, покажем это. Пусть даны два шифротекста $c_1 = y^{m_1}u_1^r$ и $c_2 = y^{m_2}u_2^r$. Гомоморфизм по сложению и вычитанию выражается следующими формулами:

$$c_1 * c_2 = (y^{m_1}u_1^r) * (y^{m_2}u_2^r) \, mod \, n = \; y^{m_1+m_2}(u_1u_2)^r \, mod \, n.$$
$$c_1 * c_2^{-1} = (y^{m_1}u_1^r) * (y^{m_2}u_2^r)^{-1} \, mod \, n = (y^{m_1}u_1^r) * (y^{-m_2} * (u_2^{-1})^r) \, mod \, n$$

Так же стоит отметить, что существует умножение на константу и возведение в степень равную ей, это выражается следующими отношениями:

$$c_1 * y^k \; mod \; n = y^{m+k} * u^r \; mod \; n$$
$$c_1^k \; mod \; n = y^{m*k}(u^k)^r \; mod \; n.$$

Рассмотрим все этапы работы данного алгоритма на примере. Первый из них – это генерация ключа

Шаг 1. Пусть $r = 13, p = 53, q = 7$.

Шаг 2. Вычисляем $n = 371, \varphi = 323$.

Шаг 3. Выбираем $y = 2$.

Шаг 4. Для выбранных параметров открытый ключ – $(2, 13, 371)$, а закрытый – $(53, 7)$.

Шифрование представляет собой следующий алгоритм.

Шаг 1. Выбираем сообщение и случайный параметр, пусть $m = 9, u = 92$.

Шаг 2. Вычислим шифротекст

$$c = \; 2^9 * 92^{13} \; mod \; 371 = 43.$$

Покажем процесс расшифрования.

Шаг 1. Составим таблицу значений $T_i, i \in \{1, m\}$.

Таблица 5 – Значения T_i.

i	1	2	3	4	5	6	7	8	9	10	11	12
T_i	225	169	183	365	134	99	15	36	309	148	281	155

Шаг 2. Вычислим T и определим исходное сообщение

$$T = 43^{312/13} \; mod \; 371 = 309,$$
$$m = 9.$$

Покажем гомоморфизм криптосистемы. Пусть $m_1 = 9, u_1 = 92, c_1 = 43$, тогда $m_2 = 2, u_2 = 205, c_2 = 57$, тогда

$$m_1 + m_2 = c_1 * c_2 \; mod \; n,$$
$$m_1 + m_2 = 43 * 57 \; mod \; 371 = 225.$$

Таблица для $T_m = y^{m*\varphi/r} \; mod \; n \, , i \in \{1, m\}$.

Таблица 6 – Значения T_i

i	1	2	3	4	5	6	7	8	9	10	11	12
T_i	225	169	183	365	134	99	15	36	309	148	281	155

Вычислим $T = m_1 + {m_2}^{\varphi/r} \; mod \; n, \, T = 281$. Таким образом $m = 11 = 9 + 2$.

Упражнение. Разберитесь в алгоритме работы данной криптосистемы. Для большего понимания принципа работы возьмите иной открытый текст, а затем проведите процедуру шифрования и расшифрования.

2.5 Индивидуальное задание

Вариант*	Криптосистема Пэйе	Криптосистема Бенало, y = 2
1	p = 11; q = 7;	p = 43; q = 61; r = 7;
2	p = 47; q = 67;	p = 59; q = 43; r = 29;
3	p = 7; q = 19;	p = 11; q = 7; r = 5;
4	p = 13; q = 67;	p = 7; q = 29; r = 3;
5	p = 5; q = 59;	p = 59; q = 17; r = 29;
6	p = 61; q = 17;	p = 61; q = 13; r = 5;
7	p = 31; q = 53;	p = 59; q = 2; r = 29;
8	p = 67; q = 61;	p = 61; q = 43; r = 5;
9	p = 17; q = 41;	p = 67; q = 53; r = 3;
10	p = 53; q = 23;	p = 53; q = 3; r = 13;
11	p = 29; q = 13;	p = 11; q = 7; r = 5;
12	p = 41; q = 43;	p = 11; q = 47; r = 5;
13	p = 59; q = 11;	p = 43; q = 2; r = 3;
14	p = 37; q = 47;	p = 19; q = 41; r = 3;
15	p = 43; q = 31;	p = 23; q = 31; r = 11;
16	p = 19; q = 17	p = 29; q = 17; r = 7;
17	p = 53; q = 43;	p = 11; q = 53; r = 5;
18	p = 19; q = 43;	p = 11; q = 7; r = 5;
19	p = 17; q = 67;	p = 7; q = 29; r = 3;
20	p = 19; q = 43;	p = 59; q = 17; r = 29;

* - Номер варианта соответствует номеру в журнале группы.

Подсказки

Вариант	Криптосистема Пэйе	Криптосистема Бенало
1	p = 11; q = 7; l = 30; n = 77; n^2 = 5929; g = 2637; mu = 57;	p = 43; q = 61; n = 2623; r = 7; f = 2520; y = 2;
2	p = 47; q = 67; l = 1518; n = 3149; n^2 = 9916201; g = 4763280; mu = 724;	p = 59; q = 43; n = 2537; r = 29; f = 2436; y = 2;
3	p = 7; q = 19; l = 18; n = 133; n^2 = 17689; g = 5962; mu = 88;	p = 11; q = 7; n = 77; r = 5; f = 60; y = 2;
4	p = 13; q = 67; l = 132; n = 871; n^2 = 758641; g = 627049; mu = 181;	p = 7; q = 29; n = 203; r = 3; f = 168; y = 2;
5	p = 5; q = 59; l = 116; n = 295; n^2 = 87025; g = 46986; mu = 112;	p = 59; q = 17; n = 1003; r = 29; f = 928; y = 2;
6	p = 61; q = 17; l = 240; n = 1037; n^2 = 1075369; g = 470848; mu = 836;	p = 61; q = 13; n = 793; r = 5; f = 720; y = 2;
7	p = 31; q = 53; l = 780; n = 1643; n^2 = 2699449; g = 1230260; mu = 1447;	p = 59; q = 2; n = 118; r = 29; f = 58; y = 2;
8	p = 67; q = 61; l = 660; n = 4087; n^2 = 16703569; g = 16485958; mu = 839;	p = 61; q = 43; n = 2623; r = 5; f = 2520; y = 2;
9	p = 17; q = 41; l = 80; n = 697; n^2 = 485809; g = 173132; mu = 281;	p = 67; q = 53; n = 3551; r = 3; f = 3432; y = 2;
10	p = 53; q = 23; l = 572; n = 1219; n^2 = 1485961; g = 1252096; mu = 501;	p = 53; q = 3; n = 159; r = 13; f = 104; y = 2;

11	p = 29; q = 13; l = 84; n = 377; n^2 = 142129; g = 96384; mu = 279;	p = 11; q = 7; n = 77; r = 5; f = 60; y = 2;
12	p = 41; q = 43; l = 840; n = 1763; n^2 = 3108169; g = 951225; mu = 576;	p = 11; q = 47; n = 517; r = 5; f = 460; y = 2;
13	p = 59; q = 11; l = 290; n = 649; n^2 = 421201; g = 347859; mu = 424;	p = 43; q = 2; n = 86; r = 3; f = 42; y = 2;
14	p = 37; q = 47; l = 828; n = 1739; n^2 = 3024121; g = 697646; mu = 103;	p = 19; q = 41; n = 779; r = 3; f = 720; y = 2;
15	p = 43; q = 31; l = 210; n = 1333; n^2 = 1776889; g = 1268491; mu = 639;	p = 23; q = 31; n = 713; r = 11; f = 660; y = 2;
16	p = 19; q = 17; l = 144; n = 323; n^2 = 104329; g = 70630; mu = 286;	p = 29; q = 17; n = 493; r = 7; f = 448; y = 2;
17	p = 53; q = 43; l = 1092; n = 2279; n^2 = 5193841; g = 2335251; mu = 157;	p = 11; q = 53; n = 583; r = 5; f = 520; y = 2;
18	p = 19; q = 43; l = 126; n = 817; n^2 = 667489; g = 437731; mu = 477;	p = 47; q = 29; n = 1363; r = 23; f = 1288; y = 2;
19	p = 17; q = 67; l = 528; n = 1139; n^2 = 1297321; g = 1024230; mu = 934;	p = 59; q = 2; n = 118; r = 29; f = 58; y = 2;
20	p = 19; q = 43; l = 126; n = 817; n^2 = 667489; g = 603447; mu = 139;	p = 67; q = 7; n = 469; r = 11; f = 396; y = 2;

3. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Варновский, Н. П. Гомоморфное шифрование / Н. П. Варновский, А. В. Шокуров // Труды Института системного программирования РАН – 2007. – Том 12.
2. Paillier, P. Public-Key Cryptsystems Based n Cmpsite Degree Residusity Classes / P. Paillier // Advances in cryptlgy, EURCRYPT'99. — 1999. — 223-238 P.
3. Benalh, J. Dense Prbabilistic Encryptin / J. Benalh // Clarksn University – 1994. – 120–128 P.