Задача. Описать способ взлома некорректного протокола Диффи-Хеллмана, в котором:

- параметр g не зафиксирован в протоколе, а выбирается каждый раз заново
- Ева может повлиять на его выбор, установив $g = p - 1$
- Ева не может менять никакие другие сообщения, но она может подслушивать сообщения, передаваемые сторонами; после выполнения всех шагов Ева должна вычислить секретный ключ S, который должен совпасть с ключом Алисы и Боба
- Алиса и Боб выполняют операции так же, как и в обычном протоколе

Описание способа взлома

1) Ева устанавливает $g = p - 1$

   Заметим, что

   $$p - 1 \equiv -1 \ (mod\ p)$$

   Тогда

   $$(p-1)^x \equiv -1 \ (mod\ p), \text{если } x - \text{нечётное}$$

   $$(p-1)^x \equiv 1 \ (mod\ p), \text{если } x - \text{чётное}$$

2) Ева перехватывает сообщения Алисы и Боба

   $$A = (p-1)^a \ mod\ p$$

   $$B = (p-1)^b \ mod\ p$$

   Рассмотрим все возможные случаи

   2.1) Ева перехватила $A = 1$ и $B = 1$

   Значит, a и b оба чётные, то есть $a = 2k, k \in Z, b = 2m, m \in Z$

   Тогда секретный ключ $S = (p-1)^{2k \cdot 2m} = (p-1)^{4km} \equiv 1 \ (mod\ p)$

   2.2) Ева перехватила $A = 1$ и $B = -1$

   Значит, a – чётное, b – нечётное, то есть $a = 2k, k \in Z, b = 2m + 1, m \in Z$

   Тогда секретный ключ $S = (p-1)^{2k \cdot (2m+1)} \equiv 1 \ (mod\ p)$

   2.3) Ева перехватила $A = -1$ и $B = 1$

   Значит, a – нечётное, b – чётное, то есть $a = 2k + 1, k \in Z, b = 2m, m \in Z$

   Тогда секретный ключ $S = (p-1)^{(2k+1) \cdot 2m} \equiv 1 \ (mod\ p)$

   2.4) Ева перехватила $A = -1$ и $B = -1$

   Значит, a и b оба нечётные, то есть $a = 2k + 1, k \in Z, b = 2m + 1, m \in Z$

   Тогда секретный ключ $S = (p-1)^{(2k+1) \cdot (2m+1)} = (p-1)^{2(2km+k+m)+1} \equiv$

   $\equiv -1 \ (mod\ p) \equiv p - 1 \ (mod\ p)$

Таким образом, если Ева при перехвате открытых ключей Алисы и Боба получает хотя бы одну единицу (по модулю p), то секретный ключ $S \equiv 1 \ (mod\ p)$; если же оба перехваченных открытых ключа от Алисы и Боба равны –1 (по модулю p), то секретный ключ $S \equiv p - 1 \ (mod\ p)$. То есть установка $g = p - 1$ гарантированно позволяет Еве вычислить секретный ключ при выполнении Алисой и Бобом операций, описанных в обычном протоколе