CS152-12

Hongchen Cao 2019533114

2020/12/15

1

1. At the first time, Olga can records $(r_1, y_1, \mathbf{Cert}(Bob))$.
2. Then Olga can pretends to be Bob and send $(r_1, y_1, \mathbf{Cert}(Bob))$ to Alice.
3. Then Olga will get $(r_2', y_3', \mathbf{Cert}(Alice))$ where r_2' is a random challenge and $y_3' = sig_{Alice}(r_2')$ is a signature.
4. Then Olga can pretends to be Alice and send $(r_2', y_3', \mathbf{Cert}(Alice))$ to Bob.
5. Then Olga will get $sig_{Bob}(r_2')$ and he can forward this response to Alice.

2

1. At the first time, Bob sends $(r_1, \mathbf{Cert}()Bob)$ to Alice.
2. Then, adversary can records $(r_1, \mathbf{Cert}()Bob)$ and pretends to be Bob and send it to Alice.
3. Then adversary will get $(r_2, y_1, \mathbf{Cert}(Alice))$ where y_1 is $\mathbf{sig}_{Alice}(ID(Bob)||r_1||r_2)$.
4. Then adversary can pretends to be Alice and send $(r_2, y_1, \mathbf{Cert}(Alice))$ to Bob.
5. Finally, Bob will accept and adversary broke this protocol.

3

1. First, Bob chooses a random $r \in \mathbb{Z}_n$. If $\gcd(r, n) > 1$ then Bob obtains the factorization, but it happens with extremely low probability.
2. Otherwise, Bob computes $x = r^2 \bmod n$.
3. Then Alice will send Bob y which is a square root of $x \bmod n$.
4. Since Alice does not know r, the probability that $y \not\equiv \pm r \bmod n$ is $\frac{1}{2}$. So, by calculating $\gcd(y + r, n)$ Bob can gets the factorization $n = pq$.
5. Finally, he can pretends Alice.

4

4.1

In [1]:
```
p = 122503
q = 1201
t = 10
alpha = 11538
```

In [2]:
```
(p-1)/q
```

Out[2]: 102

In [7]:
```
mod(5 ^ 102, p) == alpha
```

Out[7]: True

So, α has order q in Z_p*

4.2

In [9]:
```
a =357
v = inverse_mod(pow(alpha, a), p)
v
```

Out[9]: 14320

4.3

In [10]:
```
k = 868
gamma = pow(alpha, k, p)
gamma
```

Out[10]: 89937

4.4

In [12]:
```
r = 501
y = mod(k + a * r, q)
y
```
Out[12]: 776

4.5

In [15]:
```
mod(pow(alpha, y) * pow(v, r), p)
```
Out[15]: 89937

In [16]:
```
mod(pow(alpha, k), p)
```
Out[16]: 89937