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

Громов А. А.

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 №4.

Избиратель	B1 (10^0)	B2 (10^1)	B3 (10^2)	B4 (10^3)	B5 (10^4)	Голос (m)
A1	v		v			m=101
A2			v		v	m=10100
A3			v			m=100
A4		v				m=10
A5	v			v		m=1001
A6			v			m=100
Итог:	2	1	4	1	1	

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 $n > T_{max}$; $n > 66000$

Для генерации ключа выберем случайным образом 2 простых больших числа $p = 307$ и $q = 443$, где $gcd(pq, (p-1)(q-1)) = 1$

Вычисляем $n = 307 \times 443 = 136001$, $n^2 = 18496272001$

$\lambda = lcm(p-1, q-1) = lcm(306,442) = 3978$

Пусть $\alpha = 17, \beta = 7$

$g = (\alpha n + 1)\beta^n mod n^2 = (17 * 136001 + 1)7^{136001} mod 136001^2$

$= 4877987725$

$\mu = \left(L\left(g^{\lambda} mod\ n^2\right)\right) - 1\ mod\ n =$ $((4877987725^{3978}\ mod\ 18496272001 - 1)/136001)^{-1} mod\ 136001 = 87520$

Шифрование:

Зашифруем сообщения, содержащие выбор избирателей: $E(m_i) = c_i = g^{mi} \times r_i^n mod\ n^2 = 4877987725^{mi} \times r_i^{136001} mod\ 18496272001$ $r \in Z^*_n$

Избиратель	Случайное число (r_i)	Голос (m)	Зашифрованное значение голоса (c_i)
A1	21	m=101	5197777036
A2	68	m=10100	17083747880
A3	13	m=100	11662488432
A4	7	m=10	11633357469
A5	45	m=1001	6178628370
A6	9	m=100	18023831322
Подсчет:		11412	

$c_1 = 4877987725^{101} * 21^{136001} mod\ 18496272001\ = 5197777036$
$c_2 = 4877987725^{10100} * 68^{136001} mod\ 18496272001\ = 17083747880$
$c_3 = 4877987725^{100} * 13^{136001} mod\ 18496272001\ = 11662488432$
$c_4 = 4877987725^{10} * 7^{136001} mod\ 18496272001\ = 11633357469$
$c_5 = 4877987725^{1001} * 45^{136001} mod\ 18496272001\ = 6178628370$
$c_6 = 4877987725^{100} * 9^{136001} mod\ 18496272001\ = 18023831322$

Вычислим произведение криптограмм:

$$T = \prod_{i=1}^{Nv} c_i mod\ n^2$$
$$= (5197777036 * 17083747880 * 11662488432 * 11633357469 * 6178628370 * 18023831322)\ mod\ 18496272001$$
$$= 2322553511$$

Дешифрование:

$$D(T) = L\left(T^{\lambda} mod\ n^2\right) \times \mu\ mod\ n$$
$$= \left(\frac{\left(2322553511^{3978} mod\ 18496272001\right) - 1}{136001}\right) * 87520 mod\ 136001 = 11412$$

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.

$$11412 = 1 * 10^4 + 1 * 10^3 + 4 * 10^2 + 1 * 10^1 + 2 * 10^0.$$

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 В3.

Вывод:

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