Сформировать мультипликативную группу Z

p – простое число

g – порождающий элемент

Пользователь П1 выбирает элемент

x∈ Z

Пользователь П1 вычисляет y по формуле

y = gx mod p

Передать y пользователю П2

Пользователь П2 выбирает k∈ Z

Пользователь П2 выбирает b∈ {0,1}

Пользователь П2 вычисляет r по формуле

r = yb gk mod p

Пользователь П2 передает r пользователю П1

Пользователь П1 выбирает элемент

с ∈ {0,1}

Пользователь П1 передает с пользователю П2

Пользователь П2 передает элементы

k и b пользователю П1

Пользователь П1 проверяет подлинность переданных значений

r = ybgk mod p.

Подлинность подтверждена?

Результат выполнения протокола

d=b⊕c.

Подлинность не подтверждена