Які вимоги висуваються до генераторів ключів та ключової інформації в протоколах нульових знань та як їх можна виконати?

В протоколах с нулевым разглашением для генерации ключей используется в т.ч. схема Фейге-Фиата-Шамира:

Таблица 13.4. Генерация ключей по схеме Фейге-Фиата-Шамира

№ п/п	Описание операции	Пример
1	Выбирает модуль **n**, равный произведению двух простых чисел.	p = 5, q = 7, n = 35
2	Выбирает число **v** (открытый ключ), являющееся квадратичным вычетом по модулю **n** и имеется обратное значение v^{-1} по модулю **n**. **Квадратный вычет** – число, удовлетворяющее выражению $x^2 \bmod n = v$, где $1 \le x \le n$. Для модуля n = 35, квадратными вычетами являются 1 (x = 1, 6, 29, 34), 4, 9, 11, 14, 15, 16, 21, 25, 29, 30. Обратное значение вычисляется по формуле $(v * v^{-1}) \bmod n = 1$. У квадратных вычетов 14, 15, 21, 25 и 30 нет обратных значений по модулю. $v \in \{1, 4, 9, 11, 16, 29\}$.	v = 16 $v^{-1} = 11$ (16 * 11) mod 35 = 176 mod 35 = 1
3	Определяет закрытый ключ **s**, как наименьшее значение, удовлетворяющее следующему выражению $s^2 \bmod n = v^{-1}$.	s = 9 9^2 mod 35 = 11
4	Публикация открытого ключа – **v** и **n**. Передача закрытого ключа **s A**.	