1)Алгоритм RSA

Генерация ключей

|  |  |  |
| --- | --- | --- |
| № п/п | Операция | Полученные значения |
| 1 | Выбираются два простых числа **p, q** | p=3 q=7 |
| 2 | Вычисляется **n**=pq | n = 21 |
| 3 | Вычисляется функция Эйлера **ф**=(p-1)(q-1) | ф = 12 |
| 4 | Выбирается **e** как число в интервале (0,n), взаимно простое с ф | е=5 |
| 5 | Вычисляется **d** как как обратное число к е по модулю ф  (de) mod ф = 1 | (5d) mod 12 = 1  d=5 |
| 6 | Сохраняются открытый и закрытый ключи | Открытый ключ (e,n)=(5,21)  Закрытый ключ d=5 |

Отправка сообщения и электронной подписи клиентом

|  |  |  |
| --- | --- | --- |
| № п/п | Операция | Полученные значения |
| 1 | Вычисление хеш-образа **h** = h(T), где **T** – исходное сообщение | h = 12 |
| 2 | Выработка цифровой подписи **s** = hd mod n | s = 3 |
| 3 | Отправка исходного сообщения **Т** и цифровой подписи **s** на сервер | T=”Hello” |

Получение сообщения и проверка электронной подписи на сервере

|  |  |  |
| --- | --- | --- |
| № п/п | Операция | Полученные значения |
| 1 | Вычисление хеш-образа по полученному сообщению **h’** = h(T’) | h' = 12 |
| 2 | Вычисление хеш-образа из цифровой подписи **h** = se mod n | h = 12 |
| 3 | Т.к. h' = h, то делается вывод, что полученное сообщение T’ = T и оно действительно отправлено идентифицированным пользователем | 12=12  Сообщение получено |

2) ГОСТ 34.10-94

Генерация ключей

|  |  |  |
| --- | --- | --- |
| № п/п | Операция | Полученные значения |
| 1 | Выбор **р** - простого числа | p = 79 |
| 2 | Выбор **q** - простого числа - множителя (р – 1) | q = 3 |
| 3 | Выбор **а** - любого числа, меньшего (р – 1), для которого aq mod р = 1 | а3 mod 79 = 1,  a = 1 |
| 4 | Выбор закрытого ключа **х** - числа, меньшего q | x = 2 |
| 5 | Вычисление открытого ключа **y** = ax mod p | y = 1 |
| 6 | Сохраняются открытый и закрытый ключи | Открытый ключ: (79,3,1,) Закрытый ключ: 2 |

Отправка сообщения и электронной подписи клиентом

|  |  |  |
| --- | --- | --- |
| № п/п | Описание операции | Пример |
| 1 | Вычисление хеш-образа **h** = h(T) | h = 21 |
| 2 | Выбор **k** - любого числа, меньшего q | k = 2 |
| 3 | Вычисление двух значений: **w** = ak mod p и **w’** = w mod q | w = 1 w’ = 1 |
| 4 | Вычисление **s** = (x w’ + k h) mod q | s = 2 |
| 5 | Отправка на сервер исходного сообщения **Т** и цифровой подписи (**w’**, **s**) |  |

Получение сообщения и проверка электронной подписи на сервере

|  |  |  |
| --- | --- | --- |
| № п/п | Описание операции | Пример |
| 1 | Вычисление хеш-образа по полученному сообщению **h’** = h(T’) | h' = 21 |
| 2 | Вычисление **v** = h’ q-2 mod q | v = 0 |
| 3 | Вычисление двух значений: **z1** = (s v) mod q и **z2** = ((q – w’) v) mod q | z1 = 0 z2 = 0 |
| 4 | Вычисление **u** = ((az1 \* yz2) mod p) mod q | u = 1 |
| 5 | Т.к. w’ = u, то делается вывод, что полученное сообщение T’ = T и оно действительно отправлено идентифицированным пользователем | 1=1  Сообщение получено |

3) ГОСТ 34.10-2001

Генерация ключей

|  |  |  |
| --- | --- | --- |
| № п/п | Операция | Полученные значения |
| 1 | Выбирается модуль эллиптической кривой - простое число **n** | n = 41 |
| 2 | Выбираются коэффициенты эллиптической кривой **A** и **B**. Должно соблюдаться условие (4 A3 + 27 B2) mod n ≠ 0, в противном случае меняются параметры эллиптической кривой n, A или B. | A = 3, B = 7 |
| 3 | Определяется точка эллиптической кривой **P(xp, yp)** и порядок циклической подгруппы группы точек эллиптической кривой **q**\*). Принимается произвольное xp (0 < xp < n) и определяется yp из уравнения эллиптической кривой. | xp = 7  yp = 17  q = 47 |
| 4 | Выбирается закрытый ключ **d** (0 < d < q). | d = 10 |
| 5 | Определяется точка эллиптической кривой **Q(xq, yq)**: Q(xq, yq) = d \* P(xp, yp). | xq = 36, yq = 20 |
| 6 | Сохраняются открытый и закрытый ключи | Открытый ключ: (3, 7, 7, 17, 47, 36, 20)  Закрытый ключ: 10 |

Отправка сообщения и электронной подписи клиентом

|  |  |  |
| --- | --- | --- |
| № п/п | Операция | Полученные значения |
| 1 | Вычисление хеш-образа **h** = h(T) | h = 7 |
| 2 | Вычисление **e** = h mod q | e = 7 |
| 3 | Выбор **k** - любого числа, меньшего q | k = 11 |
| 4 | Определение точки эллиптической кривой **C(xc, yc)** = k P(xp, yp) | C = (16, 16) |
| 5 | Вычисление **r** = хс mod q. | r = 16 |
| 6 | Вычисление **s** = (r d + k e) mod q | s = 2 |
| 7 | Отправка исходного сообщения **Т** и цифровой подписи (**r**, **s**) на сервер |  |

Получение сообщения и проверка электронной подписи на сервере

|  |  |  |
| --- | --- | --- |
| № п/п | Операция | Полученные значения |
| 1 | Вычисление хеш-образа по полученному сообщению **h’** = h(T’). | h' = 7 |
| 2 | Вычисление **e’** = h’ mod q. | e' = 7 |
| 3 | Вычисление **v** = e’ -1 mod q. | e’ -1 = 27 |
| 4 | Вычисление двух значений: **z1** = (s v) mod q и **z2** = ((q - r) v) mod q. | z1 = 7 z2 = 38 |
| 5 | Определение точки эллиптической кривой **C’(xc’, yc’)** = z1 P(xp, yp) + z2 Q(xq, yq) | C’ = 7 P(7, 17) + 38 Q(36, 20) = (16, 16) |
| 6 | Вычисление **r’** = xc’ mod q. | r' = 16 |
| 7 | Т.к. r’ = r, то делается вывод, что полученное сообщение T’ = T и оно действительно отправлено идентифицированным пользователем | 16=16  Сообщение получено |