МЕТОДИЧЕСКАЯ РАЗРАБОТКА
для проведения лекции

Занятие № 1: «Элементы теории чисел в криптографии»

Учебные вопросы:
1. Основы модулярной арифметики
2. Односторонние функции в криптографии
Заключительная часть

Введение

Использование криптографической защиты информации в современных цифровых технологиях представляется неотъемлемой частью многих сфер жизни общества, причем этот процесс становится все более масштабным.

Интенсивное развитие инфокоммуникационных технологий и расширение круга пользователей телекоммуникационных и информационных систем еще больше актуализировали проблему защиты информации и значительно повлияли на пути дальнейшего развития криптографических систем.

На сегодняшний момент невозможно представить полноценную защиту информации без криптографических аспектов, поэтому изучение основ криптографической защиты информации необходимо для успешной профессиональной деятельности специалистов.

В лекции будут рассмотрены основные сведения о математических основах криптографии.

Учебные вопросы:

Вопрос 1. Основы модулярной арифметики.

В обычной жизни обычно пользуются позиционной системой счисления, согласно которой значение каждого числового знака (цифры) в записи числа зависит от его позиции (разряда). Однако существуют и непозиционные системы счисления, к одной из которых относится система остаточных классов (СОК) (англ. *Residue Number System – RNS*), являющаяся основой модулярной арифметики. Представление числа в СОК предполагает, что целое число представлено вычетами (остатками) по модулям из множества попарно взаимно простых чисел.

Вычет числа a по модулю n обозначается как $a \bmod n$.

Два числа называют *взаимно простыми*, если у них нет общих множителей, кроме 1. Иными словами, если наибольший общий делитель (НОД) чисел a и n равен 1.

Наиболее известный пример модулярной арифметики – запись времени в 12-часовом формате. Например, если на часах 09:00, то через 4 часа на часах будет 01:00 (рис. 1).

Аналогично для арифметики по модулю 12:

$$(10 + 13) \bmod 12 = 23 \bmod 12 = 11 \bmod 12.$$

Пусть a и n – натуральные числа. Разделить число a на число n с остатком – значит найти целые числа q и r, удовлетворяющие условию

$$a = q \cdot n + r, \text{ где } 0 \le r < n.$$

При этом число q называют неполным частным, а r – остатком от деления числа a на число n.

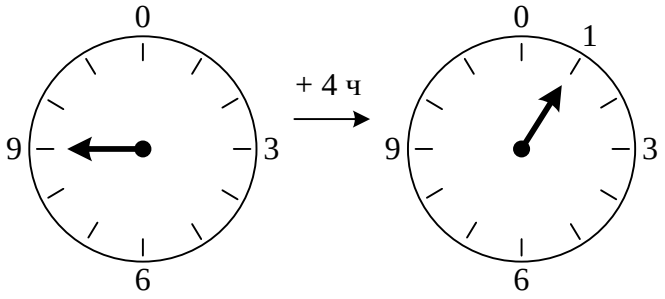

Рис. 1. Пример модулярной арифметики для 12-часового формата времени

Целые числа a и b называют *сравнимыми по модулю n*, если их остатки при делении на n совпадают. Обычно для обозначения этого факта используется запись

$$a \equiv b (\bmod n).$$

Множество целых чисел $a_0, a_1, \ldots, a_{n-1}$ таких, что для любого целого числа b найдется $k \in \{0, \ldots, n-1\}$ со свойством $a_k \equiv b \bmod n$, называется *полной системой вычетов* по модулю n (или СОК).

Свойства сравнений:

1) рефлексивность: $a \equiv a \pmod m$;

2) симметричность: $a \equiv b \pmod m \equiv b \equiv a \pmod m$;

3) транзитивность: $a \equiv b \pmod m$, $b \equiv$ c $\pmod m \equiv a \equiv c \pmod m$;

4) если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, то $a + c \equiv b + d \pmod m$;

5) если $a \equiv b \pmod m$, $m = m' \cdot d$, то $a \equiv b \pmod d$;

6) если $a \equiv b \pmod m$, $a \equiv b \pmod n$, то $a \equiv b \pmod{m \cdot n}$.

В криптографии применяются теоремы Эйлера и Ферма.

Теорема Эйлера в теории чисел гласит, если a и n взаимно простые числа, то

$$a^{\varphi(n)} \equiv 1 \pmod n,$$

где $\varphi(n)$ – функция Эйлера.

Функция Эйлера $\varphi(n)$ – мультипликативная арифметическая функция, равная количеству натуральных чисел, меньших n и взаимно простых с ним.

Для простого числа n функция Эйлера определяется формулой

$$\varphi(n) = n - 1.$$

Для составного числа n, представляемого произведением неодинаковых простых чисел p и q ($n = p \cdot q$), функция Эйлера определяется формулой (свойством мультипликативности)

$$\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p - 1) \cdot (q - 1).$$

Для любого составного числа n, которое можно представить в виде произведения различных простых чисел $p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, функция Эйлера определяется формулой

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right).$$

Например, $\varphi(60) = 60 \cdot (1 - 1/2) \cdot (1 - 1/3) \cdot (1 - 1/5) = 16$ или $\varphi(60) = (2^2 - 2^1) \cdot (3^1 - 3^0) \cdot (5^1 - 5^0) = (4-2) \cdot (3-1) \cdot (5-1) = 16$.

Частным случаем теоремы Эйлера является малая теорема Ферма, согласно которой если p – простое число, a – целое число, удовлетворяющее сравнению $a^p \equiv a \pmod p$ и не делящееся на p (т. е. если НОД(a, p) = 1), то

$$a^{p-1} \equiv 1 \pmod p.$$

Данная теорема стала одной из главных теорем для исследований в теории целых чисел, криптографии и других областях.

В арифметике действительных чисел нетрудно вычислить мультипликативную обратную величину a^{-1} для ненулевого a:

$$a^{-1} = 1 / a, \text{ т. е. } a \cdot a^{-1} = 1.$$

Например, мультипликативная обратная величина от числа 4 равна ¼, поскольку $4 \cdot ¼ = 1$.

В модулярной же арифметике вычисление обратной величины является более сложной задачей. Например, решение сравнения $4 \cdot x \equiv 1 \pmod 7$ эквивалентно нахождению таких значений x и k, при которых $4 \cdot x \equiv 7 \cdot k + 1$, где x и k – целые числа.

Общая формулировка этой задачи – нахождение такого целого числах x, при котором

$$a \cdot x \pmod n \equiv 1 \text{ или } a^{-1} \equiv x \pmod n.$$

Решение такой задачи существует не всегда. Например, обратная величина для числа 5 по модулю 14 равна 3, так как

$$5 \cdot 3 = 15 \equiv 1 \pmod{14}.$$

Однако число 2 не имеет обратной величины по модулю 14.

Сравнение $a^{-1} \equiv x \pmod n$ имеет единственное решение, только если a и n – взаимно простые числа.

Основные способы нахождения обратной величины a^{-1}:

1. Проверить поочередно значения 1, 2, …, $n - 1$, пока не будет найдена $a^{-1} \equiv 1 \pmod n$ такая, при которой $a \cdot a^{-1} \pmod n \equiv 1$.

2. Если известна функция Эйлера $\varphi(n)$, то, используя алгоритм быстрого возведения в степень, можно вычислить

$$a^{-1} \pmod n \equiv a^{\varphi(n)-1} \pmod n.$$

Например, пусть $n = 7$, $a = 5$. Надо найти $x = 5^{-1} \pmod 7$.

Так как число 7 – простое, то $\varphi(7) = 7 - 1 = 6$, тогда

$$5^{-1} \pmod 7 = 5^{6-1} \pmod 7 = 5^5 \pmod 7 = (5^2 \pmod 7) \cdot (5^3 \pmod 7) =$$
$$= (25 \pmod 7) \cdot (125 \pmod 7) \pmod 7 = (4 \cdot 6) \pmod 7 = 24 \pmod 7 = 3.$$

3. Если функция Эйлера неизвестна, то можно использовать расширенный алгоритм Евклида, который эффективно определяет НОД двух чисел a и b.

При вычислении НОД двух чисел можно попутно получить такие целые числа u и v , для которых

$$a \cdot u + b \cdot v = \text{НОД}(a, b).$$

Полученное выражение при НОД(a, b) = 1 называется Диофантовым уравнением первой степени и решается с помощью расширенного алгоритма Евклида.

Например, определим НОД(221, 19) по алгоритму Евклида:

$$221 = 19 \cdot 11 + 12;$$
$$19 = 12 \cdot 1 + 7;$$
$$12 = 7 \cdot 1 + 5;$$
$$7 = 5 \cdot 1 + 2;$$
$$5 = 2 \cdot 2 + 1;$$
$$2 = 1 \cdot 2.$$

Затем, поднимаясь по строкам этого алгоритма вверх, получаем необходимое представление:

$$\text{НОД}(221, 19) = 1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 5 \cdot 1) = 5 - 2 \cdot 7 + 2 \cdot 5 = 3 \cdot 5 - 2 \cdot 7 =$$
$$= 3\,(12 - 7 \cdot 1) - 2 \cdot 7 = 3 \cdot 12 - 3 \cdot 7 - 2 \cdot 7 = 3 \cdot 12 - 5 \cdot 7 =$$
$$= 3 \cdot 12 - 5 \cdot (19 - 12 \cdot 1) = 3 \cdot 12 - 5 \cdot 19 + 5 \cdot 12 = 8 \cdot 12 - 5 \cdot 19 =$$
$$= 8 \cdot (221 - 19 \cdot 11) - 5 \cdot 19 = 8 \cdot 221 - 88 \cdot 19 - 5 \cdot 19 = 8 \cdot 221 - 93 \cdot 19.$$

Таким образом, получаем $u = 8$ и $v = -93$.

Данное свойство алгоритма Евклида широко используется для нахождения обратных величин по модулю:

$$a \cdot u + b \cdot v = \text{НОД}(a, b) = 1.$$

Если в данном выражении принять за модуль число v, то $b \cdot v = 0 \bmod v$ и тогда $a \cdot u = 1 \bmod v$, а, следовательно, $u = a^{-1}$.

Аналогично и другое утверждение: если принять за модуль число u, то $a \cdot u = 0 \bmod u$ и $b \cdot v = 1 \bmod u$, следовательно, $v = b^{-1}$.

Применительно к приведенному примеру $221 \cdot 8 = 0 \bmod 8$, $19 \cdot (-93) = 1 \bmod 8$, $19 \cdot (-93) \bmod (-93) = 0$, $221 \cdot 8 = 1 \bmod (-93)$.

Модулярная арифметика базируется на «китайской теореме об остатках», которая формулируется следующим образом.

Если некоторое неотрицательное число $x < M$, не превосходящее произведения взаимно простых модулей $M = \prod p_i$, представлено в виде остаточных классов взаимно простых модулей $p_1, p_2, \ldots, p_k$

$$x = a_1 \bmod p_1;$$
$$x = a_2 \bmod p_2;$$
$$\ldots\ldots\ldots\ldots$$
$$x = a_k \bmod p_k,$$

то число x может быть однозначно восстановлено по формуле

$$x = \sum a_i \cdot N_i \cdot M_i \ (\bmod M),$$

где N_i – обратный элемент к M_i по модулю p_i;

$M_i = M / p_i$ – произведение всех модулей, кроме p_i.

Например, необходимо решить систему из двух сравнений:

$$x = 1 \bmod 5;$$
$$x = 10 \bmod 11.$$

Здесь $p_1 = 5$, $p_2 = 11$, $M = 5 \cdot 11 = 55$, $a_1 = 1$, $a_2 = 10$, $M_1 = M / p_1 = p_2 = 11$, $M_2 = M / p_2 = p_1 = 5$.

Значения обратных элементов N_1 и N_2 определяются как

$$M_1 \cdot N_1 \equiv 1 \bmod p_1,\ 11\ N_1 \equiv 1 \bmod 5 \rightarrow N_1 = 1;$$
$$M_2\ N_2 \equiv 1 \bmod p_2,\ 5\ N_2 \equiv 1 \bmod 11 \rightarrow N_2 = 9.$$

Тогда

$$x = (a_1 \cdot M_1 \cdot N_1 + a_2 \cdot M_2 \cdot N_2) \bmod M = (1 \cdot 11 \cdot 1 + 10 \cdot 5 \cdot 9) \bmod 55 =$$
$$= (11 + 450) \bmod 55 = 461 \bmod 55 = 21 \bmod 55.$$

Приведенные основы модулярной арифметики, когда элементами конечных полей (полей Галуа) были целые числа, справедливы и для элементов конечного поля в виде полиномов.

В частности, перемножение полиномов степени не выше n с элементами поля $GF(p^n)$ равно остатку от деления произведения полиномов на неприводимый полином $f(x)$ степени n.

Таким образом, приведенный по модулю $f(x)$ многочлен по определению равен остатку от деления этого многочлена на $f(x)$.

Например, для поля $GF(2^3)$, неприводимого полинома

$$f(x) = x^3 + x + 1$$

и элементов поля в виде полиномов

$$a = x^2 + x;$$
$$b = x^2 + x + 1$$

результат перемножения элементов поля примет вид

$$a \cdot b = x^4 + x.$$

Результат деления произведения полиномов $a \cdot b$ на неприводимый полином $x^3 + x + 1$ есть полином $-x^2$. Аналогично выполняются и все остальные операции с элементами конечного поля в виде полиномов. Нахождение НОД двух полиномов и определение полинома, обратного заданному, можно осуществить по расширенному алгоритму Евклида, как и для целых чисел.

Преимущество модулярного представления состоит в том, что арифметические операции могут быть реализованы с меньшими вычислительными затратами, чем при обычном представлении, так как вычисления выполняются независимо для каждого модуля.

Вопрос 2. Односторонние функции в криптографии.

Особую роль в криптографии играют однонаправленные функции (ОНФ), которые в общем случае не являются биективными.

Однонаправленной функцией (*односторонней функцией*, англ. *One-Way Function*) называется отображение множества всех слов конечной длины n над конечным алфавитом, для которого существует такое $\alpha < \infty$, что образ любого слова длины n можно вычислить за $O(n^{\alpha})$ операций, но ни для какого $\beta < \infty$ не существует алгоритма, вычисляющего для любого слова длины n его прообраз за $O(n^{\beta})$ операций.

Упрощенное определение ОНФ – такая функция f, что для каждого $x \in X$ вычислительно просто определить значение функции $y = f(x)$, но для всех $y \in Y$ вычислительно невозможно отыскать любой x, такой, что $f(x) = y$.

Существование ОНФ до сих пор является недоказанной гипотезой. Однако современная асимметричная криптография основывается на предположении, что односторонние функции существуют.

Теоретически по известному значению $y = f(x)$ найти x можно всегда, проверяя по очереди все возможные значения x до тех пор, пока соответствующее значение $f(x)$ не совпадет с заданным y. Однако практически при значительной размерности множества X такой подход неосуществим.

Принципиальным условием однонаправленности функции является сложность (невозможность) вычисления обратного преобразования, т. е. отсутствие эффективных алгоритмов нахождения по значению функции значения аргумента. Обратное преобразование к ОНФ может существовать, но не являться функцией в смысле определения. Обратное преобразование может быть также неоднозначным, т. е. практически для всех y из области значений Y функции невозможно отыскать единственное значение x, такое, что $f(x) = y$. Неоднозначность обратного преобразования означает, что допустимых значений $x \in X$ может быть множество и каждое из них удовлетворяет уравнению $y = f(x)$.

Для выяснения неоднозначности обратного преобразования конкретной функции необходимо убедиться, что выполнение прямого и обратного преобразований не обеспечивает взаимно однозначного соответствия между элементами множеств X и Y. Примером существования неоднозначных обратных преобразований является функция $y = x^2$, для которой каждому образу $y \in Y$ (исключая $y = 0$) соответствуют два отличающиеся друг от друга прообраза x_i и x_j: $x_i = \sqrt{y}$ и $x_j = -\sqrt{y}$.

Для построения криптографических систем защиты информации используются однонаправленные функции, для которых обратное преобразование существует и однозначно, но вычислительно нереализуемо. Такие ОНФ называются *вычислительно необратимыми функциями*.

Примером однонаправленной функции $y = f(x)$ является широко известная функция дискретного возведения в степень:

$$y = a^x (\mathrm{mod}\ p),$$

где x – целое число от 1 до $p-1$ включительно, а вычисление производится по модулю p;

p – очень большое простое число;

a – целое число ($1 < a < p$), степени которого a^1, a^2, …, a^{p-1}, взятые по mod p, равняются в некотором порядке числам 1, 2, ..., $p-1$ (значения a называются *примитивными элементами*).

Например, для простого $p = 7$ можно выбрать примитивный элемент $a = 3$, так как $a^1 (\mathrm{mod}\ 7) = 3$, $a^2 (\mathrm{mod}\ 7) = 2$, $a^3 (\mathrm{mod}\ 7) = 6$, $a^4 (\mathrm{mod}\ 7) = 4$, $a^5 (\mathrm{mod}\ 7) = 5$, $a^6 (\mathrm{mod}\ 7) = 1$.

Функция вида $y = a^x \bmod p$ вычисляется сравнительно просто, а обратная к ней функция вида $x = \log_a y \bmod p$ является вычислительно сложной практически для всех $1 < y < p$ при условии, что p велико. Задача вычисления обратного преобразования к приведенной функции называется *задачей дискретного логарифмирования*. Оценки временной и емкостной сложности алгоритмов нахождения дискретных логарифмов свидетельствуют об субэкспоненциальной вычислительной сложности их выполнения, и при значениях p длиною тысячи бит данные алгоритмы на сегодняшний момент вычислительно не реализуемы.

Другим примером однонаправленной функции является $f(x, y) = x \cdot y$. Задача вычисления обратного преобразования к приведенной функции называется *задачей факторизации целых чисел* (разложением на сомножители).

Еще одним важным классом функций, используемых при построении несимметричных криптосистем, являются *однонаправленные функции с потайным ходом*, или *функции с секретом* (англ. *Trapdoor Function*).

Функция f_z относится к классу однонаправленных функций с потайным ходом, если она является однонаправленной функцией с дополнительным свойством, таким, что зная информацию z о потайном ходе вычислительно просто определить значение $x \in X$, удовлетворяющее уравнению $y = f_z(x)$, однако без знания информации z нахождение отображения $y = f_z^{-1}(x)$ вычислительно не реализуемо. Поэтому информация z может служить секретным ключом для функций с потайным ходом.

Заключительная часть
– напомнить изученные вопросы и цели занятия;
– подвести итоги занятия, определить полноту достижения целей занятия.

Контрольные вопросы

1. Понятие системы остаточных классов.
2. Теорема Эйлера.
3. Малая теорема Ферма.
4. Способы нахождения обратной величины.
5. Понятие однонаправленной функции.
6. Примеры однонаправленных функций.
7. Понятие примитивного элемента.
8. Однонаправленные функции с потайным ходом.

Рекомендованная литература:

1. Рябко, Б. Я. Криптографические методы защиты информации : учебное пособия для вузов / Б. Я. Рябко, А. Н. Фионов. – Москва : Горячая линия – Телеком, 2012. – 229 с.

2. Фомичев, В. М. Криптографические методы защиты информации. В 2 ч. Ч.1 : Математические аспекты : учебник для академического бакалавриата

/ В. М. Фомичев, Д. А. Мельников; под ред. В. М. Фомичева. – Москва : Юрайт, 2017. – 209 с.

3. Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. – Москва : Юрайт, 2016. – 473 с.