Project C - TPM
Grading Report of
`2de00a5d0d148aec_HA1_solution.pdf`

Grade: $26/8 = 3.25$

1 Assignment 1: Setting up the environment

5/5 points, good description on how to set up the environment. Although the last 2 steps should have been presented as part of the next assignment.

2 Assignment 2: Getting the TPM ready for use

1/2 points, only parts of the EK was presented, not the whole dump of the public key.

2/2 points, complete dump of SRK with the correct command.

3 Assignment 3: Key hierarchy

2/2 Good answer about identity keys.

2/2 Storage keys are the correct answer.

0/2 No, the right answer is Legacy keys.

2/2 No not all keys are possible to create so that the properties described in the table holds, very good.

2/2 The hierarchy is correctly drawn.

4 Assignment 4: Key Migration

2/2 This is correct, although I would phrase the answer with a simple "no", since the child key is no longer non-migratable, which was the point of the question. Either way the answer is correct.

2/2 Correct, `TPM_AuthorizeMigrationKey` is the first command.

2/2 Good and detailed answer to question about the convert blob command.

2/2 Yes `TPM_LoadKey` is correct.

0/2 No the TPM is a passive device, it must be the TSS that transfers tha actual blob.

1/2 The migration commands are not very clear. Also there are some steps missing on TPM2 for loading the actual migrated key.

0/2 The quote did nothing to explain the concept (unless you already know it).

1/2 Correct but a bit thin explanation, I would like to read a bit more on how it does this and what's the difference between it and "normal" mode.

5 Assignment 5: Extending values to PCRs

0/6 This assignment was not completed.

6 Assignment 6: File encryption

0/13 This assignment was not completed.

7 Assignment 7: TPM Authentication

0/8 This assignment was not completed.

8 Assignment 8: Attestation

0/5 This assignment was not completed.

9 Assignment 9: Your first TPM application

0/4 This assignment was not completed.

10 General remarks

The report outline and section numbering is very confusing.