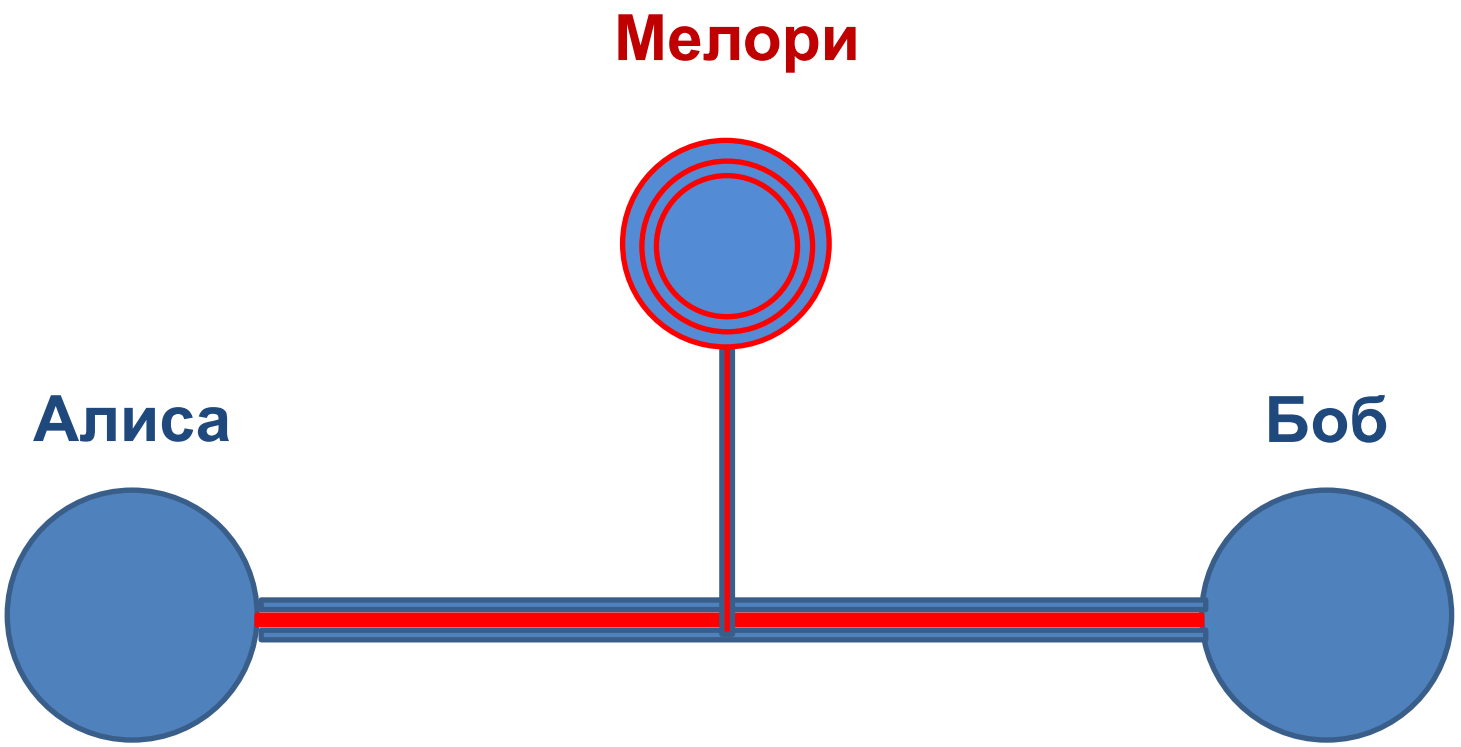
Алгоритм Диффи - Хелмана


Мелори
Алиса
Боб

Общие данные:

g, p

Алиса	Боб
Личные данные: **a**	Личные данные: **b**
$X = g^a \bmod(p)$	$Y = g^b \bmod(p)$
Y	X
$K_1 = Y^a \bmod(p)$	$K_2 = X^b \bmod(p)$

$K_1 == K_2$

Спасибо за внимание!

А. Сёмин А. Самородов