**ЛЕКЦИОННЫЕ МАТЕРИАЛЫ**

|  |  |
| --- | --- |
| **Б2.В,ДВ.3.1 «Криптографические методы защиты информации»»** | |
| *(наименованиедисциплины (модуля) в соответствии с учебнымпланом)* | |
| Уровень | бакалавриат, специалитет |
|  | *(бакалавриат, магистратура, специалитет)* |
| Формаобучения | очная |
|  | *(очная, очно-заочная, заочная)* |
| Направление(-я)  подготовки | 10.05.02 «Информационнаябезопасность» |
|  | *(код(-ы) и наименование(-я))* |
|  |  |
| Институт | Кибербезопасности и цифровых технологий. |
|  | *(полное и краткоенаименование)* |
| Кафедра | Информационное противоборство (КБ-8) |
|  | *(полное и краткоенаименованиекафедры, реализующейдисциплину (модуль))* |
| Лектор | ДоцентДедовОлегПетрович |
|  | *(сокращенно – ученаястепень, ученоезвание; полностью – ФИО)* |

|  |  |  |
| --- | --- | --- |
| Используются в даннойредакции с учебногогода | 2021/2022 | |
|  | *(учебныйгодцифрами)* | |
| Проверено и согласовано «\_\_\_\_» \_\_\_\_\_\_\_\_20\_\_\_г. |  |  |
|  | *(подписьдиректораИнститута/Филиала с расшифровкой)* | |

Москва 2020 г.

|  |  |  |  |
| --- | --- | --- | --- |
| Федеральноегосударственноебюджетноеобразовательноеучреждение высшегообразования  **«МИРЭА – Российскийтехнологическийуниверситет»**  **МИРЭА**  Кафедра КБ-8 " Информационное противоборство " | | | |
|  | | |  |
|  | | |  |
|  | | | |
| **ЛЕКЦИЯ № 8** | | | |
| По дисциплине: | | **Б2.В,ДВ.3.1 « Криптографические методы защиты информации »** | |
|  | | (шифр и наименованиеучебнойдисциплины) | |
| По теме: | **Ведение. Поля Галуа на основе арифметики по модулю неприводимых многочленов. Поля Галуа типа GF(2n)** | | |
|  | (наименованиетемылекции) | | |
|  | | |
|  | | |  |
| МИРЭА – 2020 г. | | | |

Тема лекции: **Поля Галуа на основе арифметики по модулю неприводимых многочленов. Поля Галуа типа GF(2n)**

Учебные и воспитательныецели:

1. Сформировать у студентов представление о предмете, изучаемом в рамках курса «Математические основы криптологии».

2. Рассмотреть следующие вопросы Сформировать у студентов представление о полях Галуа на основе арифметики по модулю неприводимых многочленов и их использовании в современной криптографии.

**2. Дать анализ полей Галуа типа GF(2n). Разобрать примеры вычислений в конечных полях.**

3. Привить чувство ответственности за будущую профессию.

**Время:** 2 часа (90 мин.).

Литература:

а) Основная:

1. Рябко Б.Я.,Фионов А.Н. Криптография в современноммире.-М.: Горячаялиния-Телеком, 2018.-300с.:ил.

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

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

4.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:

Наглядныепособия.

Техническиесредстваобучения: проектор.

Приложения: рисунки, таблицы, слайды.

ПЛАН ЛЕКЦИИ:

**Введение**– до 5 мин.

Тема лекции: **ПоляГалуанаосновеарифметикипомодулюнеприводимыхмногочленов. ПоляГалуатипа GF(2n)**

Учебные и воспитательныецели:

1. Сформировать у студентов представление о предмете, изучаемом в рамках курса «Математические основы криптологии».

2. Рассмотреть следующие вопросы Сформировать у студентов представление о полях Галуа на основе арифметики по модулю неприводимых многочленов и их использовании в современной криптографии.

**2. Дать анализ полей Галуа типа GF(2n). Разобрать примеры вычислений в конечных полях.**

3. Привить чувство ответственности за будущую профессию.

**Время:** 2 часа (90 мин.).

ПЛАН ЛЕКЦИИ:

**Введение**– до 5 мин.

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

1-й учебныйвопрос:Свойства полей Галуа.

Поля Галуа на основе арифметики по модулю неприводимых многочленов.– 40 мин.

2-й учебныйвопрос:**Арифметические операции в** Полях Галуа типа GF(2n) – 40 мин.

Заключение – до 5 мин.

Введение – до 5 мин.

Методические рекомендации:

- показатьактуальностьтемы;

- довестицелевуюустановкучерезосновныеположениялекции;

- охарактеризоватьместо и значениеданнойтемы в курсе;

- датьобзорважнейшихисточников, монографий, литературыпотеме;

- вскрытьособенностиизучениястудентамиматериалапорассматриваемойпроблеме.

Основнаячасть – до 80 мин.

**1.Поля Галуанаосновеарифметикипомодулюнеприводимыхмногочленов.**

Свойства полей Галуа.ПоляГалуанаосновеарифметикипомодулюнеприводимыхмногочленов.–

Поле-множество элементов(конечное) с операциями \*,+.

Для этих операций +: а+в=в+а - коммутативность

(а+в)+с=a+(b+c) -ассоциативность

Для умножения \* :a\*b=b\*a

a\*(b+c)=a\*b+a\*c

( a\*b)\*c=a\*(b\*c) (a+b)\*c=a\*c+b\*c

Существует нейтральный элемент по сложению: а+0=0+а=а

Существует единичный элемент а\*1= 1\*a=a

Для любого элемента входящему в множество существует элемент (–а) , который удовлетворяет условию а+(-а) =0

Для любого элемента а входящему в множество существует элемент а(^(-1)) , который удовлетворяет условию а+(а(^(-1))=1

Поле обозначается GF(p^n)- всегда конечно в нём (p^n) элементов, n-натуральное число, р-характеристика поля- простое число.

**Дополнительное замечание**

Поле — структура, которая поддерживает две пары операций, используемые в математике: сложение/вычитание и умножение/деление. Есть одно исключение: не разрешено деление на нуль.

**Конечные поля**

Хотя общее определение касается полей бесконечного порядка, в криптографии используются экстенсивно только конечные поля. **Конечное поле** — поле с конечным числом элементов — является очень важной структурой в криптографии. Галуа показал что поля, чтобы быть конечными, должны иметь число элементов **pn**, где **p** — простое, а **n**— положительное целое число. Конечные поля обычно называют **полями Галуа** и обозначают как **GF(pn**).

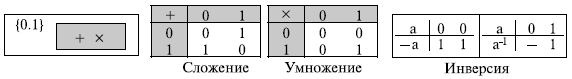
**Поле Галуа, GF(p** n**), — конечное поле с p** n **элементами**.

**Поля GF (p)**

Когда **n = 1**, мы имеем поле **GF (p).** Это поле может быть множеством **Zp, (0, 1, …p–1)** с двумя арифметическими операциями (сложение и умножение). Любой элемент в этом множестве имеет аддитивную *инверсию*, и элементы, отличные от нуля, имеют мультипликативную *инверсию* (мультипликативная *инверсия* для 0 отсутствует).

**Пример .**

Очень общее поле в этой категории — **GF (2)** с множеством **{0,1}** и двумя операциями, сложением и умножением, как показано на рисунке 8.1.



**Рис. 8.1.**Поле GF (2)

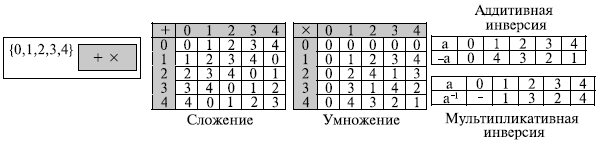
Есть несколько моментов, которые следует отметить в определении этого поля. Первый: множество имеет только два элемента, которые являются двоичными цифрами или битами (**0, 1**). Второй: операция сложения — фактически ИСКЛЮЧАЮЩЕЕ ИЛИ (XOR), операция, которую мы используем с двумя двоичными цифрами. Третий: операция умножения —AND, операция, которую мы используем с двумя двоичными цифрами. Четвертый: сложение и операции вычитания — те же самые (операция **XOR** ). Пятый: умножение и операции деления — те же самые (ОПЕРАЦИЯ AND).

**Сложение/вычитание в GF(2) — операция ИСКЛЮЧАЮЩЕЕ ИЛИ (XOR); умножение/деление — ОПЕРАЦИЯ И (AND)**.

**Пример.**

Мы можем определить **GF(5)** на множестве **Z5** ( **5** простое) с операторами сложения и умножения, показанными на рис. 8.2.

Хотя мы можем использовать расширенный алгоритм Евклида, чтобы найти мультипликативные инверсии элементов в **GF(5),** проще составить таблицу умножения и находить каждую пару, произведение которой равняется **1**. Это **(1, 1), (2, 3), (3, 2) и (4, 4)**. Заметим, что мы можем на этом множестве применить вычитание и умножение/деление (за исключением запрещенного деления на 0 ).



**Рис. 8.2.** Поле GF (5)

**Поля GF(p в степени n)**

В дополнение к полям **GF(p)** в криптографии мы также интересуемся полями GF(pn). Однако множества Z, Zn, Zn\* и Zp, которые мы использовали до сих пор с операциями сложения и умножения, не могут удовлетворить требованиям поля. Поэтому должны быть определены некоторые новые множества и некоторые новые операции на этих множествах.

**Полиномы**

Хотя мы можем непосредственно определить правила для операций сложения и умножения слов из двух бит, которые удовлетворяют свойства в **GF(2n),** проще работать с полиномиальным степени **n – 1** по битным представлением слов. **Полиномиальное** выражение степени **n – 1** имеет форму

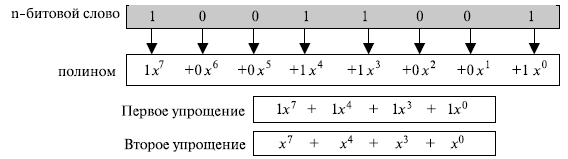
**f(x) = an-1xn-1 + an-2xn-2 + …… + a1x1 + a0x0**

где **xi** назван термином **i**-тый элемент, **ai** называется коэффициентом **i** - этого элемента. Хотя мы знаем полиномы в алгебре, но при представлении n -битовых слов полиномами необходимо следовать некоторым правилам:

1. Cтепень **x** определяет позицию бита в **n** битовых слов. Это означает, что крайний левый бит находится в нулевой позиции (связан с **x0** ), самый правый бит находится в позиции **n–l**(связан с **xn-l**);

2. Kоэффициенты сомножителей определяют значение битов. Каждый бит принимает только значение **0** или **1**, поэтому наши полиномиальные коэффициенты могут иметь значение **0** или **1**.

Использование полиномов для предоставления слова из **8 бит** **(10011001)** показано на [8](https://www.intuit.ru/studies/curriculums/4081/courses/408/lecture/9358?page=1#image.6.2).3.



**Рис. 8.3.** Представление 8-ми битового слова полиномом

Заметим, что элемент полностью пропущен, если его коэффициент равен **0**, и не пропущен только коэффициент, если это **1**. Также заметим, что элемент **x0** равен **1**.

**Пример.**

Чтобы найти слово на **8** битов, связанное с полиномом **X5+ X2+ X**, мы сначала восстановим пропущенные сомножители. Мы имеем **n = 8**, это означает *полином* степени **7**. Расширенный *полино*м имеет вид

**0X7 + 0X6 + 1X5 + 0X4 + 0X3 + 1X2 + 1X1 + 0X0**

Он связан со словом на **8** битов **00100110**.

**Операции**

Обратите внимание, что любая операция на полиномах фактически включает две операции: операции И коэффициентов двух полиномов. Другими словами, мы должны определить два поля: одно для коэффициентов и одно для полиномов. Коэффициенты равны **0** или **1** ; для этой цели мы можем использовать **GF(2)** -поле. Мы уже говорили о таком поле (см. пример 8.1). Для полиномов нам нужно поле **GF(2n),**которое мы коротко обсудим ниже.

**Полиномы, представляющие n-битовые слова, используют два поля: GF(2) и GF(2** n **)**.

**Модуль**

Перед определением операций на полиномах мы должны поговорить о полиномах-модулях. Сложение двух полиномов никогда не создает *полином*, выходящий из множества. Однако умножение двух полиномов может создать *полином* со степенью большей, чем **n – 1**. Это означает, что мы должны делить результат на модуль и сохранять только остаток, как мы сделали в модульной арифметике. Для множеств полиномов в **GF(2n)** группа полиномов степени **n** определена как модуль. Модуль в этом случае действует как *полиномиальное простое число*. Это означает, что никакие полиномы множества не могут делить этот *полином*. Простое полиномиальное число не может быть разложено в полиномы со степенью меньшей, чем **n**. Такие полиномы называются **неприводимые полиномы**. [Таблица](https://www.intuit.ru/studies/curriculums/4081/courses/408/lecture/9358?page=1#table.6.1)8.1 показывает примеры полиномов **1-5 степеней.**

Для каждого значения степени часто есть более чем один неразлагаемый *полином*, — это означает, что когда мы определяем наш **GF(2n),** мы должны объявить, какой неприводимый *полином* мы используем как модуль.

|  |  |
| --- | --- |
| Таблица 8.1. Список неприводимых полиномов | |
| **Степень** | **Неприводимый *полином*** |
| **1** | **(x+1)x** |
| **2** | **(x2+x+1)** |
| **3** | **(x3+x2+1)(x3+x+1)** |
| **4** | **(x4+x3+x2+x+1)(x4+x3+1)(x4+x+1)** |
| **5** | **(x5+x2+1) (x5+x3+x2+x+1) (x5+x4+x3+x+1) (x5+x4+x3+x2+1) (x5+x4+x2+x+1)** |

2.**Арифметические операции в Полях Галуатипа GF(2n) – 40 мин.**

**Сложение**

Теперь определим операцию сложения для полиномов с коэффициентом в GF(2). Операция сложения очень простая: мы складываем коэффициенты соответствующих элементов полинома в поле GF(2). Обратите внимание, что сложение двух полиномов степени n – 1 всегда дает *полином* со степенью n – 1 — это означает, что мы не должны использовать вычитание из модуля их результата.

**Пример.**

Произведем сложение ({x^5} + {x^2} + x) \oplus ({x^3} + {x^2} + 1) в **GF(28).** Мы используем символ \oplus для обозначения полиномиального сложения. Ниже показана процедура

0x^{7} + 0x^{6} + 1x^{5} + 0x^{4} + 0x^{3} + 1x^{2} + 1x^{1} + 0x^{0} \oplus 
\\
0x^{7} + 0x^{6} + 0x^{5} + 0x^{4} + 1x^{3} + 1x^{2} + 0x^{1} +1x^{0}
\\
\_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ \_ 
\\

\\
0x^{7} + 0x^{6} + 1x^{5} + 0x^{4} + 1x^{3} + 0x^{2} + 1x^{1} + 1x^{0}  \to   x^{5} + x^{3} + x + 1

В упрощенном полиноме (показан справа) сохранены элементы с коэффициентом 1 и удалены элементы с коэффициентом **0**. Кроме того, удалены совпадающие элементы обоих полиномов, а несовпадающие сохраняются. Другими словами, **x5, x3,x1** сохраняются, а **x2**, который является совпадающим в этих двух полиномах, удален.

**Пример.**

Поскольку сложение в GF(2) означает операцию *ИСКЛЮЧАЮЩЕЕ ИЛИ* (*XOR*), мы можем получить результат *ИСКЛЮЧАЮЩЕГО ИЛИ* для этих двух слов бит за битом. В предыдущем примере **x5+ x2+ x** есть **00100110**, или *полином*, и **x3 + x2 + 1** есть **00001101**. Результат — **00101011** или, в полиномиальном обозначении**, x5 + x3 + x + 1.**

**Аддитивный нейтральный элемент — тождество**. Аддитивный нейтральный элемент полинома — нулевой *полином* (*полином* со всеми коэффициентами, равными нулю), потому что, прибавляя этот *полином* к самому себе, в результате получаем нулевой *полином*.

**Аддитивная инверсия** полинома с коэффициентами в GF(2) — сам *полином*. Это означает, что операция вычитания та же самая, что и операция сложения.

**Сложение и операции вычитания на полиномах — та же самая операция.**

**Умножение**

Умножение в полиномах — сумма умножения каждого элемента одного полинома с каждым элементом второго полинома. Однако необходимо отметить три особенности.

Первая: умножение коэффициента проводится в поле **GF(2).**

Вторая: **умножение xi на xj дает результат xi+j.**

Третья: умножение может создать элементы со степенью большей, чем **n–1**, и это означает, что результат должен быть уменьшен с использованием полинома-модуля.

Сначала покажем, как умножить два полинома согласно вышеупомянутому определению. Позже будет дан более эффективный алгоритм, который может использоваться компьютерной программой.

**Пример.**

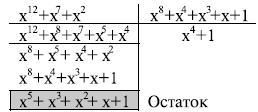
Найдите результат (x^{5} + x^{2} + x)\otimes (x^{7} + x^{4}+ x^{3} + x^{2} +x) в **GF(28)**с неразлагаемым полиномом **(x8 + x4+ x3+ x + 1).** Обратите внимание, что для обозначения умножения двух полиномов используется символ \otimes.

**Решение**

Сначала умножаем эти два полинома так, как мы это делали в обычной алгебре. Обратите внимание, что в этом процессе пара элементов с равной степенью удаляется. Например, результат **x9 + x9** полностью удален, потому что он нулевой *полином*, по причине, которую мы обсуждали раньше при рассмотрении операции сложения.

P_{1} \otimes  P_{2} = x^{5}(x^{7} + x^{4} + x^{3} + x^{2}  + x) + x^{2}(x^{7} + x^{4} + x^{3} + x^{2} + x) + x(x^{7} + x^{4}+ x^{3} + x^{2} + x)
\\
P_{1} \otimes  P_{2} = x^{12} + x^{9} + x^{8} + x^{7} + x^{6} + x^{9} + x^{6} + x^{5} + x^{4} + x^{3} + x^{8} + x^{5} + x^{4} + x^{3} + x^{2}
\\
 P_{1} \otimes  P_{2} = (x^{l2} +x^{7}+x^{2}) \mod (x^{8}+x^{4}+x^{3}+x+1) = x^{5}+x^{3}+x^{2}+x+1

Чтобы найти конечный результат, разделим *полином* степени **12** на *полином* степени **8** (модуль) и сохраним только остаток. Процесс деления тот же самый, что и в обычной алгебре, но мы должны помнить, что здесь вычитание то же самое, что и сложение. Рисунок 8.5 показывает процесс деления.

  
**Рис. 8.5.**Полиномиальное деление с коэффициентами в поле GF (2).

**Мультипликативное тождество** — всегда равно **1**. Например, в **GF(28)** мультипликативная *инверсия* — в побитном изображении **00000001**.

**Мультипликативная инверсия**. Поиск мультипликативной *инверсии* требует привлечения расширенного *алгоритма Евклида*. *Алгоритм Евклида* должен быть применен к модулю и полиному, выполнение алгоритма является таким же, как и для целых чисел.

**Пример.**

**В GF(24)найдите *инверсию* (x2 + 1) mod (x4+ x + 1).**

Решение

Мы используем расширенный евклидов алгоритм, как это показано в [таблице 8.2](https://www.intuit.ru/studies/curriculums/4081/courses/408/lecture/9358?page=2#table.6.2):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Таблица 8.2. *Алгоритм Евклида* . | | | | | | |
| **q** | **rj** | **r2** | **r** | **tj** | **t2** | **t** |
| **x2+1** | **(x4+x+1)** | **(x2+1)** | **(x)** | **(0)** | **(1)** | **(x2+1)** |
| **(x)** | **(x2+1)** | **(x)** | **(1)** | **(1)** | **(x2+1)** | **(x3+x+1)** |
| **(x)** | **(x)** | **(1)** | **(0)** | **(x2+1)** | **(x3+x+1)** | **(x4+x+1)** |
|  | **(1)** | **(0)** |  | **(x3+x+1)** | **(0)** |  |

Это означает, что **(x2 + 1)-1mod (x4+ x + 1)**есть**(x3+ x + 1**). Ответ может быть проверен просто: надо перемножить эти два полинома и найти остаток. В этом случае результат деления на модуль равен

[(x^{2} + 1) \otimes  (x^{3} + x + 1)]  \mod (x^{4} + x + 1) = 1

**Пример.**

**В GF(28)найдите *инверсию* (x5) mod (x8 + x4+ x3+ x + 1).**

Решение

Будем использовать расширенный евклидов алгоритм, как это показано в[Таблице 8.3](https://www.intuit.ru/studies/curriculums/4081/courses/408/lecture/9358?page=2#table.6.3):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Таблица 8.3. Евклидов алгоритм для примера 6.8 | | | | | | |
| **q** | **rj** | **r2** | **r** | **T1** | **t2** | **t** |
| **(x3)** | **(x8+x4+x3+x+1)** | **(x5)** | **(x4+x3+x2+x+1)** | **(0)** | **(1)** | **(x3)** |
| **(x+1)** | **(x5)** | **(x4+x3+x+1)** | **(x3+x2+1)** | **(1)** | **(x3)** | **(x4+x3+1)** |
| **(x)** | **(x4+x3+x+1)** | **(x3+x2+1)** | **(1)** | **(x3)** | **(x4+x3+1)** | **(x5+x4+x2+x)** |
|  | **(x3+x2+1)** | **(1)** | **(0)** | **(x4+x3+1)** | **(x5+x4+x2+x)** | **(0)** |
|  | **(1)** | **(0)** |  | **(x5+x4+x2+x)** | **(0)** |  |

Это означает, что**(x5)-1mod (x8+ x4+ x3+ x + 1)** есть**(x5+ x4+ x2+ x).**

Результат может быть легко проверен умножением этих двух полиномов и определением остатка деления по модулю.

[(x^{5}) \otimes  (x^{5}+x^{4}+x^{3}+x)] \mod (x^{8}+x^{4}+x^{3}+x+1) =1

**Заключение – до 5 мин.**

Методическиерекомендации:

- обобщитьнаиболееважные, существенныевопросылекции;

- сформулироватьобщиевыводы;

- поставитьзадачидлясамостоятельнойработы;

- ответитьнаопросыстудентов.

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

\_\_\_\_\_\_\_\_\_\_\_\_ /Дедов О.П./