Доп. Дисциплины

Магистры весна 2021

Занятие 7

МАТЕМАТИЧЕСКИЙ АНАЛИЗ ШИФРА AES

22.04.2021

ВТОРОЕ РАУНДОВОЕ ПРЕОБРАЗОВАНИЕ

Это линейное преобразование, точнее аффинное – поворот и сдвиг.

В этом случае элементы s_{ij} открытого текста

$$\begin{pmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{pmatrix}$$

представляют из себя 8-мерные вектора над полем GF(2).

Само преобразование имеет вид $s \mapsto As + b$, где

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

Матрица A – циркулянт, каждая строка является сдвигом предыдущей.

Нам нужно найти жорданову форму матрицы A. А для этого вычислить ее характеристический многочлен, найти его корни. После этого найти собственные вектора, корневые векторы высоты 2 и 3 и т.д.

Сделаем мы это средствами языка Julia и ее пакетов Nemo, LinearAlgebra, SymPy – математический пакет языка Python.

```
using Nemo
using SymPy
using LinearAlgebra
```

Характеристический многочлен

Вначале создадим пространство матриц размера 8 на 8 над полем GF(2) и пространство вектор столбцов над этим же полем

```
S = MatrixSpace(GF(2),8,8)
T = MatrixSpace(GF(2),8,1)
```

Теперь зададим матрицу A. Зададим построчечно, так меньше писать знаков препинания, и столбец вектора сдвига b

```
A=[1 0 0 0 1 1 1 1;1 1 0 0 0 1 1 1;1 1 1 0 0 0 1 1;1 1 1 1 0 0 0 1;1 1 1 1 1 0 0 0;0 1 1 1 1 1 0 0;0 0 1 1 1 1 1 0;0 0 0 1 1 1 1 1]
b = [1,1,0,0,0,1,1,0]
```

По умолчанию - это целые числа Int64, а нам нужны остатки по модулю 2. Поэтому укажем какому пространству матриц они принадлежат

```
A = S(A)  b = T(b).
```

Теперь создадим единичную матрицу, чтобы не набивать ее руками

```
E=Matrix{Int64}(I,8,8)
```

И переформатируем ее в матрицу над полем GF(2): E = S(E).

После этого можно вычислить характеристический многочлен, задав, предварительно переменную “x”

```
@vars x
p(x)=det(x*E-A)
p(x)
```

Однако, к сожалению, SymPy в Julia не вычисляет характеристические многочлены над полем Галуа (пока не вычисляет)

```
julia> p(x)
ERROR: MethodError: no method matching *(::Sym, ::gfp_mat)
Closest candidates are:
  *(::Any, ::Any, ::Any, ::Any...) at operators.jl:529
  *(::fmpz, ::T) where T<:Union{gfp_mat, nmod_mat} at
C:\Users\rosav\.julia\packages\Nemo\Pc5ui\src\flint\nmod_mat.jl:308
  *(::fmpz, ::MatElem) at
C:\Users\rosav\.julia\packages\Nemo\Pc5ui\src\flint\adhoc.jl:422
Stacktrace:
 [1] p(::Sym) at .\REPL[16]:1
 [2] top-level scope at REPL[17]:1
```

Но наши старания не совсем напрасны. Вычислять преобразование $s \mapsto As + b$ мы можем сразу над полем GF(2).

Пример. *Преобразований вида* $s \mapsto As + b$.

Положим s=[1,0,1,0,1,0,1,0]. Переформатируем s=T(s) и выполним операцию A*s+b.

Ответ запишем в виде вектор-строки ([0], [1], [1], [0], [1], [1], [0], [0]).

Нули и едины в квадратных скобках означают, что это не числа, а остатки по модулю 2.

Поэтому вычислим характеристический многочлен по умолчанию в формате Int64.

Имеем

```
julia> @vars x
(x,)
julia> p(x)=det(x*E-A)
p (generic function with 1 method)
julia> p(x)
 8       7        6        5         4         3        2
x  - 8?x  + 24?x  - 64?x  + 114?x  - 104?x  + 48?x  - 16?x + 5
```

Над полем рациональных чисел получился характеристический многочлен

$$x^8 - 8x^7 + 24x^6 - 64x^5 + 114x^4 - 104x^3 + 48x^2 - 16x + 5 \equiv x^8 + 1 (\mathrm{mod}\, 2) \equiv (\mathrm{x}+1)^8 .$$

Над полем GF(2) характеристический многочлен имеет единственный корень 1 кратности 8.

Нахождение жордановой формы

Вычислим значение характеристической матрицы при x = 1. Снова выполним все вычисления

```
using Nemo
using SymPy
using LinearAlgebra
S = MatrixSpace(GF(2),8,8)
A=[1 0 0 0 1 1 1 1;1 1 0 0 0 1 1 1;1 1 1 0 0 0 1 1;1 1 1 1 0 0 0 1;1 1 1
1 1 0 0 0;0 1 1 1 1 1 0 0;0 0 1 1 1 1 1 0;0 0 0 1 1 1 1 1]
E=Matrix{Int64}(I,8,8)
A = S(A);  E = S(E); B=A+E
 julia> A = S(A);  E = S(E); B=A+E
 [0  0  0  0  1  1  1  1]
 [1  0  0  0  0  1  1  1]
 [1  1  0  0  0  0  1  1]
 [1  1  1  0  0  0  0  1]
 [1  1  1  1  0  0  0  0]
 [0  1  1  1  1  0  0  0]
 [0  0  1  1  1  1  0  0]
 [0  0  0  1  1  1  1  0]
```

Итак, матрица B задает систему линейных уравнений, фундаментальная система решений которой дает нам базис собственных векторов. Систему решаем методом Гаусса

$$\begin{pmatrix} 0&0&0&0&1&1&1&1\\ 1&0&0&0&0&1&1&1\\ 1&1&0&0&0&0&1&1\\ 1&1&1&0&0&0&0&1\\ 1&1&1&1&0&0&0&0\\ 0&1&1&1&1&0&0&0\\ 0&0&1&1&1&1&0&0\\ 0&0&0&1&1&1&1&0 \end{pmatrix} \Rightarrow \begin{pmatrix} 0&0&0&0&1&1&1&1\\ 1&0&0&0&0&1&1&1\\ 0&1&0&0&0&1&0&0\\ 0&0&1&0&0&0&1&0\\ 0&0&0&1&0&0&0&1\\ 0&1&0&0&0&1&0&0\\ 0&0&1&0&0&0&1&0\\ 0&0&0&1&0&0&0&1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1&0&0&0&0&1&1&1\\ 0&1&0&0&0&1&0&0\\ 0&0&1&0&0&0&1&0\\ 0&0&0&1&0&0&0&1\\ 0&0&0&0&1&1&1&1 \end{pmatrix}$$

Следовательно, система имеет три свободных переменных, и мы получаем 3 линейно независимых собственных вектора.

$e_1 = (1,1,0,0,1,1,0,0)$, $e_2 = (1,0,1,0,1,0,1,0)$, $e_3 = (1,0,0,1,0,0,1)$.

Пример. *Применение собственных векторов к анализу шифра.*

Пусть $V_1 = \langle e_1, e_2, e_3 \rangle$. подпространство, порожденное собственными векторами. Так как собственное значение, которому отвечают эти собственные вектора, равно 1, то под действием линейного отображения, задаваемого матрицей A, все вектора из V не изменяются. Следовательно,

$$\forall x \in V,\ f(x) = Ax + b = x + b.$$

Теперь выясним – существуют ли элементы векторного пространства, которые остаются неподвижными под действием преобразования f(x).

То есть, решим уравнение

f(x) = Ax + b = x, следовательно (A-E)x = -b.

Поскольку характеристика равна 2, то получаем следующую расширенную матрицу исследуемой системы, которую решаем методом Гаусса

$$\begin{pmatrix} 0&0&0&0&1&1&1&1&1\\ 1&0&0&0&0&1&1&1&1\\ 1&1&0&0&0&0&1&1&0\\ 1&1&1&0&0&0&0&1&0\\ 1&1&1&1&0&0&0&0&0\\ 0&1&1&1&1&0&0&0&1\\ 0&0&1&1&1&1&0&0&1\\ 0&0&0&1&1&1&1&0&0 \end{pmatrix} \Rightarrow \begin{pmatrix} 1&0&0&0&0&1&1&0&0\\ 0&1&0&0&0&1&0&0&0\\ 0&0&1&0&0&0&1&0&0\\ 0&0&0&1&0&0&0&0&0\\ 0&0&0&0&1&1&1&0&0\\ 0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&1 \end{pmatrix}$$

Из-за последнего уравнения система несовместна. Что не удивительно, если бы такие решения были, то это было бы слабостью шифра. Пример закончен.

Вернемся к поиску жордановой формы матрицы A. Поскольку собственных векторов 3, то и жордановых клеток будет 3. Чтобы найти их размер

```
julia> B^2
[1  0  1  0  1  0  1  0]
[0  1  0  1  0  1  0  1]
[1  0  1  0  1  0  1  0]
[0  1  0  1  0  1  0  1]
[1  0  1  0  1  0  1  0]
[0  1  0  1  0  1  0  1]
[1  0  1  0  1  0  1  0]
[0  1  0  1  0  1  0  1]
```

Получаем систему

$$B^2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Следовательно, пространство решений имеет размерность 6. Поэтому, раз собственных векторов 3, то корневых векторов высоты 2 тоже 3. Значит жордановы клетки имеют размерности или 4 + 2 + 2 или 3 + 3 + 2.

Первый случай имеет место только тогда, когда $B^3 \neq 0$. Однако, это не так `julia> B^3` - нулевая матрица, мы для экономии мечта ее не приводим.

Следовательно, жорданова форма матрицы A над полем GF(2)имеет вид

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Продолжая вычисления в Julia получаем

```
julia> A^3
[0  0  1  0  0  1  0  1]
[1  0  0  1  0  0  1  0]
[0  1  0  0  1  0  0  1]
[1  0  1  0  0  1  0  0]
[0  1  0  1  0  0  1  0]
[0  0  1  0  1  0  0  1]
[1  0  0  1  0  1  0  0]
[0  1  0  0  1  0  1  0]
```

```
julia> A^4
```
 - единичная матрица

Следовательно, обратной матрицей к A будет A^3, поэтому процедура расшифрования будет выглядеть так $s' = As + b \Rightarrow A^3(s' - b) = A^3 s' - A^3 b$.

Упражнение. Вычислить произведение $A^3 b$.

ЛИТЕРАТУРА

1. Рябко Б.Я, Фионов А.Н. Криптографические методы защиты информации, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2017. - URL: https://e.lanbook.com/reader/book/111097/
2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. [Электронный ресурс]. - СПб.: Лань, 2011. - URL: https://e.lanbook.com/reader/book/68466