Homework

Design your own protocol for mutual authentication and secure message transmission. You do not need to actually implement the protocol. However, you have to describe it on very detailed level (e.g., what mode of cipher is used, how many blocks are encrypted, what padding is used, when the protocol should abort due to incorrect values, …) and you can use only simple cryptographic primitives available on smart card (e.g., you can use DES cipher, SHA-1 hash function or random generator but not the OPSystem.getSecurityDomain() secure messaging object).
You protocol must provide:

- Mutual authentication between smart card and PC application based on pre-shared symmetric cryptography secret.
- Secure message exchange after authentication – all subsequent commands send to and from smart card after authentication must be confidential and integrity protected.

Few things you should keep in the mind:

- It is not a good idea to use long-term secrets to directly protect ordinary communication.
- Be aware of replay attack.
- What block cipher mode are you using, how the IV is, what type of padding is used.
- How the integrity is protected, is the apdu header and response protected as well?

You have 1 week to complete this task. Submit your description of the protocol (informal language, but detailed description what primitives were used, why and what threat are mitigated by the construction – should be around 1-2 A4 text) into IS before 6.10. (resp. 7.10.) and prepare short presentation (5 minute max.) for 6.10. (resp. 7.10.) lesson. Your design will be discussed and "attacked" by your classmates.