

Раздел: Основы прикладной криптографии

Практическое задание. «Модуль 1. Криптографические алгоритмы и особенности их применения»

Выполнил: Александр Ганицев

Задание.

Вы закончили первый модуль, посвящённый криптографическим примитивам и особенностям их применения. Чтобы закрепить знания, предлагаем вам решить три задачи.

Задание № 1

Условие задачи

Исходный алфавит $\{A, B, C, D\}$. Используется моноалфавитная система, в которой индивидуальные буквы зашифровываются так:

$A \rightarrow BV, B \rightarrow AAB, C \rightarrow BAV, D \rightarrow A$

Например, слово ABDA зашифровывается как BBAABABB.

Что нужно сделать.

Докажите, что расшифрование всегда однозначно. Покажите, что оно не будет однозначным, если буквы зашифровывать так:

$A \rightarrow AB, B \rightarrow BA, C \rightarrow A, D \rightarrow C$

Формат сдачи

Напишите ответ в свободной форме. Он должен содержать математически строгое доказательство необходимых утверждений.

Задание № 2

Постройте систему защиты информации с открытым ключом на основе решений диофантового уравнения над конечным полем.

$$x^n + y^n = z^n$$

Формат сдачи

Напишите ответ в свободной форме. Он должен содержать описание построенной криптосистемы, включая описание ключевого множества, процессов зашифрования и расшифрования.

Задание № 3

При передаче сообщений используется некоторый шифр. Известно, что каждому из трёх зашифрованных текстов:

ЙМЫВОТСЬЛКЪГВЦАЯЯ

УКМАПОЧСРКЩВЗАХ

ШМФЭОГЧСЙЪКФЪВЫЕАКК

соответствовало исходное сообщение МОСКВА.

Дешифруйте три текста:

ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЬТКУБЧКГЕИШНЕИАЯЯ

ЛСИЕМГОРТКРОМИТВАВКНОПКРАСЕОГНАЪЕП

РТПАИОМВСВТИЕОБПРОЕННИГЪКЕЕАМТАЛВТДЬСОУМЧШСЕОНШЬИАЯК

при условии, что двум из них соответствует одно и то же сообщение. Сообщениями являются крылатые фразы.

Выполнение.

Задача № 1

Исходный алфавит {A, B, C, D}. Используется моноалфавитная система, в которой индивидуальные буквы зашифровываются так:

$A \rightarrow BB, B \rightarrow AAB, C \rightarrow BAB, D \rightarrow A$ (code #1)

Докажите, что расшифрование всегда однозначно. Покажите, что оно не будет однозначным, если буквы зашифровывать так:

$A \rightarrow AB, B \rightarrow BA, C \rightarrow A, D \rightarrow C$ (code #2)

Доказательство.

Возьмём и зашифруем слова, используя данные шифры.

При анализе первого шифра (code #1) выясняется, что каждому символу соответствует свой код и один символ нельзя прочесть двояко:

Слово ABDA зашифровывается как BBAABABB \rightarrow BB (A AB - такого нет), значит только AAB, (ABB – такого нет), значит только A BB.

При использовании второй системы (code #2) пропадает однозначность, ибо символы можно расшифровать более одним вариантом:

Слово АССА зашифровывается как АВАААВ, но оно расшифровывается как АССА и СВСА, два варианта.

Задание № 2

Постройте систему защиты информации с открытым ключом на основе решений диофантового уравнения над конечным полем.

Уравнение:

$$x^n + y^n = z^n$$

Согласно теории, построение криптосистемы с открытым ключом на основе диофантового уравнения $x^n + y^n = z^n$ над конечным полем может быть сложной задачей, так как диофантово уравнение Эйлера ($n > 2$) не имеет целых решений, как известно из теоремы Ферма. Однако мы будем использовать его как исходную математическую основу для создания криптосистемы.

Генерируем открытый и секретный ключи.

Секретный ключ: Выбираем случайное n , которое будет параметром уравнения. Это значение остается в секрете.

Открытый ключ: Вычисляется некоторое большое простое число p , которое будет конечным полем, и выбирается случайная точка (x, y) на кривой $x^n + y^n = z^n \pmod{p}$, которая удовлетворяет диофантову уравнению.

Шифрование:

Пользователь, который хочет отправить зашифрованное сообщение M , выбирает случайное число k и вычисляет точку $(x, y) = k * (\text{открытый ключ})$, где k - секретное число пользователя. Затем пользователь шифрует сообщение M , применяя операцию XOR между битами сообщения и координатами x и y , а затем отправляет (x, y) как зашифрованное сообщение.

Расшифрование:

Владелец секретного ключа получает зашифрованное сообщение в виде точки (x, y) .

Он использует секретное число n для вычисления $z = (x^n + y^n) \pmod{p}$.

Затем владелец секретного ключа может вычислить обратную точку $k(x, y)$ - это точка $(-x, -y) \pmod{p}$.

Далее он использует координаты $(-x, -y)$ и значение z для расшифровки сообщения, выполняя операцию XOR между координатами и битами сообщения, чтобы восстановить исходное сообщение M .

Это предполагает, что диофантово уравнение имеет решение в конечном поле, и оно может быть использовано для создания криптосистемы с открытым ключом. Однако следует отметить, что детали реализации и безопасность такой системы могут быть сложными и требуют тщательного анализа и исследования, чтобы удостовериться в ее надежности и стойкости к атакам.

Построение системы шифрования, пример.

Исходные данные:

$$x = 4$$

$$y = 6$$

$$n \text{ (закрытый ключ)} = 7$$

$$M \text{ (передаваемое сообщение)} = 2$$

$$p \text{ (конечное поле)} = 11, \text{ в него входят значения } x \text{ и } y.$$

Вычисляем z :

$$z = (4^7 + 6^7) \% 11 = (16384 + 279936) \% 11 = 2$$

Открытый ключ – набор параметров $\{p = 11, x = 4, y = 6, z = 2\}$.

Для передачи с $M = 2$, выберем случайное число $k = 5$ ($0 < k < p$).

Зашифровываем наше сообщение M . Тройка зашифрованного сообщения C :

$$C1 = (x^k \% p) = (4^5 \% 11) = 1$$

$$C2 = (y^k \% p) = (6^5 \% 11) = 10$$

$$C3 = (M * z^k \% p) = (2 * 2^5 \% 11) = 9$$

$$C = \{C1 = 1, C2 = 10, C3 = 9\}.$$

Расшифровывание.

Для нахождения обратного элемента k_{inv} для числа k по модулю p , мы ищем такое целое число k_{inv} , которое удовлетворяет следующему условию: $(k * k_{inv}) \% p = 1$ следовательно выражение примет вид: $(5 * k_{inv}) \% 11 = 1$

Для нахождения x , удовлетворяющего этому уравнению, нам найти число x , которое, умноженное на 5 и взятое по модулю 11, дает остаток 1. Подбором находим, что наименьшим числом будет $k_{inv} = 9$, которое удовлетворяет условию, так как: $(5 * 9) \% 11 = 45 \% 11 = 1$

Вычисляем обратные элементы $C1_{inv}$ и $C2_{inv}$ для $C1$ и $C2$ по модулю p :

$$C1_{inv} = C1^{k_{inv}\%11} = 1^9\%11 = 9$$

$$C2_{inv} = C2^{k_{inv}\%11} = 10^9\%11 = 10$$

Восстанавливаем оригинальное сообщение M :

$$M = (C3 * (C1_{inv}^n) * (C2_{inv}^n)) \% p = (9 * (9^7) * (10^7)) \% 11 = (9 * 4782969 * 10000000) \% 11 = 4304672100000000 \% 11 = 8$$

Используя данное уравнение для шифрования я не получил значение расшифрованного текста $M = 2$. Заранее прошу прощения Анна Васильевна, мой математический аппарат слаб для криптографии (я занимался предметом лет 25 назад) и я поддавшись на заверения “кураторов” от Skillfactory про “можно освоить с нуля”, не рассчитал мои силы. Задание выполнил по примеру из интернета и с помощью коллеги.

Задание № 3

При передаче сообщений используется некоторый шифр. Известно, что каждому из трёх зашифрованных текстов:

ЙМЫВОТСЬЛКЪГВЦАЯЯ

УКМАПОЧСРКЩВЗАХ

ШМФЭОГЧСЙЪКФЬВЫЕАКК

соответствовало исходное сообщение [МОСКВА](#).

Дешифруйте три текста:

ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЪТКУБЧКГЕИШНЕИАЯЯЯ

ЛСИЕМГОРТКРОМИТВАВКНОПКРАСЕОГНАЪЕП

РТПАИОМВСВТИЕОБПРОЕННИГЪКЕЕАМТАЛВТДЪСОУМЧШСЕОНШЬИАЯК

при условии, что двум из них соответствует одно и то же сообщение. Сообщениями являются крылатые фразы.

Решение.

Ищем исходное слово МОСКВА:

ЙМЫВОТСЫЛКЪГВЦАЯЯ

УКМАПОЧСРКЩВЗАХ

ШМФЭОГЧСЙЪКФЬВЫЕАКК

Я обратил внимание, что отыскав буквы нашего исходного слова, выявилась закономерность, они встречаются в определенной последовательности:

М * * О * С * * К * * В * А, то есть для получения данного слова из последовательности надо убирать буквы * * * * *.

Применяем данный подход/алгоритм к шифрованным текстам:

ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЪТКУБЧКГЕИШНЕИАЯРЯ

ЛСИЕМГОРТКРОМИТВАВКНОПКРАСЕОГНАЪЕП

РТПАИОМВСВТИЕОБПРОЕННИГЪКЕЕАМТАЛВТДЪСОУМЧШСЕОНШЬИАЯК

Здесь подбираем и смотрим. ТПЕОИРВНТМОЛ... не имеет смысла, продолжаем со второй буквы и так далее, пока не находим комбинации:

ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЪТКУБЧКГЕИШНЕИАЯРЯ
* * * * *

РТПАИОМВСВТИЕОБПРОЕННИГЪКЕЕАМТАЛВТДЪСОУМЧШСЕОНШЬИАЯК
* * * * *

Второй шифр подбирается схожим методом перебора читаемых цепочек:

ЛСИЕМГОРТКРОМИТВАВКНОПКРАСЕОГНАЪЕП
* * * * *

Расшифрованные тексты: ПОВТОРЕНИЕМАТЬУЧЕНИЯ и СМОТРИВКОРЕНЬ.