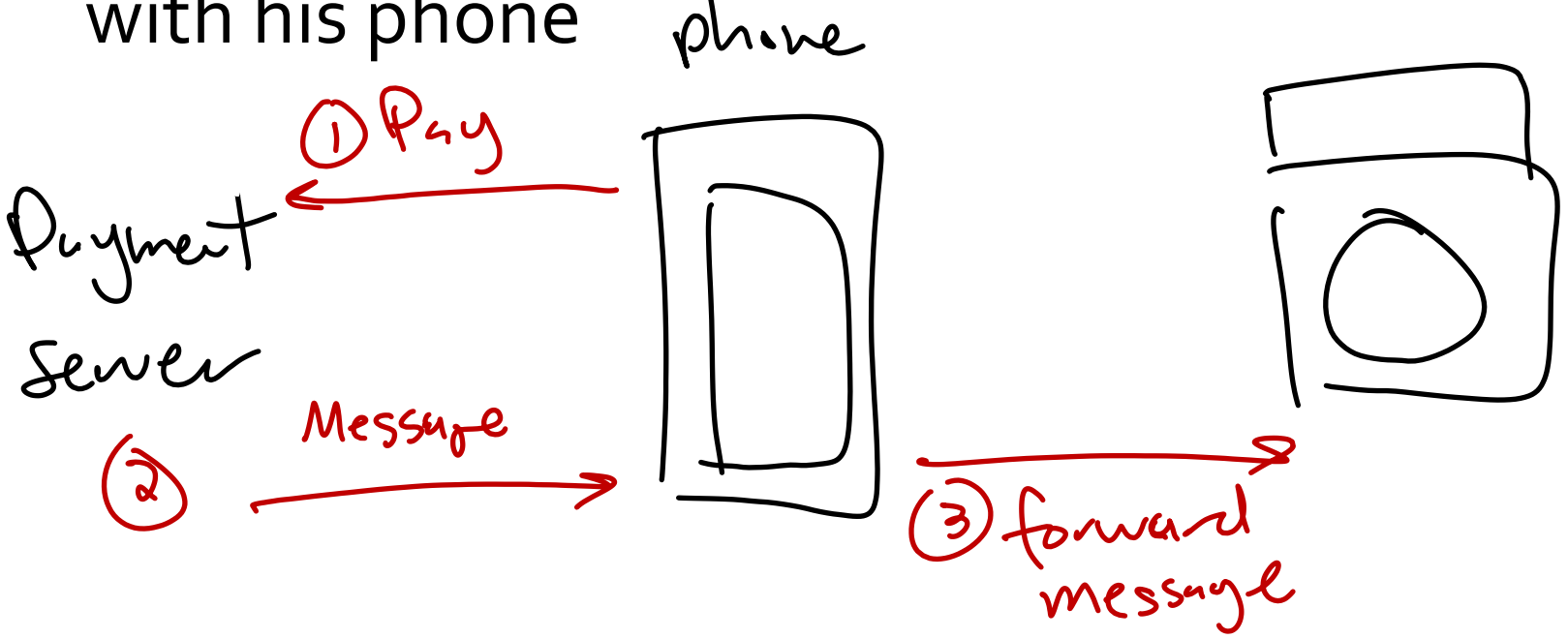
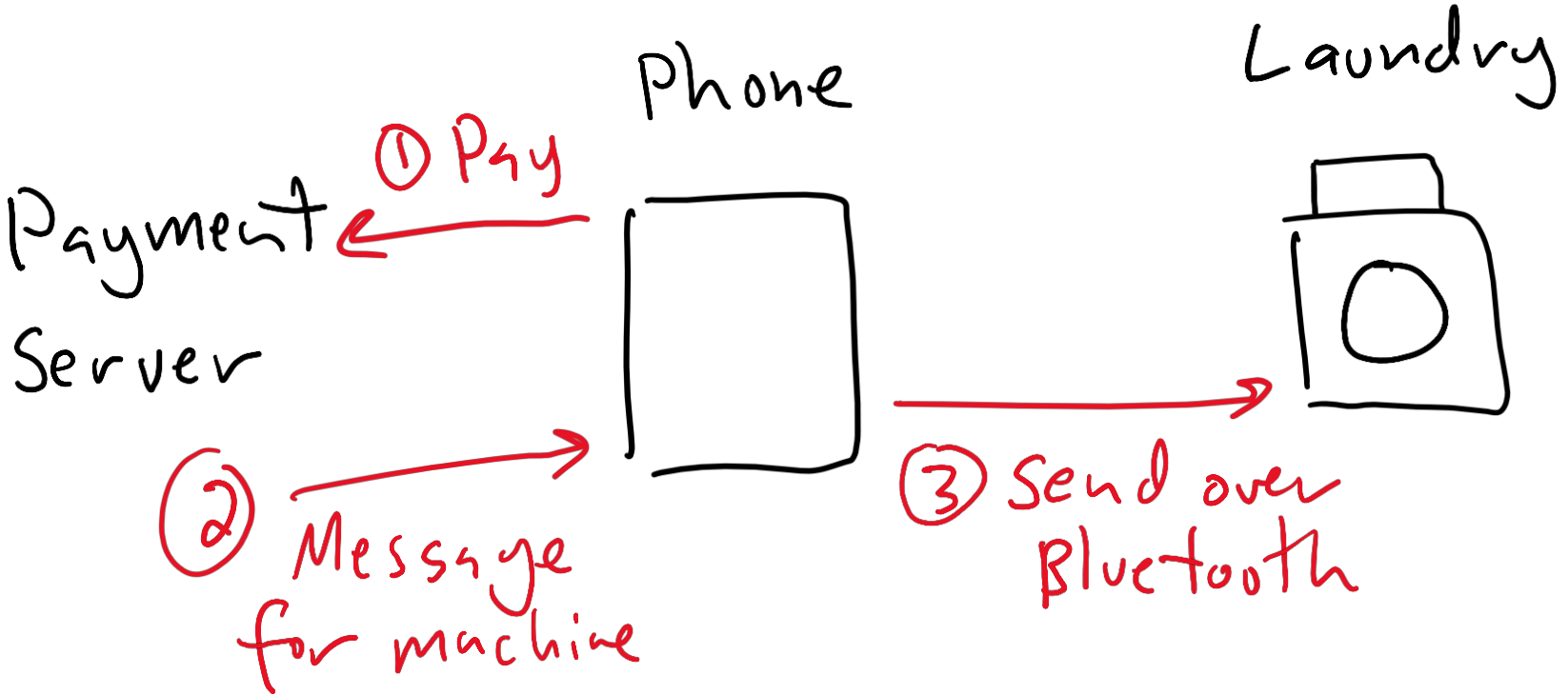
Exercise: Laundry Machine

- At Prof. Kloosterman's old apartment, you can pay for laundry with an app
- The laundry machine is not connected to the Internet and can only communicate with his phone

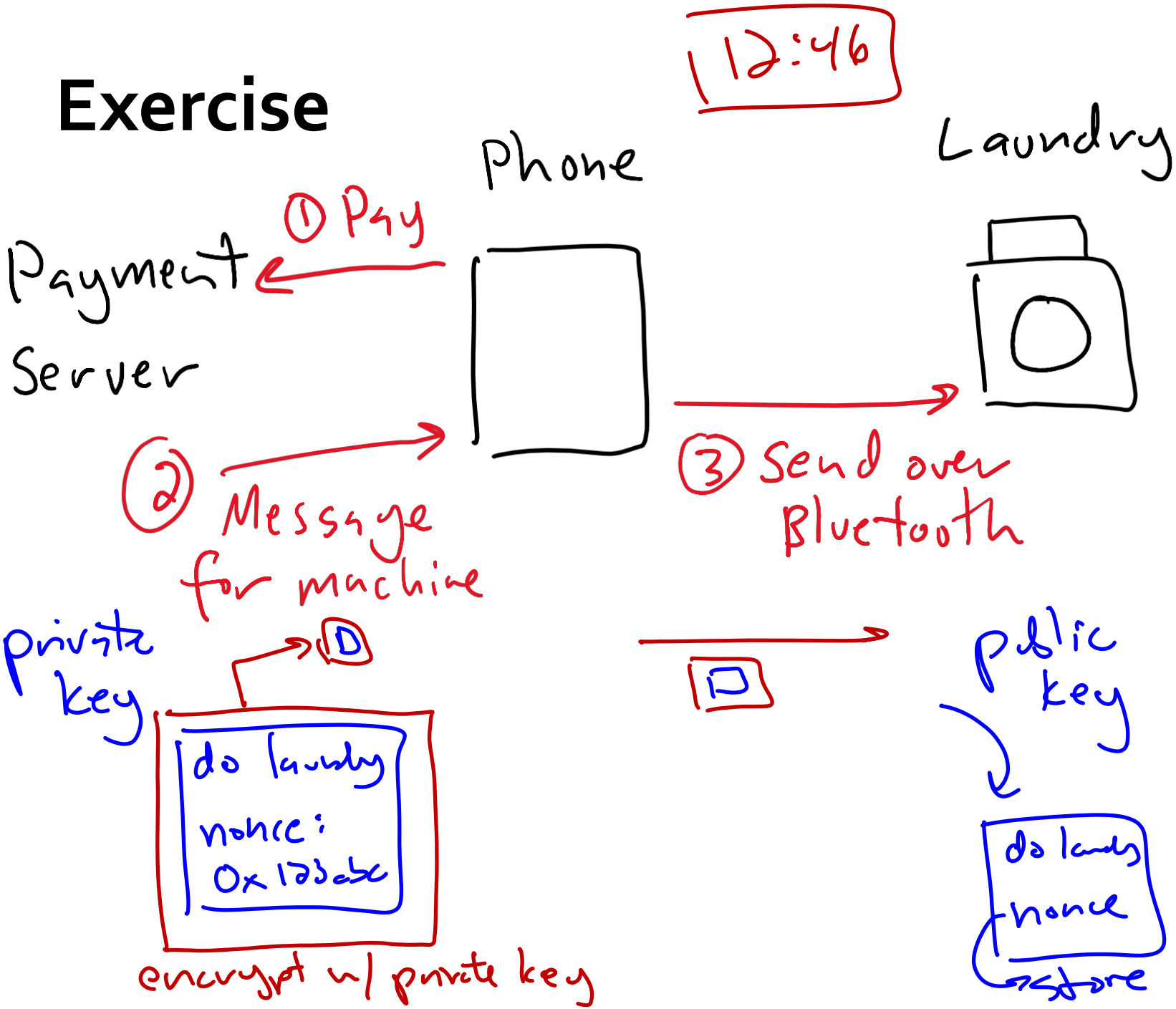


Exercise

- How could you use asymmetric cryptography to make sure I can't create my own Bluetooth messages to get free laundry?



Exercise


12:46
Phone
Laundry
① Pay
Payment Server
② Message for machine
③ Send over Bluetooth
private key
D
do laundry
nonce:
0x123abc
encrypt w/ private key
D
public key
do laundry
nonce
store