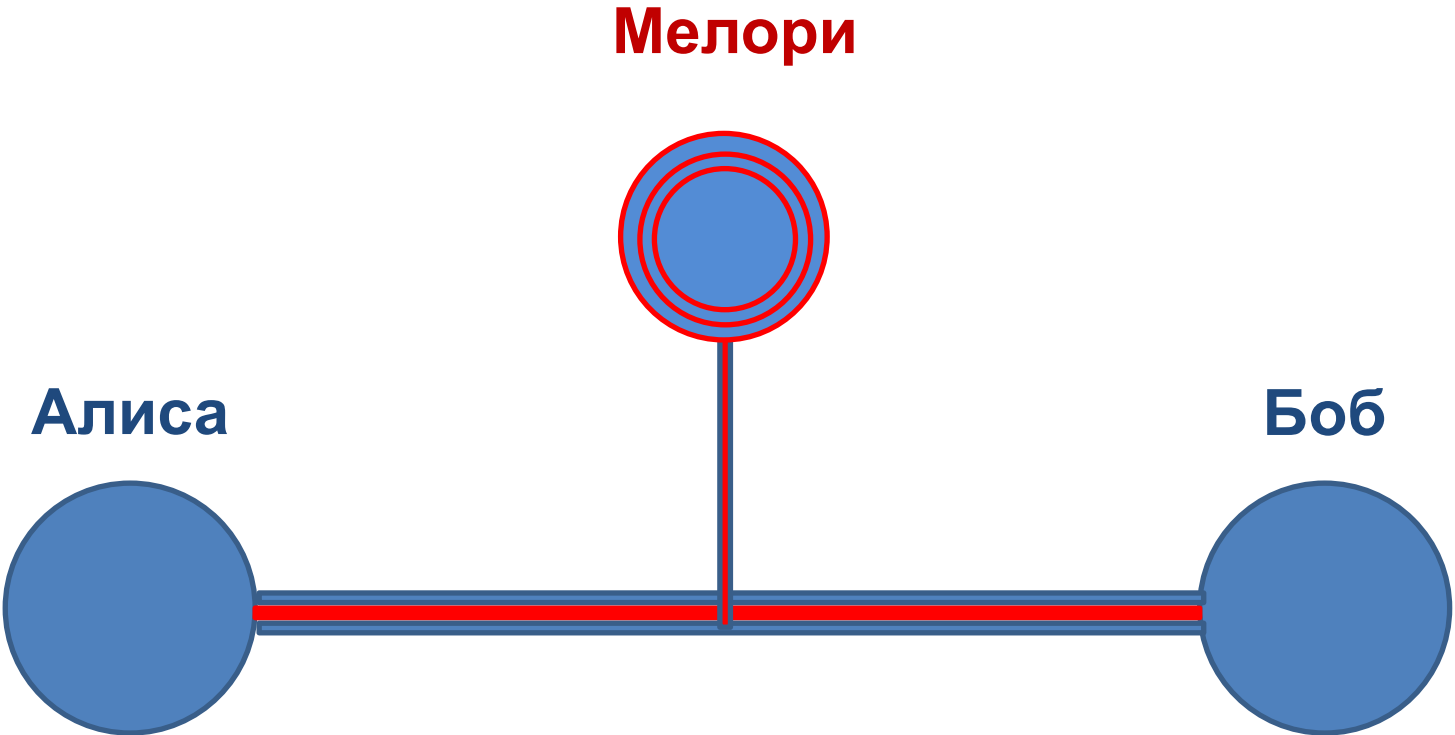


# **Алгоритм Диффи - Хелмана**



**Алис**

**а**

Личные  
данные:

$$X = g^a \text{ mod}(p)$$

Общие данные:

**g, p**

**Боб**

**б**

Личные  
данные:

$$Y = g^b \text{ mod}(p)$$

**Y**



**X**

$$K_1 = Y^a \text{ mod}(p)$$

$$K_2 = X^b \text{ mod}(p)$$

$$K_1 == K_2$$

**Спасибо за внимание!**

**А. Сёмин А. Самородов**