Задание № 1

Условие задачи

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

A → BB, B → AAB, C → BAB, D → 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 → AB, B → BA, C → A, D → C

Решение

В задание используется моноалфавитная система с неравномерным кодированием. Для неравномерного кодирования расшифрование будет всегда однозначно, если выполняется одно из двух условий:

1. *Сообщение однозначно декодируемо с начала, если никакое кодовое слово не является префиксом другого кодового слова.*
2. *Сообщение однозначно декодируемо с конца, если никакое кодовое слово не является постфиксом другого кодового слова.*

Проверим моноалфавитную систему A → BB, B → AAB, C → BAB, D → A

Выполним проверку первого условия:

Первое кодовое слово BB не является префиксом ни AAB, ни BAB, ни A.

Второе кодовое слово AAB не является префиксом ни BB, ни BAB, ни A.

Второе кодовое слово BAB не является префиксом ни BB, ни AAB, ни A.

Четвёртое кодовое слово A не является префиксом ни BB, ни BAB, но является префиксом кодового слова AAB.

Отсюда делаем вывод, что первое условие не выполняется, и сообщение нельзя однозначно декодировать с его начала.

Выполним проверку второго условия:

Первое кодовое слово BB не является постфиксом ни AAB, ни BAB, ни A.

Второе кодовое слово AAB не является постфиксом ни BB, ни BAB, ни A.

Второе кодовое слово BAB не является постфиксом ни BB, ни AAB, ни A.

Четвёртое кодовое слово A не является постфиксом ни BB, ни AAB, ни BAB.

Отсюда делаем вывод, что второе условие выполняется, и сообщение можно однозначно декодировать с его конца.

Вывод:

Моноалфавитную систему A → BB, B → AAB, C → BAB, D → A можно использовать для однозначного расшифрования.

Проверим моноалфавитную систему A → AB, B → BA, C → A, D → C

Выполним проверку первого условия:

Первое кодовое слово AB не является префиксом ни BA, ни A, ни C.

Второе кодовое слово BA не является префиксом ни AB, ни A, ни C.

Третье кодовое слово A не является префиксом ни BA, ни C, но является префиксом кодового слова AB.

Отсюда делаем вывод, что первое условие не выполняется, и сообщение нельзя однозначно декодировать с его начала.

Выполним проверку второго условия:

Первое кодовое слово AB не является постфиксом ни BA, ни A, ни C.

Второе кодовое слово BA не является постфиксом ни AB, ни A, ни C.

Третье кодовое слово A не является постфиксом ни AB, ни C, но является постфиксом кодового слова BA.

Отсюда делаем вывод, что второе условие не выполняется, и сообщение нельзя однозначно декодировать с его конца.

Вывод:

Моноалфавитную систему A → AB, B → BA, C → A, D → C нельзя использовать для однозначного расшифрования.

Задание № 2

Что нужно сделать

Постройте систему защиты информации с открытым ключом на основе решений диофантового уравнения $x^n+y^n=z^n$ над конечным полем.

Решение

Математический аппарат решения диофантового уравнения в n-ой степени над конечным полем можно использовать в криптосистемах с открытым ключом.

Согласно Великой теореме Ферма, это уравнение не имеет ненулевых целых решений при n>2, а значит решение обратной задачи невозможно за полиномиальное время.

В то же время мы будем решать уравнение над конечным полем, а значит, решения будет существовать.

Выберем большое простое число *p,* принадлежащее конечному полу $F_{p,}$ которое будет являться модулем.

А также выберем простое число *n*, которое будет определять степень уравнения.

Теперь мы можем выбрать одну буквенную пару (*k,l*), принадлежащую нашему конечному полю F_p. Это будет **открытый ключом**.

А пара (x,y) в решение $x^n+y^n \equiv k*x+l*y \pmod p$ станет **закрытым ключом**.

Теперь для того, чтобы **зашифровать** сообщение *m* нам достаточно взять случайное число *q* также принадлежавшее конечному полю F_p

Вычислить шифрованную пару (c_1,c_2) из $c_1 \equiv k*q \bmod p$ и $c_2 \equiv m + l*q \bmod p$

Для того, чтобы **расшифровать** сообщение достаточно вычислить $m \equiv c_2 – x *c_2 \bmod p$, где m оригинальное сообщение.

Задание № 3

Условие задачи

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

ЙМЫВОТСЬЛКЪГВЦАЯЯ

УКМАПОЧСРКЩВЗАХ

ШМФЭОГЧСЙЪКФЬВЫЕАКК

соответствовало исходное сообщение МОСКВА.

Что нужно сделать

Дешифруйте три текста:

ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЬТКУБЧКГЕИШНЕИАЯРЯ

ЛСИЕМГОРТКРОМИТВАВКНОПКРАСЕОГНАЬЕП

РТПАИОМВСВТИЕОБПРОЕННИГЬКЕЕАМТАЛВТДЬСОУМЧШСЕОНШЬИАЯК

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

Решение

Изучим первые три шифртекста. Нам известно, что в них зашифровано слово МОСКВА.

Выделим в первом шифртексте буквы, соответствующие этому слову. Вначале ищем букву М:

Й**М**ЫВОТСЬЛКЪГВЦАЯЯ

После этого, продолжая с найденной буквы М, ищем следующую букву О:

Й**М**ЫВ**О**ТСЬЛКЪГВЦАЯЯ

После этого, продолжая с найденной буквы О, ищем следующую букву С:

Й**М**ЫВ**О**Т**С**ЬЛКЪГВЦАЯЯ

И так далее, пока не найдём все буквы. В итоге получим:

Й**М**ЫВ**О**Т**С**ЬЛ**К**ЪГ**В**Ц**А**ЯЯ

Делаем вывод, что используется шифрование с добавлением «мусора». Проверим аналогичным образом оставшиеся два шифртекста:

УКМАПОЧСРКЩВЗАХ

ШМФЭОГЧСЙЪКФЬВЫЕАКК

Делаем вывод, что для шифрования крылатых фраз используется такая же система. В начале, в конце и между буквами вставляется одна или две «мусорные» буквы.

Мы знаем, что в двух из трёх шифртекстов крылатых фраз используется одна и та же фраза. Предполагаем, что длина шифртекстов для одинаковых фраз будет примерно одинаковая. Первый шифртекст имеет длину 50 знаков, второй – 34 знака, третий – 52 знака. Поэтому для сравнения берём первый и третий шифртексты.

ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЬТКУБЧКГЕИШНЕИАЯРЯ

РТПАИОМВСВТИЕОБПРОЕННИГЬКЕЕАМТАЛВТДЬСОУМЧШСЕОНШЬИАЯК

Ранее мы установили, что в начале шифртекста может находиться одна или две «мусорные» буквы. Значит, нам необходимо сравнивать 2 и 3 буквы из первого шифртекста со 2 и 3 буквами третьего шифртекста, чтобы найти совпадающие.

Для первого это – ПЕ, для второго – ТП. Совпадающая буква П. Отметим её:

ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЬТКУБЧКГЕИШНЕИАЯРЯ

РТПАИОМВСВТИЕОБПРОЕННИГЬКЕЕАМТАЛВТДЬСОУМЧШСЕОНШЬИАЯК

Следуя такому же правилу, пропускаем первую букву (так как она всегда будет «мусорной») после найденной и сравниваем две следующие.

Для первого это – ОИ, для второго – ИО. Первая неоднозначность, подходит как и буква И, так и буква О. Проверяем следующую букву для обоих случаев. Вначале для буквы О:

ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЬТКУБЧКГЕИШНЕИАЯРЯ

РТПАИОМВСВТИЕОБПРОЕННИГЬКЕЕАМТАЛВТДЬСОУМЧШСЕОНШЬИАЯК

Аналогично берём вторую и третью букву после найденной.

Для первого это – РВ, для второго – ВС. Совпадающая буква В.

Теперь проверим следующую букву для случая с буквой И:

ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЬТКУБЧКГЕИШНЕИАЯРЯ

РТПАИОМВСВТИЕОБПРОЕННИГЬКЕЕАМТАЛВТДЬСОУМЧШСЕОНШЬИАЯК

Аналогично берём вторую и третью букву после найденной.

Для первого это – ВН, для второго – МВ. Совпадающая буква В.

Как видно эта неоднозначность не повлияет на дальнейшее расшифрования. Поэтому мы продолжаем анализировать шифротексты по правилу выше. В итоге мы получим следующее:

ТПЕОИРВНТМОЛАРГЕИАНВИЛЕДНМТААГТДЬТКУБЧКГЕИШНЕИАЯРЯ

РТПАИОМВСВТИЕОБПРОЕННГЬИКЕЕАМТАЛВТДЬСОУМЧШСЕОНШЬИАЯК

То есть зашифрованной крылатой фразой для первого и третьего шифртекста является ПОВТОРЕНИЕМАТЬУЧЕНИЯ.

Теперь осталось только расшифровать второй шифртекст. Делаем мы это похожим образом.

ЛСИЕМГОРТКРОМИТВАВКНОПКРАСЕОГНАЬЕП

Предполагаем, что первая буква крылатой фразы либо 2, либо 3, т.е. либо С, либо И. Теперь продолжаем для каждого варианта. Для С следующими буквами могут быть Е и М, для И – М и Г. Теперь проверяем следующую букву для каждой пары. Для СЕ следующими буквами могут быть Г и О, для СМ – О и Р, для ИМ – О и Р, для ИГ – Р и Т. Может показаться, что задача слишком усложняется, но уже на этом этапе можно отбросить заведомо «нечитаемые» цепочки. Например, СЕО, СМР, ИМО, ИМР, ИГТ. И продолжить проверять только цепочки СЕГ, СМО и ИГР. В итоге продолжая наши цепочки и отбрасывая «нечитаемые» приходим к следующему:

ЛСИЕМГОРТКРОМИТВАВКНОПКРАСЕОГНАЬЕП

То есть зашифрованной крылатой фразой для второго шифртекста является СМОТРИВКОРЕНЬ.