МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «СГУ ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»

ЛАБОРАТОРНАЯ РАБОТА №7

студента 4 курса 431 группы
направления 10.05.01 — Компьютерная безопасность
факультета КНиИТ
Никитина Арсения Владимировича

Проверил
доцент _____ А. В. Жаркова

Саратов 2022

СОДЕРЖАНИЕ

1 Задание лабораторной работы

Стандарт шифрования AES. Перемножить байты:

$$(1,1,0,1,0,0,1,1) \cdot (0,1,1,1,0,0,1,1),$$
$$(0,1,0,1,0,1,0,1) \cdot (1,0,1,0,1,0,1,0)$$

2 Теоретическая часть

Алгоритм AES оперирует с байтами, которые интерпретируются как элементы поля $GF(2^8)$. В данном поле определены операции сложения и умножения двух элементов, причем результатом такого умножения будет точно элемент данного поля.

Итак, для того, чтобы выполнить умножение двух байтов p и q, каждый из байтов требуется представить в виде полинома:

$$p(x) = p_7x^7 + p_6x^6 + p_5x^5 + p_4x^4 + p_3x^3 + p_2x^2 + p_1x + p_0,\ p_i \in \{0,1\};$$
$$q(x) = q_7x^7 + q_6x^6 + q_5x^5 + q_4x^4 + q_3x^3 + q_2x^2 + q_1x + q_0,\ q_i \in \{0,1\}.$$

Умножение байт в таком представлении производится по модулю неприводимого в $GF(2^8)$ многочлена $f(x) = x^8 + x^4 + x^3 + x + 1$, то есть получаем конечную формулу:

$$r(x) \equiv p(x)q(x)\ (mod\ f(x))$$

3 Практическая часть

№7 Стандарт шифрования AES. Перемножить байты:

① $(1,1,0,1,0,0,1,1)\cdot(0,1,1,1,0,0,1,1)$

② $(0,1,0,1,0,1,0,1)\cdot(1,0,1,0,1,0,1,0)$

① Для того, чтобы найти произведение байтов $(\overset{7}{1},\overset{6}{1},0,\overset{4}{1},0,0,\overset{1}{1},\overset{0}{1})\cdot(0,\overset{6}{1},\overset{5}{1},\overset{4}{1},0,0,\overset{1}{1},\overset{0}{1})$, запишем их в виде многочленов и выполним вначале умножение в кольце $Z_2[x]$:

$$(x^7+x^6+x^4+x^1+1)\cdot(x^6+x^5+x^4+x^1+1)=$$

$$=(x^{13}+x^{12}+x^{11}+x^8+x^7+x^{12}+x^4+x^{10}+x^7+x^6+x^{10}+x^9+x^8+$$

$$+x^5+x^4+x^7+x^6+x^5+x^2+x^1+x^6+x^5+x^4+x^1+1)\bmod 2$$

$$=x^{13}+x^9+x^7+x^6+x^5+x^2+1$$

Затем вычислим остаток при делении полученного многочлена на $f(x)$, где $f(x)=x^8+x^4+x^3+x^1+1$:

$$\begin{array}{l} x^{13}+x^9+x^7+x^6+x^5+x^2+1 \;\Big|\; x^8+x^4+x^3+x^1+1 \\ \underline{-\,x^{13}+x^9+x^8+x^6+x^5} \qquad\qquad\qquad\qquad\quad x^5+1 \\ x^8+x^7+x^2+1 \qquad\qquad\qquad\qquad\qquad \text{частное} \\ \underline{-\,x^8+x^4+x^3+x^1+1} \\ x^7+x^4+x^3+x^2+x \\ \text{остаток} \end{array} \quad \bmod 2$$

Получаем: $x^{13}+x^9+x^7+x^6+x^5+x^2+1=f(x)\cdot(x^5+1)+(x^7+x^4+x^3+x^2+x)$

А, значит, произведение будет байт:

$(1,0,0,1,1,1,1,0)$

② $(x^6+x^4+x^2+1)\cdot(x^7+x^5+x^3+x^1) =$

$= (x^{13}+x^{11}+x^9+x^7+x^{11}+x^9+x^7+x^5+x^9+x^7+x^5+x^3+x^7+x^5+x^3+x^1) \bmod 2 = x^{13}+x^9+x^5+x^1$

$\bmod 2$ — $\dfrac{x^{13}+x^9+x^5+X \;\big|\; x^8+x^4+x^3+x^1+1}{x^{13}+x^9+x^8+x^6+x^5 \;\big|\; x^5+1}$

$\dfrac{x^8+x^6+X^1}{}$

$\bmod 2$ — $\dfrac{x^8+x^4+x^3+x^1+1}{x^6+x^4+x^3+1} \Rightarrow (0,1,0,1,1,0,0,1)$