Практическая работа 1
Поля Галуа $\mathrm{GF}(2^m)$

1.1. Цель работы

Рассмотреть на примере и получить навыки в решении задач по теме «Конечные поля Галуа» в части, относящейся в вопросам помехоустойчивого кодирования.

1.2. Порядок выполнения задания

Задание выполняется каждым учащимся индивидуально.

Все расчеты должны быть расписаны максимально подробно.

1.2.1.

Для заданного полинома $p_1(x)$ показать, что он не является неприводимым. Для этого проверить значение

$$x^{2^m-1} \mod p(x).$$

Полином $p_1(x)$ выбирается из табл. 1.1 по номеру в журнале.

Таблица 1.1

Полином $p_1(x)$. Выбирается по номеру в журнале

Цифра номера	Полином	Цифра номера	Полином
1, 11, 21	x^4+x^2+x+1	**2, 12, 22**	x^4+x^3+x+1
3, 13, 23	$x^4+x^3+x^2+1$	**4, 14, 24**	x^5+x+1
5, 15, 25	x^5+x^2+x+1	**6, 16, 26**	x^5+x^3+x+1
7, 17, 27	$x^5+x^3+x^2+1$	**8, 18, 28**	x^5+x^4+x+1
9, 19, 29	$x^5+x^4+x^2+1$	**10, 20, 30**	$x^5+x^4+x^3+1$

1.2.2.

Для заданного образующего полинома $p_2(x)$ построить конечное поле Галуа. Полином $p_2(x)$ выбирается из табл. 1.2 по номеру в журнале. Полученные элементы записать в табл. 1.3.

Таблица 1.2

Полином $p_2(x)$. Выбирается по номеру в журнале

Цифра номера	Полином
1, 5, 9, 13, 17, 21, 25, 29	$x^5+x^3+x^2+x+1$
2, 6, 10, 14, 18, 22, 26, 30	$x^5+x^4+x^2+x+1$

Продолжение табл. 1.2

Полином $p_2(x)$. Выбирается по номеру в журнале

Цифра номера	**Полином**
3, 7, 11, 15, 19, 23, 27	$x^5+x^4+x^3+x+1$
4, 8, 12, 16, 20, 24, 28	$x^5+x^4+x^3+x^2+1$

Таблица 1.3

Таблица для записи элементов поля

Степенная форма	**Полином**	**Вектор** $[a_0\,a_1\,a_2\,a_3\,a_4]$	**Десятичная форма**
...	...	...	...

1.2.3.

Для заданного образующего полинома $p_2(x)$ построить генератор конечного поля Галуа. Полином $p_2(x)$ выбирается из табл. 1.2 по номеру в журнале. Продемонстрировать работу генератора, вычислив первые 12 элементов поля.

1.2.4.

Для заданного поля Галуа (см. табл. 1.4) осуществить расчет по заданной формуле. Формула берется из табл. 1.5. Номер формулы соответствует предпоследней цифре зачетной книжки. Значения переменных берутся из табл. 1.6 по последней цифре номера зачетной книжки.

Таблица 1.4

Поле Галуа $\mathrm{GF}(2^4)$. $p(x)=x^4+x+1$.

Элемент поля	**Полином**	**Двоичный вид** $[a_0\,a_1\,a_2\,a_3]$	**Десятичный вид**
$\varepsilon^0=1$	1	1000	1
ε	x	0100	2
ε^2	x^2	0010	4
ε^3	x^3	0001	8
ε^4	$1+x$	1100	3
ε^5	$x+x^2$	0110	6
ε^6	x^2+x^3	0011	12
ε^7	$1+x+x^3$	1101	11
ε^8	$1+x^2$	1010	5
ε^9	$x+x^3$	0101	10
ε^{10}	$1+x+x^2$	1110	7
ε^{11}	$x+x^2+x^3$	0111	14
ε^{12}	$1+x+x^2+x^3$	1111	15

Продолжение табл. 1.4

Поле Галуа $\mathrm{GF}(2^4)$. $p(x) = x^4 + x + 1$.

Элемент поля	**Полином**	**Двоичный вид** $[a_0\, a_1\, a_2\, a_3]$	**Десятичный вид**
ε^{13}	$1 + x^2 + x^3$	1011	13
ε^{14}	$1 + x^3$	1001	9

Таблица 1.5

Формула для расчета. По предпоследней цифре номера зачетной книжки

Цифра	**Формула**	**Цифра**	**Формула**
1	$\frac{a+b}{c} + ad^e$	6	$\frac{ab}{a+c} + d^e$
2	$ab + \frac{b+c}{d^e}$	7	$(a+c)b^e + \frac{d}{c}$
3	$\frac{ad}{b+c} + a^e$	8	$(a^e + b)c + \frac{d}{a}$
4	$(a+b)c + \frac{d^e}{a}$	9	$\frac{a}{c} + (b + c^e)d$
5	$\frac{a^e}{b+c} + cd$	0	$\frac{a+d^e}{bc} + c$

Таблица 1.6

Переменные для рассчета. По последней цифре номера зачетной книжки

	Последняя цифра номера									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**
a	ε^{12}	ε^{11}	ε^{10}	ε^{9}	ε^{8}	ε^{7}	ε^{6}	ε^{5}	ε^{4}	ε^{3}
b	ε^{2}	ε^{3}	ε^{4}	ε^{5}	ε^{7}	ε^{6}	ε^{8}	ε^{9}	ε^{10}	ε^{11}
c	ε^{14}	ε^{12}	ε^{11}	ε^{8}	ε^{6}	ε^{4}	ε^{2}	ε^{13}	ε^{11}	ε^{9}
d	ε^{3}	ε^{5}	ε^{7}	ε^{11}	ε^{9}	ε^{13}	ε^{12}	ε^{10}	ε^{8}	ε^{6}
e	2	3	4	5	6	2	3	4	5	6

1.2.5.

Для заданного поля Галуа (см. табл. 1.4) и элементов поля a и b найти характеристическую матрицу F_b и осуществить умножение элемента a на элемент b, используя матрицу F_b. Значения элементов a и b выбираются из табл. 1.7 по предпоследней и последней цифрам номера зачетной книжки соответственно.

Таблица 1.7

Переменные для умножения по характеристической матрице

	Предпоследняя цифра номера									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**
a	ε^{12}	ε^{11}	ε^{10}	ε^{9}	ε^{8}	ε^{7}	ε^{6}	ε^{5}	ε^{4}	ε^{3}
	Последняя цифра номера									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**
b	ε^{2}	ε^{3}	ε^{4}	ε^{5}	ε^{7}	ε^{6}	ε^{8}	ε^{9}	ε^{10}	ε^{11}

1.3. Порядок защиты практической работы

Защита работы может осуществляться одним из нижеперечисленных способов или их сочетанием на усмотрение преподавателя.

1. Устный ответ по теме работы.
2. Тестирование по теме работы.
3. Задача по теме работы.
4. Иные варианты на усмотрение преподавателя.