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 (7^0)	B2 (7^1)	B3 (7^2)	B4 (7^3)	B5 (7^4)	Голос (m)
A1	v		v			m=50
A2			v		v	m=2450
A3			v			m=49
A4		v				m=7
A5	v			v		m=344
A6			v			m=49
Итог:	2	1	4	1	1	2949

$2949_{10} = 11412_7$

Nv = 6, Nc = 5

Основание системы счисления b = Nv + 1 = 7

Выполнение работы:

Генерация ключей:

Максимальное число сообщений, которые можно зашифровать

$m_{max} = 7^4 + 7^3 + 7^2 + 7^1 + 7^0 = 2801$

Следовательно, максимально возможная сумма всех голосов

$T_{max} = Nv * m_{max} = 6 * 2801 = 16806$

По условию $n > T_{max}$; $n > 16806$

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=50	5197777036
A2	68	m=2450	17083747880
A3	13	m=49	11662488432
A4	7	m=7	11633357469
A5	45	m=344	6178628370
A6	9	m=49	18023831322
Подсчет:		2949	

$$c_1 = 4877987725^{50} * 21^{136001} mod\ 18496272001 = 2457790475$$

$$c_2 = 4877987725^{2450} * 68^{136001} mod\ 18496272001 = 10019542800$$

$$c_3 = 4877987725^{49} * 13^{136001} mod\ 18496272001 = 13630098806$$

$$c_4 = 4877987725^{7} * 7^{136001} mod\ 18496272001 = 15686081260$$

$$c_5 = 4877987725^{344} * 45^{136001} mod\ 18496272001 = 15296550907$$

$$c_6 = 4877987725^{49} * 9^{136001} mod\ 18496272001 = 17323384321$$

Вычислим произведение криптограмм:

$$T = \prod_{i=1}^{Nv} c_i mod\ n^2 = (2457790475 * 10019542800 * 13630098806 *$$

$$* 15686081260 * 15296550907 * 17323384321)\ mod\ 18496272001 =$$

$$= 1154822184$$

Дешифрование:

$$D(T) = L\left(T^{\lambda} mod\ n^2\right) \times \mu\ mod\ n = \left(\frac{\left(1154822184^{3978} mod\ 18496272001\right)-1}{136001}\right) *$$

$$* 87520 mod\ 136001 = 2949$$

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.

$2949_{10} = 1 * 7^4 + 1 * 7^3 + 4 * 7^2 + 1 * 7^1 + 2 * 7^0 = 11412_7$

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 B3.

Вывод:

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