|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ЛЕКЦИОННЫЕ МАТЕРИАЛЫ** | | | |  |
| . | | |  | |
|  | | |  | |
|  | | | |  |
| **ЛЕКЦИЯ№ 7.** | | | |  |
| Подисциплине: | | **Б2.В,ДВ.3.1 «Криптографическиеметодызащитыинформации»** | | |
|  | | (шифр и наименованиеучебнойдисциплины) | | |
| Потеме: | **Линейные уравнения,содержащие сравнения.Китайскаятеоремаобостатках. Формулировкатеоремы. Алгоритмнахождениярешениясистемысравнений, использующийкитайскуютеоремуобостатках.Афинный шифр.** | | | |
|  | (наименованиетемылекции) | | | |
| РТУ МИРЭА 2020 г. | | | |  |

Темалекции: **Линейные уравнения, содержащие сравнения.Китайская теорема об остатках. Формулировка теоремы. Алгоритмн ахождения решения системы сравнений, использующий китайскую теорему об остатках.Афинный шифр.**

**Учебные и воспитательныецели:**

1. Сформировать у студентов понимания возможностей китайской теоремы об остатках как эффективного инструмента криптографии

2. Реализовать на примерах алгоритм нахождения решения системы сравнений, использующий китайскую теорему об остатках.

3. Привить чувство ответственности за будущую профессию.

**Время:** 2 часа (90 мин.).

Литература:

а) Основная:

1. ГорбенкоА.О.,Основыинформационнойбезопасности: введение в профессию.Учебноепособие, СПб: ИЦ «Интермедия», 2016.‒ 224 с.

2. БутаковаН.Г.,Федоров Н.В. Криптографическиеметодызащитыинформации. Учебноепособие, СПб: ИЦ «Интермедия», 2016. ‒ 312 с.

3.Хорев А.А.,Защитаинформацииотутечкипотехническимканалам. Учебник. СПб: ИЦ «Интермедия», 2016. 920 с.

б) Дополнительнаялитература:

1. Зайцев А.П. и др. Техническиесредства и методызащитыинформации. Уч. пособие. М.:Горячаялиния – Телеком. 2009. – 615 с.

2. Романец Ю.В. и др. Защитаинформации в компьютерныхсистемах и сетях. М.:Радио и связь. 1999. – 376 с.

3. Лозовецкий В.В. Информационнаябезопасность. М.: Изд. ИУИ. 2011. – 169 с.

Учебно-материальноеобеспечение:

1. Наглядныепособия.

2. Техническиесредстваобучения: проектор.

3. Приложения: рисунки, таблицы, слайды.

ПЛАН ЛЕКЦИИ:

**Введение**– до 5 мин.

**Основнаячасть** (учебныевопросы) – до 80 мин

1. Линейные уравнения, содержащие сравнения.Решение системы линейных уравнений сравнения.- 25мин.

2-й учебныйвопрос :Китайская теорема об остатках. Формулировка теоремы.

30 мин.

3-й учебныйвопрос:Афинный шифр – 30 мин.

Заключение – до 5 мин.

Введение – до 5 мин.

Методическиерекомендации:

- показать актуальность темы;

- довести целевую установку через основные положения лекции;

- охарактеризоват ьместо и значение данной темы в курсе;

- дать обзор важнейших источников, монографий, литературы по теме;

- вскрыть особенности изучения студентами материала п орассматриваемой проблеме.

Основнаячасть – до 80 мин.

**7.1. Линейноеуравнение, содержащие сравнения.** *Криптография* часто включает в себя решение уравнения или *множества* уравнений с одной или более переменнми с коэффициентом в Zn. Это траздел показывает, как решатьуравнения с одним неизвестным, когда степень переменной равна 1 (*линейноеуравнение*).

**Линейные уравнения с однимнеизвестным, содержащие сравнения**

Давайте посмотрим, как решаются уравнения с одним неизвестным, содержащие сравнения, то есть уравнения **ax=b modn** Уравнение этого типа может не иметь ни одного решения или иметь ограниченное число решений. Предположим, что **НОД (a, n) = d**. Если **d†b**, решение не существует. Если **d|b**, то имеется **d** решений.

Если **d|b**, то для того, чтобы найти решения, мы используем следующую стратегию.

* Сократить уравнение, разделив обе стороныу равнения (включаямодуль) на **d**.
* Умножить обе стороны сокращенного уравнения на мультипликативную  *инверсию*, чтобы найти конкретное решение **x0**.
* Общие решения будут **x = x0 + k (n/d) для k = 0, 1..., (d – 1).**

**7.1.1 Решить сравнение**

**5\*x=7 mod 8НОД(5,8)=1**

**Перебирая значения Х= 1,2,3….**

**Получим ,что при Х=3**

**5\*3=7 mod8**

**7.1.2 Пример**

**6х=7mod 15**

**НОД(6,15)=3, но 3 и 7 не имеют общего делителя – решения нет**

**Пример7.2**

Решитьуравнение .

Сначаламынайдем **НОД(10,15) = 5.**Полученноечисло **5**неделитсяна **2**, решениеотсутствует.

**Пример7.3**Решитьуравнение

**14X= 12 mod 18( делим на d=2)**

Заметим, что **НОД (14, 18) = 2.**Поскольку **2** делит **12**, мы имеем точно два решения, но сначала сократим уравнение:

**7x= 6 mod9 ….. x=6\*7-1 mod9**

**7-1 (mod 9)=4 Отсюда Х0 = 24 mod 9 =6 mod 9 иK=0,1(0…d-1)Х1  =X0+9=15.**

Оба решения, **6 и 15**, удовлетворяют уравнению сравнения, потомучто , а также .

**Пример7.4**

Решитьуравнение .

**Решение**

Сначаламыприводимуравнение к форме . Мыприбавляем **(–4)** к обеимсторонам( **4** аддитивная *инверсия*). Получим . Поскольку **НОД (3, 13) = 1**, уравнениеимееттолькооднорешение, 

**Так как 3-1 mod 13= 9**

Мыможемвидеть, чтоответудовлетворяетпервоначальномууравнению: .

**Решение уравнения типа a\*x=b (modp)(1)**

**Умножив обе части данного уравнения на a-1 получим**

**X=a-1bmod(p)**

**Уравнение Эйлера**

**aφ(p) =1 (modP) (2)**

**Умножив обе части данного уравнения на bполучим**

**aφ(p) \*b =b (modP) (3)**

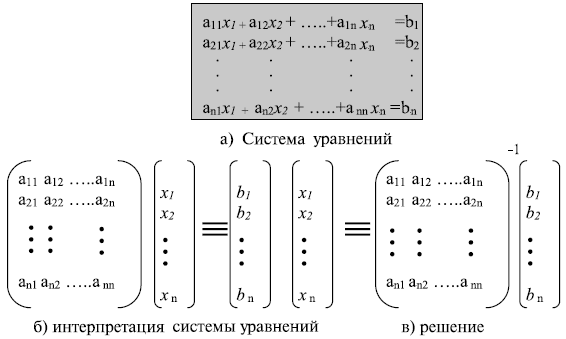
**Таким образом, х будет вычисляться по формуле**

**X= aφ(p)-1 \*bmodp**

**Системалинейныхуравнений, содержащихсравнения**

Мыможемрешитьсистему *линейныхуравнений* с одним и темжемодулем, еслиматрица, сформированнаяиз *коэффициентовсистемы* уравнений, имеетобратнуюматрицу. Длярешенияуравнениясоставляютсятриматрицы. Первая — квадратнаяматрица — формируетсяизкоэффициентовуравнения. Вторая — матрица-столбец — составляетсяизпеременных. Третья — матрица-столбец в правойсторонеоператорасравнения — состоитиззначения **bn**. Мыможемэтоуравнениепредставитькакпроизведениематриц. Еслиобесторонысравненияумножитьнамультипликативную *инверсию* первойматрицы, в результатемыполучимрешениесистемыуравнений, какэтопоказанона [7](#image.3.9).1.

Мы рассматривали это на одной из предыдущих лекций-как показано ниже:



**Рис. 7.1.**Системалинейныхуравнений.

**Решение системы линейных уравнений НОД(m1,m2) не равен 1**.

Рассмотрим систему линейных сравнений следующего вида(НОД (m1,m2)) отличается от 1 и которую можно решить методом подстановки:

X=5 (mod18),

X=8 (mod21).

Так как **НОД(18,21)=3**, то эта система не подходит под китайскую теорему об остатках.

Поэтому решаем её методом подстановки – из первого уравнения получаем

**X=5 +18t1**и подставляем во второе уравнение

**5+18t1= 8 mod21**, переносим **5** в правую часть

**18t1= 3 mod 21**, сокращаем левую и правую части на 3 получим

**6t1 = 1 mod 7**.

ПрименяемтеоремуЭйлера – **t1=a(^φ(p-1))b(modp)**, где**φ(p)= φ(7)=6**

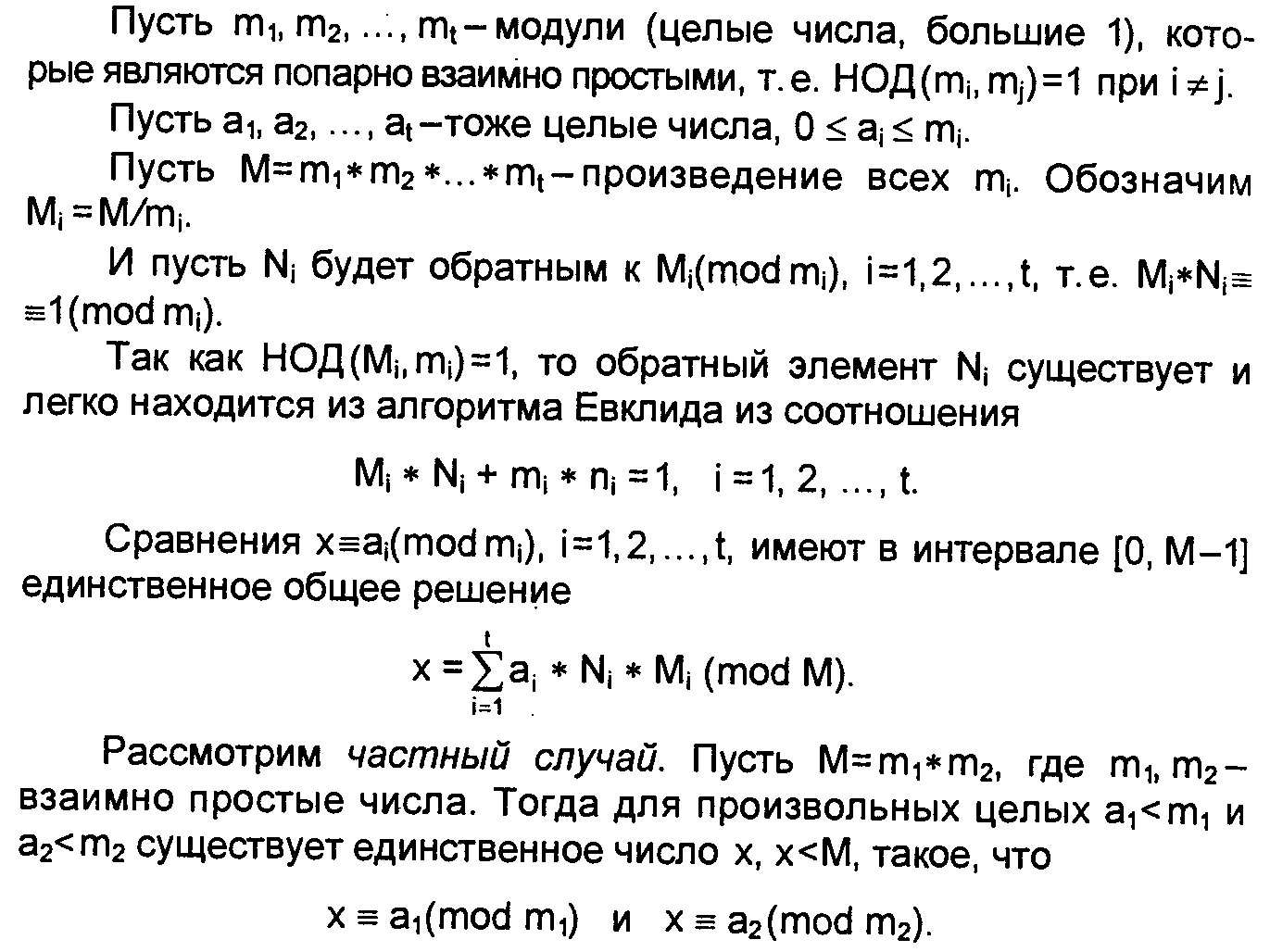
Тогда **t1=6(^(6-1))\*1( mod7)= (-1)( mod7)**.

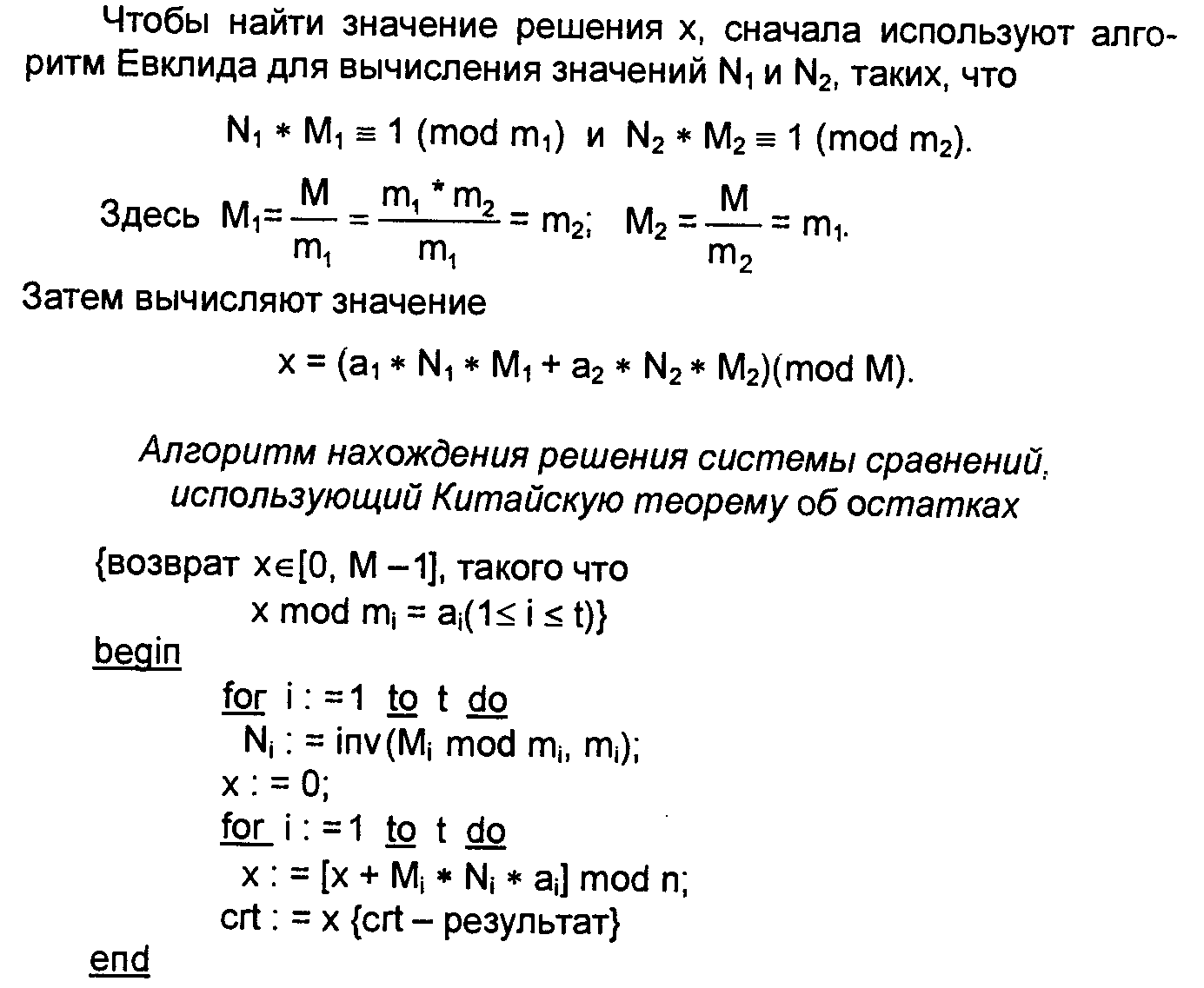
То есть **t1= -1(+-) 7t2**, подставляя данное значение в **x**получим, что

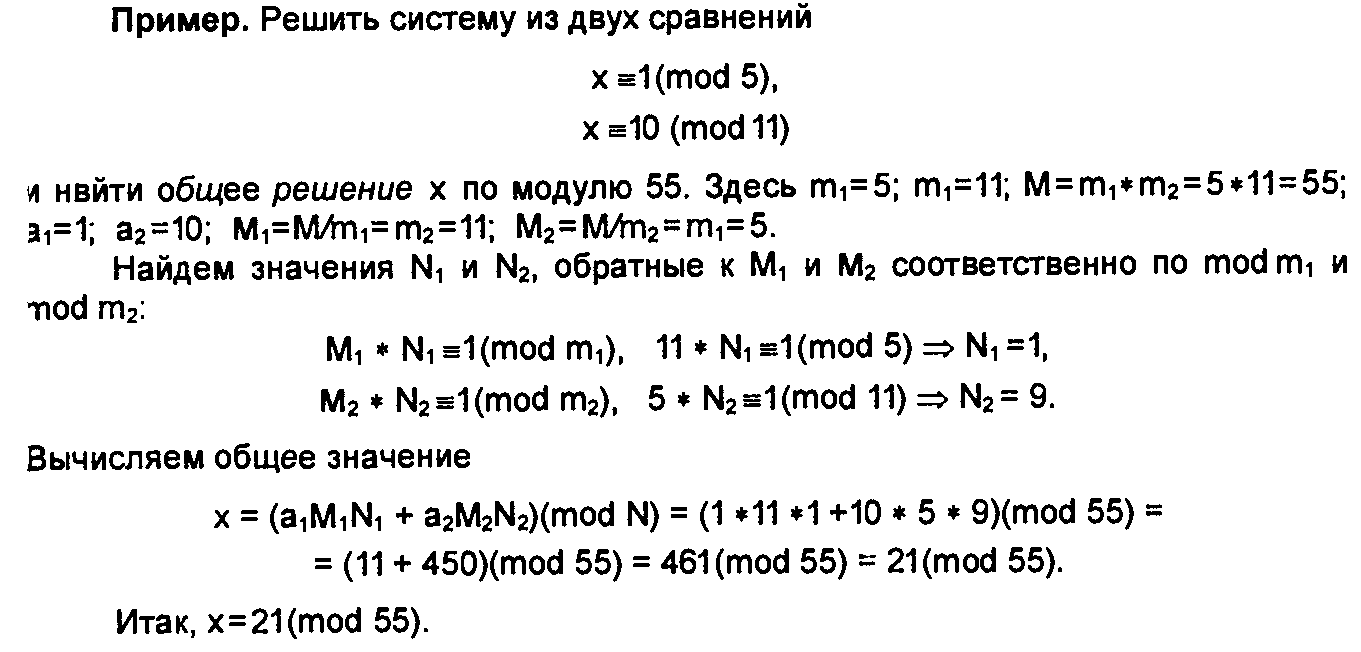
**Х= 5+18\*(-1(+-)7t2)=-13 +-126t2=113(при t2=1).**

2.

#### 







### Элементарнаяалгебра

**Как пример рассмотрим систему:**

|  |  |
| --- | --- |
|  |  |

**X=1 mod 2;**

**X=2 mod3;**

**X=6 mod 7;**

**Для решения системы выпишем отдельно решения первого, второго и третьего уравнений (достаточно выписать решения не превосходящие 2 × 3 × 7 = 42):**

**X 1  ={1,3,5,7,9,11,,39, {41} ,43,},**

X2 ={2,5,8,11,14,38, {41} ,44,},

X3 ={6,13,20,27,34, {41} ,48,}.

**Очевидно, что множество решений системы будет пересечение представленных выше множеств. По утверждению теоремы решение существует и единственно с точностью до операции взятия по модулю 42.**

**X1 =(1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41..)**

**X2 =(2,5,8,11,14,17,20,23,26,29,32,35,38,41,..)**

**X3 =(6,13,20,27,34,41..)**

**3. Аффинный шифр.**

**Аффинный шифр.**

**Аффинный шифр**— это частный случай более общего моноалфавитного [шифра подстановки](https://ru.wikipedia.org/wiki/Шифр_подстановки). К [шифрам подстановки](https://ru.wikipedia.org/wiki/Шифр_подстановки) относятся также [шифр Цезаря](https://ru.wikipedia.org/wiki/Шифр_Цезаря), [ROT13](https://ru.wikipedia.org/wiki/ROT13) и [Атбаш](https://ru.wikipedia.org/wiki/Атбаш). Поскольку аффинный [шифр](https://ru.wikipedia.org/wiki/Шифр) легко дешифровать, он обладает слабыми [криптографическими](https://ru.wikipedia.org/wiki/Криптография) свойствами

В аффинном шифре каждой букве алфавита размера ставится в соответствие число из диапазона 0..m-1. Затем при помощи [модульной арифметики](https://ru.wikipedia.org/wiki/Модульная_арифметика) для каждого числа, соответствующего букве исходного алфавита, вычисляется новое число, которое заменит старое в шифротексте.

Функция [шифрования](https://ru.wikipedia.org/wiki/Шифрование)длякаждойбуквы

**E(x)= (aх+b)mod m**, где m-размер алфавита, a, b -ключ, a и m- взаимнопростые числа.

Функция рас[шифрования](https://ru.wikipedia.org/wiki/Шифрование) длякаждойбуквы

D(x)=a(^(-1))((E(x)-b) mod m = x mod m, где

1= a(^(-1))\*a.

Примеры шифрования и расшифрования.

В следующих примерах используются латинские буквы от A до Z, соответствующие им численные значения приведены в таблице.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**Шифрование**.

В этом примере необходимо зашифровать сообщение "**ATTACK AT DAWN**", используя упомянутое выше соответствие между буквами и числами, и значения **a=3,b=4,** так как в используемом алфавите **26** букв. Только на число a=3 наложены ограничения, так как оно должно быть взаимно простым с 26. Возможные значения :**1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 и 25.** Значение может быть любым, только если не равно единице, так как это сдвиг шифра. Итак, для нашего примера функция шифрования . Первый шаг шифрования — запись чисел, соответствующих каждой букве сообщения.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| сообщение | A | T | T | А | C | K | A | T | D | A | W | N |
| x | 0 | 19 | 19 | 0 | 2 | 10 | 0 | 19 | 3 | 0 | 22 | 13 |

Теперь, для каждого значения x найдем значение 3x+4. После нахождения значения для каждого символа возьмем остаток от деления на 26. Следующая таблица показывает первые четыре шага процесса шифрования.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| сообщение | A | T | T | А | C | K | A | T | D | A | W | N |
| x | 0 | 19 | 19 | 0 | 2 | 10 | 0 | 19 | 3 | 0 | 22 | 13 |
| 3x+4 | 4 | 61 | 61 | 4 | 10 | 34 | 4 | 61 | 13 | 4 | 70 | 43 |
| (3x+4)mod26 | 4 | 9 | 9 | 4 | 10 | 8 | 4 | 9 | 13 | 4 | 18 | 17 |

Последний шаг процесса шифрования заключается в подстановке вместо каждого числа соответствующей ему буквы. В этом примере шифротекст будет "EJJEKIEJNESR". Таблица ниже показывает все шаги по шифрованию сообщения аффинным шифром.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| сообщение | A | T | T | А | C | K | A | T | D | A | W | N |
| x | 0 | 19 | 19 | 0 | 2 | 10 | 0 | 19 | 3 | 0 | 22 | 13 |
| 3x+4 | 4 | 61 | 61 | 4 | 10 | 34 | 4 | 61 | 13 | 4 | 70 | 43 |
| (3x+4)mod26 | 4 | 9 | 9 | 4 | 10 | 8 | 4 | 9 | 13 | 4 | 18 | 17 |
| шифротекст | E | J | J | E | K | I | E | J | N | E | S | R |

**Расшифрование**

Для расшифрования возьмем шифротекст из примера с шифрованием. Заменим букву х на букву у – для лучшего понимания методики расшифрования.Функциярасшифрования будет **D(y) =a(^(-1))(y+m- b)** ., где a=9, b=4.(+ m –для ухода от отрицательных чисел).

Замечание: если каждая y больше или равно b, то функция расшифрование принимает вид D(y)= a(^(-1))(y-b) .

Точно так же, как и в обозреваемом примере, но разберём общий вариант.

Для начала запишем численные значения для каждой буквы шифротекста, как показано в таблице ниже.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| шифротекст | E | J | J | E | K | I | E | J | N | E | S | R |
| y | 4 | 9 | 9 | 4 | 10 | 8 | 4 | 9 | 13 | 4 | 18 | 17 |

Теперь для каждого необходимо рассчитать и взять остаток от деления этого числа на 26. Следующая таблица показывает результат этих вычислений.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| шифротекст | E | J | J | E | K | I | E | J | N | E | S | R |
| y | 4 | 9 | 9 | 4 | 10 | 8 | 4 | 9 | 13 | 4 | 18 | 17 |
| 9\*(y+26-4) | 234 | 279 | 279 | 234 | 288 | 270 | 234 | 279 | 315 | 234 | 360 | 351 |
| 9(y+26-4)mod26 | 0 | 19 | 19 | 0 | 2 | 10 | 0 | 19 | 3 | 0 | 22 | 13 |

Последний шаг операции расшифрования для шифротекста — поставить в соответствие числам буквы. Сообщение после расшифрования будет "ATTACKATDAWN". Таблица ниже показывает выполнение последнего шага.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| шифротекст | E | J | J | E | K | I | E | J | N | E | S | R |
| y | 4 | 9 | 9 | 4 | 10 | 8 | 4 | 9 | 13 | 4 | 18 | 17 |
| 9\*(y+26-4) | 234 | 279 | 279 | 234 | 288 | 270 | 234 | 279 | 315 | 234 | 360 | 351 |
| 9(y+26-4)mod26 | 0 | 19 | 19 | 0 | 2 | 10 | 0 | 19 | 3 | 0 | 22 | 13 |
| сообщение | A | T | T | A | C | K | A | T | D | A | W | N |

**Шифрование всего алфавита**

Чтобы ускорить шифрование и расшифрование, можно провести процедуру шифрования для всех букв алфавита и получить таблицу соответствий между буквами исходного сообщения и шифротекста. Для использованных выше примеров такая таблица будет выглядеть следующим образом:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **буква сообщения** | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|  | 4 | 7 | 10 | 13 | 16 | 19 | 22 | 25 | 2 | 5 | 8 | 11 | 14 | 17 | 20 | 23 | 0 | 3 | 6 | 9 | 12 | 15 | 18 | 21 | 24 | 1 |
| буква шифротекста | E | H | K | N | Q | T | W | Z | C | F | I | L | O | R | U | X | A | D | G | J | M | P | S | V | Y | B |

Заключение – до 5 мин.

Методическиерекомендации:

- обобщитьнаиболееважные, существенныевопросылекции;

- сформулироватьобщиевыводы;

- поставитьзадачидлясамостоятельнойработы;

- ответитьнавопросыстудентов.

Лекцияразработана «\_\_\_»\_\_\_\_\_\_\_\_20\_\_г.

\_\_\_\_\_\_\_\_\_\_\_\_ /Дедов О.П../