# Схема подписи 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.

Алгоритм подписи:

(1) Алиса выбирает t случайных целых чисел в диапазоне от 1 до и вычисляет такие что

(2) Алиса хэширует объединение сообщения и строки , создавая битовые поток . Она использует первые битов этой строки в качестве значений , где i пробегает от 1 до t, а j от 1 до k

(3) Алиса вычисляет где

(4) Алиса посылает Бобу , все биты и все значения . У Боба уже есть открытый ключ Алисы:

Проверка подписи:

(5) Боб вычисляет , где

(6) Боб проверяет, что первые битов -это значения , которые прислала ему Алиса.