1)Тайные многосторонние вычисления для расчета средней величины трех чисел

Генерация ключей для троих участников

|  |  |  |
| --- | --- | --- |
| № п/п | Операция | Полученные значения |
| 1 | Выбираются два простых числа **p** и **q** | p1=7, q1=13  p2=5, q2=11  p3=11, q3=3 |
| 2 | Вычисляется произведение **n** = p \* q | n1=91  n2=55  n3=33 |
| 3 | Вычисляется функция Эйлера **φ(n) = (p-1)(q-1)** | φ1 = 72  φ2=40  φ3=20 |
| 4 | Выбирается открытый ключ **e**, как произвольное число (0 < e < n), взаимно простое с φ | e1=5  e2=17  e3=7 |
| 5 | Вычисляется закрытый ключ **d**, как обратное число к **e** по модулю φ(n), из соотношения (d\*e) mod φ(n) = 1. | d1=29  d2=33  d3=51 |

Таим образом, имеем три открытых ключа (5,91), (17,55), (91,187) и три закрытых ключа 29,33,51. Ниже представлен протокол вычисления среднего трех чисел с помощью тайных многосторонних вычислений.

Входные данные: 12, 21, 9. Секретное число – 8

|  |  |  |
| --- | --- | --- |
| № п/п | Операция | Полученные значения |
| 1 | **1** прибавляет случайное секретное число к своему числу, шифрует результат с помощью открытого ключа **2** и отсылает его **2**. | х1 = 15 |
| 2 | **2** расшифровывает результат, добавляет к нему свое число, шифрует результат с помощью открытого ключа **3** и отсылает его **3**. | у1=20  х2=184 |
| 3 | **3** расшифровывает результат, добавляет к нему свое число, шифрует результат с помощью открытого ключа **1** и отсылает его **1** | у2=41  х3=85 |
| 4 | **1** расшифровывает результат, отнимает секретное число  и вычисляет среднее | у3=50  **Ср=14** |

2) Разбиение секрета с использование гаммирования

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Операция | Полученные значения | | | | |
| 1 | Кодирование секрета – слово «КУЗ». | Секрет | Буква | К | У | З |
| Bin-код | 11001010 | 11010011 | 11000111 |
| 2 | Генерация случайных гамм и передача их участникам. | Гамма1 | Буква | К | О | Т |
| Bin-код | 11001010 | 11001110 | 11010010 |
| Гамма2 | Буква | В | К | Р |
| Bin-код | 11000010 | 11001010 | 11010000 |
| Гамма3 | Буква | Р | О | М |
| Bin-код | 11010000 | 11001110 | 11001100 |
| 3 | Получение шифрограммы (Секрет⊕Гамма1⊕Гамма2⊕Гамма3) и выкладывание её в доступное для участников место. | Шифрограмма | Bin-код | 00010010 | 00011001 | 00001001 |
| 4 | Восстановление секрета (Шифрограмма⊕Гамма1⊕Гамма2⊕Гамма3) | Секрет | Bin-код | 11001010 | 11010011 | 11000111 |
| Буква | К | У | З |

3)Разделение секрета по схеме Шамира

Определение долей, секрет S=12

|  |  |  |
| --- | --- | --- |
| № п/п | Операция | Полученные значения |
| 1 | Выбор простого числа **p**, которое больше количества долей **n** и секрета **S** | p = 19 |
| 2 | Выбор произвольного многочлена степени **m-1**: **f(x)** = (a2х2 + a1x + S) mod p | a2=5, a1=7 |
| 3 | Определение долей (**xi**, **yi**), где **yi** = f(xi) и **xi** = i + 1 | y0 = 5 y1 = 8 y2 = 2 y3 = 6 y4 = 1 |
| 4 | Публикация **p** и распределение долей (**xi**, **yi**) | p = 19 (x0, y0) = (1, 5) (x1, y1) = (2, 8) (x2, y2) = (3, 2) (x3, y3) = (4, 6) (x4, y4) = (5, 1) |

Процедура восстановления секрета:

|  |  |  |
| --- | --- | --- |
| № п/п | Операция | Полученные значения |
| 1 | Сбор **m** долей. | (x0, y0) = (1, 5) (x1, y1) = (2, 8) (x4, y4) = (5, 1) |
| 2 | Определение базисных полиномов. |  |
| 3 | Определение интерполяционного полинома Лагранжа. |  |
| 4 | Определение обратного числа по модулю **b-1** для дробного множителя полинома **1 / b**. | b=12, b-1 = 8 |
| 5 | Замена дробного множителя **1 / b** и умножение коэффициентов полинома на множитель **b-1**. |  |
| 6 | Приведение коэффициентов полинома и определение секрета **S**. | a2 = -128 mod 19 = 5 a1 = -672 mod 19 = 7 S = -64 mod 19 = 12 L(x) = (5х2 + 7x + 12) mod 19 |

4)Разделение секрета по схеме Асмута-Блума

Определение долей, секрет S=12, n=5, m=3

|  |  |  |
| --- | --- | --- |
| № п/п | Операция | Полученные значения |
| 1 | Выбор простого числа **p**, которое больше секрета **S**. | p = 13 |
| 2 | Выбор **n** взаимно простых чисел **di**, удовлетворяющих условиям: - di > p; - di < di+1; - d1 \* d2 \* … \* dm < p \* dn-m+2 \* dn-m+3 \* … \* dn. | d= {17, 20, 23, 29, 37} |
| 3 | Выбор произвольного числа **r**, удовлетворяющего условию https://www.sites.google.com/site/anisimovkhv/_/rsrc/1496670739641/learning/kripto/lecture/tema16/table_Blum31.png. Вычисление **S’** = S + r p. | r<600  r=15 S’ = 12 + 15 \* 13 = 207 |
| 4 | Определение долей (**di**, **ki**), где **ki** = S’ mod di. | k1 = 3 k2 = 7 k3 = 0 k4 = 4 k5 = 22 |
| 5 | Публикация **p** и распределение долей (**di**, **ki**) | p = 13 (d1, k1) = (17, 3) (d2, k2) = (20, 7) (d3, k3) = (23, 0) (d4, k4) = (29, 4) (d5, k5) = (37, 22) |

Восстановление секрета

|  |  |  |
| --- | --- | --- |
| № п/п | Описание операции | Пример |
| 1 | Сбор **m** долей. | (d1, k1) = (17, 3) (d3, k3) = (23, 0) (d5, k5) = (37, 22) |
| 2 | Вычисление произведения **D** взаимно простых чисел **dj**. | D = 14467 |
| 3 | Вычисление сомножителей **Dj** = D / dj. | D1= 851 D2 = 629 D3 = 391 |
| 4 | Определение обратных чисел **Dj-1** по модулям **dj**. | D1-1 = 1 D2-1 = 3 D3-1 = 30 |
| 5 | Вычисление **S’** = (Σ kj Dj Dj-1) mod D. | S’ = 207 |
| 6 | Определение секрета **S** = S’ mod p. | S = 12 |