40. Сутність та якими властивостями володіє криптографічний протокол узгодження ключів Діффі - Гелмана?

Вот уже более 30 лет протокол распределения ключей Диффи-Хеллмана радует глаз простого криптомана своей простотой и надежностью. Для тех, кто эти последние 30 лет провел за занятиями более веселыми, нежели изучение криптографических протоколов, поясняю.
Протокол Диффи-Хеллмана был опубликован в 1976 году и послужил началом эры асимметричной криптографии. Суть его до гениального проста: Алиса и Боб хотят получить общий ключ для симметричной криптосистемы. Для этого они, договорившись, выбирают два больших числа g и p. Эти числа известны им обоим и держать их в секрете не имеет никакого смысла. Затем Алиса в тайне генерирует большое секретное число a, а Боб — большое число b. А далее за дело берется простая арифметика. Алиса посылает Бобу число
$A = g^a \bmod p$.
Боб в свою очередь высылает Алисе
$B = g^b \bmod p$.

Теперь, чтобы получить общий ключ Алиса вычисляет $K_a = B^a \bmod p$, а Боб находит $K_b = A^b \bmod p$.
Нетрудно проверить, что $K_a = K_b$, т.к.
$K_a = B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = A^b \bmod p = K_b$.
Гениальность идеи заключается в том, что для получения ключа K Алисе и Бобу не понадобится много времени, в то время, как злоумышленнику, чтобы найти K нужно уметь решать задачу дискретного логарифмирования.
Боясь утомить читателя общеизвестными фактами, перехожу сразу к сути дела. А что если абстрагироваться от теории и перейти к практике? То получим следующее.

Протокол Диффи-Хеллмана отлично противостоит пассивному нападению, но в случае реализации атаки «человек посередине» он не устоит. В самом деле, в протоколе ни Алиса, ни Боб не могут достоверно определить, кем является их собеседник, поэтому вполне возможно представить следующую ситуацию, при которой Боб и Алиса установили связь с Меллори, который Алисе выдает себя за Боба, а Бобу представляется Алисой. И тогда вместо протокола Диффи-Хеллмана получаем, что-то похожее на следующее:

Шаг	Алиса	Меллори	Боб
1	g^a →	g^a	
2	g^m g^{am} ←	g^m g^{am}	
3		g^m →	g^m
4		g^b g^{mb} ←	g^b g^{mb}

То есть, Меллори получает один ключ общий с Алисой(которая считает, что это Боб), и один ключ общий с Бобом(который считает, что это Алиса). А, следовательно, он может получать от Алисы любое сообщение для Боба расшифровать его ключом g^{am}, прочитать, зашифровать ключом g^{mb} и передать Бобу. Таким образом, подлог может оставаться незамеченным очень долгое время.