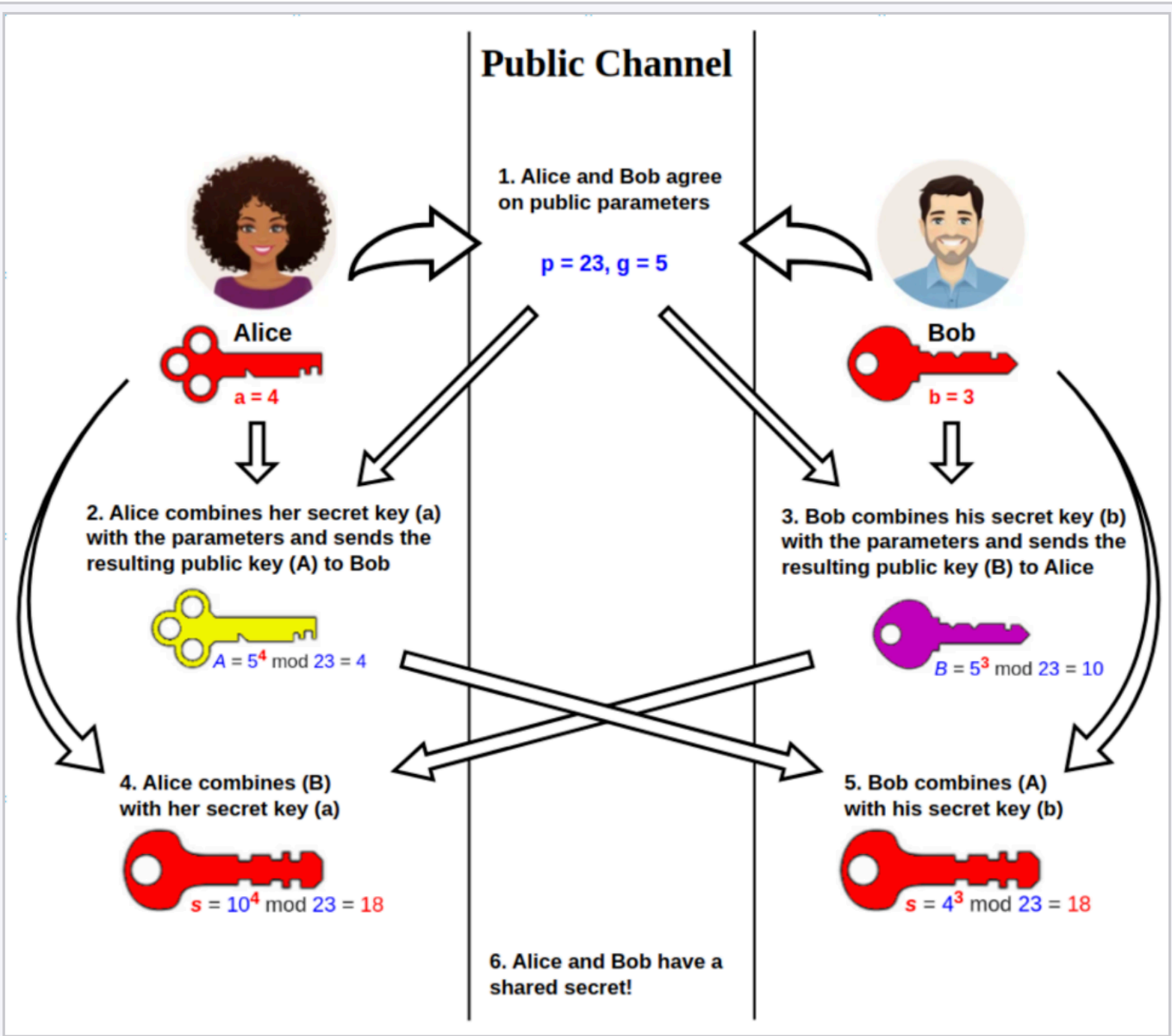

With Diffie–Hellman key exchange, two parties arrive at a common secret key, without passing the common secret key across the public channel.