45 Имя + имя

Задача. Трент поручил Бобу наладить аутентификацию между сотрудниками его организации. Боб предложил следующее решение. Сначала все сотрудники получают у Трента общий секретный ключ K. Затем для проверки подлинности друг друга пары сотрудников обмениваются своими именами. Каждый из сотрудников проверяет, что его имя отличается от имени визави, а затем вычисляет на ключе K имитовставку от своего имени, дополненного именем визави и меткой времени. Например, Алиса для аутентификации перед Бобом вычисляет имитовставку от строки

`alicebob2015-10-07T17:10:08+03:00`,

а Боб — от строки

`bobalice2015-10-07T17:10:10+03:00`,

Корректность имитовставки для некоторой метки времени в 10-секундном интервале назад доказывает подлинность противоположной стороны. Трент забраковал решение Боба. Почему?

Решение. Виктор может пройти аутентификацию без знания ключа. Виктор обращается к Бобу под именем `bobbob`. Боб высылает имитовставку

`bobbobbob2015-10-07T17:10:08+02:00`,

Виктор отвечает ей же. □