МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

Кафедра Защищенных систем связи

Дисциплина «Основы криптографии с открытыми ключами»

Лабораторная работа № 11

СИСТЕМА ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ НА ОСНОВЕ ГОМОМОРФНЫХ СВОЙСТВ КРИПТОСИСТЕМЫ ПЭЙЕ

Выполнил: ст. г. ИКТЗ-83

Миколаени М. С.

Проверил: Яковлев В. А.

Санкт-Петербург
2021

Цель лабораторной работы:

Изучение принципов построения системы электронного голосования на основе криптосистемы Пэйе и анализ выполнения требований по обеспечению ее безопасности.

Исходные данные:

Вариант 15

Избиратель	**B1** (10^0)	**B2** (10^1)	**B3** (10^2)	**B4** (10^3)	**B5** (10^4)	**Голос (m)**
A1			v			m=100
A2	v				v	m=10001
A3	v				v	m=10001
A4	v			v		m=1001
A5	v			v		m=1001
A6			v			m=100
Итог:	4	0	2	2	2	

Nv = 6, Nc = 5

Основание системы счисления b = Nv + 1 = 7

Выполнение работы:

Генерация ключей:

Максимальное число сообщений, которые можно зашифровать

$m_{max} = 10^4 + 10^3 = 11000$

Следовательно, максимально возможная сумма всех голосов

$T_{max} = Nv * m_{max} = 6 * 11000 = 66000$

По условию $n > \mathrm{T_{max}}$; $n > 66000$

Для генерации ключа выберем случайным образом 2 простых больших числа $p = 263$ и $q = 433$, где $gcd(pq, (p-1)(q-1)) = 1$

Вычисляем $n = 263 \times 433 = 113879$, $n^2 = 12968426641$

$\lambda = lcm(p-1, q-1) = lcm(262,432) = 56592$

Пусть $\alpha = 13, \beta = 11$

$g = (\alpha n + 1)\beta^n mod n^2 = (13 * 113879 + 1)11^{113879} mod 113879^2$

$= 2714779336$

$\mu = \left(L\left(g^{\lambda} mod\ n^2\right)\right) - 1\ mod\ n =$ $((2714779336^{56592}\ mod\ 12968426641 - 1/113879)^{-1} mod\ 113879 = 52422$

Шифрование:

Зашифруем сообщения, содержащие выбор избирателей: $E(m_i) = c_i = g^{mi} \times r_i^n mod\ n^2 = 2714779336^{mi} \times r_i^{113879} mod\ 12968426641$ $r \in Z^*_n$

Избиратель	Случайное число (r_i)	Голос (m)	Зашифрованное значение голоса (c_i)
A1	7	100	2056971025
A2	16	10001	882704169
A3	13	10001	12874601278
A4	21	1001	5239906734
A5	11	1001	7131914147
A6	9	100	574084670
Подсчет:		22204	

$c_1 = 2714779336^{100} * 7^{113879} mod\ 12968426641 = 2056971025$
$c_2 = 2714779336^{10001} * 16^{113879} mod\ 12968426641 = 882704169$
$c_3 = 2714779336^{10001} * 13^{113879} mod\ 12968426641 = 12874601278$
$c_4 = 2714779336^{1001} * 21^{113879} mod\ 12968426641 = 5239906734$
$c_5 = 2714779336^{1001} * 11^{113879} mod\ 12968426641 = 7131914147$
$c_6 = 2714779336^{100} * 9^{113879} mod\ 12968426641 = 574084670$

Вычислим произведение криптограмм:

$$T = \prod_{i=1}^{Nv} c_i mod\ n^2$$
$$= (2056971025 * 882704169 * 12874601278 * 5239906734 * 7131914147 * 574084670)\ mod\ 12968426641$$
$$= 8859988450$$

Дешифрование:

$$(T) = L\left(T^{\lambda} mod\ n^2\right) \times \mu\ mod\ n$$
$$= \left(\frac{\left(8859988450^{56592} mod\ 12968426641\right) - 1}{113879}\right) * 52422\ mod\ 113879 = 22204$$

Таким образом, подсчет зашифрованных голосов дает сумму всех голосов. Для определения победителя голосования необходимо преобразовать получившееся значение в числовую форму, представленную в начале выборов. В данном случае сервер для подсчетов голосов работает с десятичными числами, поэтому перевод не обязателен.

$$22204 = 2 * 10^4 + 2 * 10^3 + 2 * 10^2 + 0 * 10^1 + 4 * 10^0.$$

В силу гомоморфности криптосистемы индекс максимального элемента результирующего вектора и будет индексом победившего кандидата. Следовательно, можно сделать вывод о том, что победителем электронных выборов является кандидат B1.

Вывод:
В ходе выполнения данной лабораторной работы был изучен алгоритм электронного голосования на основе КС Пэйе и определен победитель электронного голосования.