Лекция 4. СТАНДАРТ AES. АЛГОРИТМ RIJNDAEL.

Стандарт AES (Advanced Encryption Standard) представляет собой новый стандарт шифрования с одним ключом, который заменил стандарт DES. Алгоритм Rijndael (рейн-дал) стал победителем конкурса на создание нового стандарта шифрования и был выбран для стандарта AES. Он представляет собой еще один алгоритм, не использующий сетей Фейстела. Для того, чтобы описать этот алгоритм нам понадобятся некоторые сведения из теории полей Галуа и их расширений, которые и рассматриваются ниже.

Некоторые сведения из теории полей Галуа

Введем некоторые определения.

Группой называется множество элементов с определенной для каждой пары элементов операцией (сложение или умножение), для которой справедливы следующие аксиомы:

1. Группа замкнута по определенной на ней операции, т.е. для любых элементов группы a, b элемент $c = a * b$ тоже принадлежит группе. Здесь $*$ обозначает операцию, определенную на группе.
2. Ассоциативность. Для любых a, b, c, принадлежащих группе выполняется $(a * b) * c = a * (b * c)$
3. В группе существует единичный элемент e такой, что $a * e = e * a = a$. Если групповая операция – это сложение, то e – ноль группы, если операция – умножение, то e – это единица группы.
4. Существует обратный элемент a^{-1} для каждого элемента a группы, т.е. $a^{-1} * a = e$.

Группа называется ***коммутативной*** или ***абелевой***, если для ее элементов выполняется $a * b = b * a$.

Если групповая операция $*$ это умножение, то группа называется мультипликативной. Если $*$ – это сложение, то группа называется аддитивной.

Примеры: целые числа относительно сложения, положительные рациональные числа относительно умножения – это группы с бесконечным числом элементов. Двухэлементное множество $\{0,1\}$ относительно операции сложения по модулю два образует группу с конечным числом элементов.

Кольцо – это абелева группа, наделенная дополнительными свойствами. ***Кольцом*** R называется множество с двумя, определенными на нем операциями. Первая называется сложением, вторая умножением. При этом имеют место следующие аксиомы:

1. Относительно сложения (+) кольцо является абелевой группой.
2. Замкнутость относительно операции умножения: для любых a и b из кольца $c = ab$ тоже принадлежит кольцу.
3. Дистрибутивность: $a(c + b) = ac + ab$
4. Ассоциативность: $a(bc) = (ab)c$

Коммутативным называется кольцо, для которого выполняется $ab = ba$ для любых элементов a и b, принадлежащих кольцу.

Операция сложения в кольце, очевидно, имеет единичный элемент, называемый нулем. Операция умножения не обязательно имеет единичный элемент. Кольцо, обладающее единичным элементом по умножению, называется кольцом с единицей. Если единичный элемент по умножению существует, то он – единственный и обозначается символом 1. Тогда для всех a из кольца имеет место $1a = a1 = a$. Относительно операции сложения каждый элемент имеет обратный. Относительно операции умножения элемент обратный данному элементу не обязательно существует, но в кольце с единицей обратные элементы могут существовать. Например, множество вещественных чисел образует коммутативное кольцо с единицей относительно обычных операций сложения и умножения. Множество всех целых чисел (включая положительные, отрицательные и нуль), образует коммутативное кольцо с единицей.

Нестрого говоря, абелевой группой является множество, в котором можно складывать и вычитать, а кольцом – множество, в котором можно складывать, вычитать и умножать. Более сильной алгебраической структурой, называемой полем, является множество, в котором можно складывать, вычитать, умножать и делить.

Полем называется алгебраическая структура, для которой справедливы следующие аксиомы:

1. Поле – это коммутативное кольцо с единицей по умножению.
2. Для любого ненулевого элемента поля a существует обратный элемент a^{-1} такой, что $aa^{-1} = 1$.

Например, множество вещественных чисел представляет собой поле. Множество рациональных чисел тоже представляет собой поле. Эти поля содержат бесконечное число элементов. Далее мы будем рассматривать только поля с конечным числом элементов.

Поле с p элементами, если оно существует (а оно существует не при всех p), называется ***конечным полем*** или ***полем Галуа*** и обозначается через $GF(p)$. Наименьшее поле состоит из двух элементов 0 и 1 при следующих правилах выполнения операций сложения и умножения:

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Это поле GF(2). Можно показать, что для любого ***простого*** p существует поле, содержащее p различных элементов. Таким полем является числовое поле с элементами $\{0,1,2,\ldots,p-1\}$, операции сложения и умножения в котором выполняются по модулю p.

Пример. Пусть $p=5$. Элементами поля являются 0,1,2,3,4. Таблицы сложения и умножения имеют вид

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Примитивным элементом поля $GF(p)$ называется такой элемент α, что первые $p-1$ степеней этого элемента задают все ненулевые элементы поля. Например, в поле $GF(5)$ получаем $2^1=2$, $2^2=4$, $2^3=3$, $2^4=1$. Таким образом 2 является примитивным элементом поля $GF(5)$. Говорят, что примитивный элемент имеет порядок $p-1$. Для примитивного элемента α справедливо, что $\alpha^{p-1}=1$. В общем случае порядок элемента это такое наименьшее целое положительное число, что элемент, возведенный в степень равную этому числу, дает 1. Порядок любого элемента β является делителем порядка примитивного элемента, т.е. $p-1$.

Например, $4^1 = 4$, $4^2 = 1$, порядок элемента 4 равен 2, $p-1=4$. Очевидно, что $\beta^{p-1} = 1$.

Пусть теперь $q = p^m$, где $p-$ простое, а $m-$ положительное целое. Можно показать, что при числе элементов $q = p^m$, $m > 1$, множество чисел $\{0,\dots q-1\}$ не является полем. Рассмотрим пример. Пусть $q = 2^2$. Зададим таблицы сложения и умножения вида

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Нетрудно видеть, что элемент 2 не имеет обратного по умножению, т.е. структура является кольцом, но не полем. Однако, поле из четырех элементов $GF(4)$ можно построить. Алгебраическая структура поля $GF(p^m)$ вытекает из рассмотрения кольца многочленов переменной x с коэффициентами из поля $GF(p)$ по модулю некоторого многочлена $p(x)$ степени m. Говорят, что полином $a(x) = b(x) \bmod p(x)$, если $b(x) = a(x) + Q(x)p(x)$, где $Q(x)$ - некоторый многочлен.

Известно, что кольцо многочленов с коэффициентами из поля $GF(p)$ по модулю некоторого многочлена $p(x)$ степени m является полем тогда и только тогда, когда многочлен $p(x)$ неприводим, т.е. не может быть разложен на множители с коэффициентами из этого поля. Число элементов этого поля равно p^m. Если корнем неприводимого многочлена является примитивный элемент поля $GF(p^m)$, то такой многочлен называется примитивным, а порождаемое им поле содержит p^m различных элементов, а каждый элемент может быть представлен в виде линейной комбинации m степеней примитивного элемента. Заметим, что рассмотренное поле называют ***полем характеристики*** p, т.к. коэффициенты полиномов принадлежат $GF(p)$ и, соответственно, все операции над ними выполняются по модулю p.

Пример. Выберем примитивный полином $p(x) = x^2 + x + 1$. Тогда элементами поля $GF(2^2)$ будут полиномы:

$$0,\ 1,\ x,\ x^2 = x + 1.$$

Для выполнения операции сложения элементы поля удобно представлять в виде векторов длины m, т.е., в данном примере, в виде последовательностей 00, 01, 10, 11. Сложение полиномов сводится к покомпонентной сумме по модулю два соответствующих последовательностей. Еще одно представление элементов поля можно получить, используя примитивный элемент поля α. Неприводимый полином $p(x)$ в нашем примере является также примитивным полиномом и примитивный элемент поля α - это его корень. Другими словами, α удовлетворяет соотношению $\alpha^2 = \alpha + 1$. Все ненулевые элементы поля могут быть получены как степени примитивного элемента, т.е.

$$\alpha^0 = 1,\ \alpha^1 = \alpha,\ \alpha^2 = \alpha + 1.$$

Нетрудно видеть, что два представления элементов поля эквивалентны с точностью до замены переменной. Представление элементов поля в виде степеней примитивного элемента обычно используется для умножения в этом поле. Порядок примитивного элемента равен $p^m - 1$. В нашем примере $\alpha^3 = \alpha^2 + \alpha = 1$.

Заметим, что порядок любого элемента поля является делителем порядка примитивного элемента, т.е. числа $p^m - 1$. Следовательно, для любого элемента β имеет место тождество $\beta^{p^m-1} = 1$. Если $\left(p^m - 1\right)$ - простое число, то все ненулевые элементы поля (кроме 1) примитивны, в противном случае в поле найдутся элементы, имеющие порядки делящие число $\left(p^m - 1\right)$. Например, в поле $GF\left(2^4\right)$ существуют элементы порядка 1, 3, 5, 15.

Найдем обратный элемент к элементу $x+1$. Так как $x(x+1) = x^2 + x = 1$, то обратным элементом к $x+1$ будет x.

Для нахождения обратного к данному элементу в поле Галуа или его расширении используют алгоритм деления Евклида. Рассмотрим вначале алгоритм деления Евклида для целых чисел и обсудим, как он может быть применен для нахождения обратного элемента в поле Галуа $GF(p)$, где p – простое. Суть алгоритма Евклида состоит в нахождении наибольшего общего делителя (НОД) двух целых положительных чисел (a_0, a_1), $a_0 \geq a_1$ путем вычисления последовательности остатков

$$a_{i+1} = a_{i-1} - Q_i a_i,\ i = 1,2,\ldots,k \qquad (1)$$

где $Q_i = \left[\frac{a_{i-1}}{a_i}\right]$, $[\cdot]$ обозначает целую часть. Вычисления прекращаются, когда остаток $a_{k+1} = 0$, что означает, что a_k делит нацело a_{k-1}. Тогда НОД$(a_0, a_1) = a_k$. Так называемый расширенный алгоритм Евклида позволяет находить не только НОД

двух целых положительных чисел, но и его представление в виде $НОД(a_0, a_1) = xa_0 + ya_1$, где x, y - это целые (необязательно положительные) числа. Для нахождения x, y алгоритм Евклида модифицируется следующим образом:

1. Инициализация $x_0 = 1$, $x_1 = 0$, $y_0 = 0$, $y_1 = 1$, $i = 1$
2. $Q_i = \left[\frac{a_{i-1}}{a_i} \right]$
3. $a_{i+1} = a_{i-1} - Q_i a_i$
4. Если a_{i+1}=0, то $НОД(a_0, a_1) = a_i$, $x = x_i$, $y = y_i$ и закончить вычисления, иначе

$$x_{i+1} = x_{i-1} - Q_i x_i$$

$$y_{i+1} = y_{i-1} - Q_i y_i$$

$$i = i + 1$$

Перейти к шагу 2.

Пример. Найдем НОД(57,33) и его разложение $НОД(57,33) = x \cdot 57 + y \cdot 33$. Результаты вычислений сведены в таблицу

i	a_i	Q_i	x_i	y_i
0	57	—	1	0
1	33	[57/33]=1	0	1
2	57–1×33=24	[33/24]=1	1–1×0=1	0–1×1=–1
3	33–1×24=9	[24/9]=2	0–1×1=–1	1–1×(–1)=2
4	24–2×9=6	[9/6]=1	1–2×(–1)=–1	–1–2×2=–5
5	9–1×6=3	[6/3]=2	–1–1×3=–4	2–1×(–5)=7
6	6–2×3=0	НОД(57,33)=3 3=57×(–4)+33×7		

Таким образом, получаем, что $НОД(57,33) = 3 = 57 \cdot (-4) + 33 \cdot 7$

Нахождение обратного элемента в поле Галуа и его расширении.

Теперь рассмотрим, как расширенный алгоритм Евклида может быть применен для нахождения обратного элемента к заданному в $GF(p)$. Пусть a –некоторый элемент поля $GF(p)$, тогда обратный к нему элемент a^{-1}, очевидно, удовлетворяет уравнению

$$aa^{-1} = 1 \bmod p \ . \qquad (2)$$

Уравнение (2) эквивалентно уравнению

$$aa^{-1} + py = 1, \qquad (3)$$

где y– некоторое целое число. Тогда с помощью расширенного алгоритма Евклида мы находим $НОД(p,a) = 1 = x \cdot a + y \cdot p$, где $x = a^{-1}$. Например, пусть $p = 5$, $a = 3$. Получаем

$$a_2 = 5 - 1 \cdot 3 = 2$$

$$x_2 = 1 - 0 \cdot 1 = 1$$

$$y_2 = 0 - 1 \cdot 1 = -1$$

$$a_3 = 3 - 1 \cdot 2 = 1$$

$$x_3 = 0 - 1 \cdot 1 = -1$$

$$y_3 = 1 - 1 \cdot (-1) = 2$$

Таким образом, имеем $1 = (-1) \cdot 5 + 2 \cdot 3$, т.е. $a^{-1} = 2$.

Расширенный алгоритм Евклида легко обобщается для полиномов и может быть использован для нахождения обратного элемента в расширении поля Галуа $GF(p^m)$.

Теорема. Пусть $r_0(x)$ и $r_1(x)$ – два полинома, причем $\deg(r_0(x)) \geq \deg(r_1(x))$, тогда существуют такие два полинома $U(x)$ и $V(x)$, что имеет место равенство

$НОД(r_0(x), r_1(x)) = U(x)r_0(x) + V(x)r_1(x)$ и $\deg(U(x))$ и $\deg(V(x)) < \deg(r_0(x))$.

Рассмотрим снова поле $GF(2^2)$, построенное по модулю полинома $p(x) = x^2 + x + 1$. Найдем элемент обратный к элементу x. Положим $r_0(x) = p(x)$ и

$r_1(x) = x$. Аналогично рассмотренным выше примерам, выполним следующие вычисления

$$r_2(x) = x^2 + x + 1 - (x+1)x = 1$$

$$U_2(x) = 1 - (x+1) \cdot 0 = 1$$

$$V_2(x) = 0 - (x+1) \cdot 1 = x + 1$$

Таким образом, получаем, что $НОД(p(x), x) = 1 = 1 \cdot (x^2 + x + 1) + (x+1) \cdot x$, т.е. обратным к элементу x является $(x+1)$. Заметим, что, так как рассматриваемое поле является расширением поля $GF(2)$, то все поразрядные операции между векторами (коэффициентами полиномов) выполняются по модулю 2 и, следовательно, в данном поле имеет место равенство $-1 = 1$.