**Протокол аутентификации Фейга-Фиата-Шамира**

Сначала генерируем n равное произведению двух простых чисел *p* и *q*. Далее выбирается *k* чисел *v*1,*v*2, .., *vk* являющимися квадратичными остатками по модулю *n*. Иными словами *vi* выбирается так чтобы *x*2 ≡ *vi*(mod *n*) имело решение и существовало *vi*-1 mod *n*. Значения *v*1,…*vk* будут являться открытым ключом. Затем вычисляются *s*2*i*≡ *vi*-1  mod *n*. Числа *s*1, …, *sk* будут являться закрытым ключом.

1. Алиса выбирает случайное *r* < *n* и вычисляет *х = r*2 mod *n*. Алиса отправляет *х* Бобу
2. Боб генерирует случайный *к*-битный вектор (*b*1,…,*bk*) и отправляет его Алисе
3. Алиса вычисляет и отправляет Бобу 
4. Боб проверяет что 

Алиса и Боб повторяют этот протокол *t* раз, пока Боб не убедиться, что Алиса знает *s*1, …, *sk*