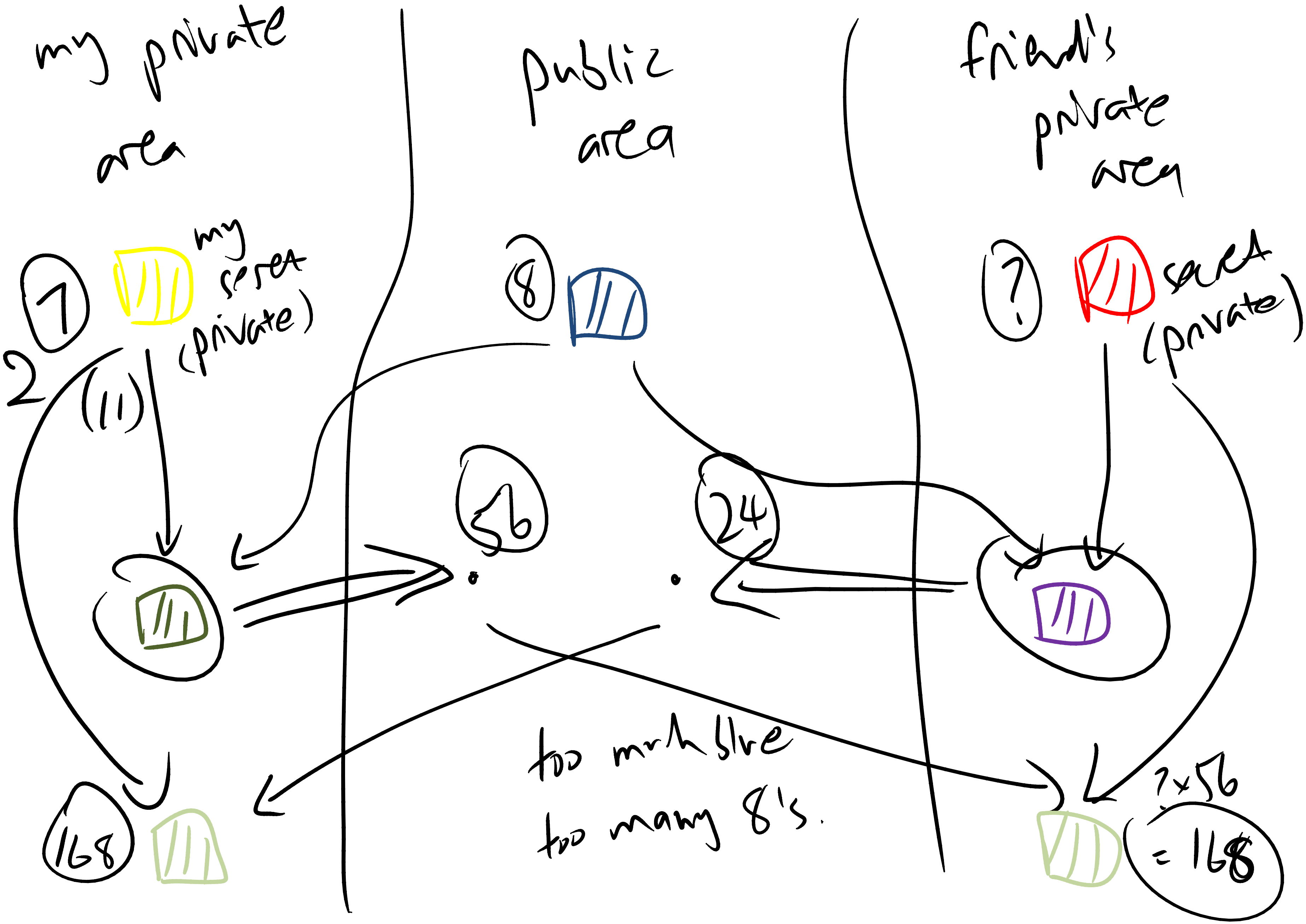
shared secret

how do we got this?

rest of talk


my private area
public area
friend's private area
7
my secret (private)
8
?
secret (private)
2
(11)
56
24
168
?×56
=168
too much blue
too many 8's.

discrete logarithm

Diffie-Hellman key exchange

RSA