**Security of embedded devices:**

In use of embedded devices, we often want an owner to control a device. For example, your smartphone might be the "owner" for your DVD player. Commands from other parties (including previous owners) are to be ignored by the device.

**(a)** Explain how such a device might be programmed to recognize commands from its owner, and only its owner. Show how this can be done with public-key technology.

**(b)** Explain how such a device might be programmed to recognize commands from its owner, and only its owner. Show how this can be done with secret-key technology.

**(c)** Describe a protocol explaining how "transfer of ownership" can be accomplished, under the public-key framework of your answer in part (a).

**(d)** Describe a protocol explaining how "transfer of ownership" can be accomplished, under the classical (symmetric-key) framework of your answer in part (b).