

Project 1

Post-Quantum Access & Character Forge

Individual assignment | Submit privately on Gradescope

Due date: see the Project 1 assignment on Gradescope. Follow course announcements for service availability and generation deadlines.

1. Your task

Build and verify a post-quantum character-access ticket, use it to unlock the course-hosted Character Forge, and create the hero you will use in **King of Security (KOS)**. Your finalized image and matching background will later provide the visual identity and story context for AI-generated combat videos.

You will use the supplied lab script; you do not need to implement a cryptographic algorithm or purchase an API subscription. Run the commands yourself, inspect their output, and understand why an altered ticket fails verification.

Required Gradescope files	What to submit
character-access.ticket	Your original countersigned ticket produced by the lab and accepted by Character Forge.
character.png	The original finalized three-view PNG downloaded from Character Studio.
character-background.txt	The background exported for that same finalized character.

2. Prepare your access

1. Find the course links. Open the [CS253 course homepage](#) and follow the Character Forge link. Connect to the university VPN if required. If it says Coming soon or generation is disabled, wait for the instructor announcement; do not substitute another service.

2. Activate your own account. Use the username and private activation code sent directly and privately by the instructor. Choose your own password; never use another student's account.

3. Confirm automatic course access. Setting your password with a valid activation code activates your course access immediately. Sign in and open the character-access panel. No Gradescope enrollment submission or separate instructor approval is required.

4. Download your lab inputs. Click **Download ticket parts** to save `ticket-parts.json`. Open **Crypto lab** and download `package.json` and `lab.mjs`.

Two different tickets: The numeric QR ticket is only for topic signup. For Project 1, submit `character-access.ticket` from the crypto lab, not the QR ticket.

3. Run the post-quantum lab

5. Prepare a private working folder. Install Node.js 24 and open a terminal. On Windows, use a folder such as %LOCALAPPDATA%\CS253-lab; on macOS/Linux, use a private folder under your home directory. Avoid OneDrive, shared drives and public repositories. Put the three downloaded files in this folder, with their exact names and no extra .txt suffix.

```
node --version
npm --version
npm install
```

Run each command below separately in that folder. The dependency installation requires network access; the subsequent cryptographic commands run locally.

Command	Expected result / action
node lab.mjs keygen	Creates student-secret.json and student-public.json. Keep the secret file private.
node lab.mjs inspect	Prints the issuer-key SHA-256 fingerprint, header and readable claims. Compare the fingerprint with the instructor's trusted announcement. Stop and ask the TA if it differs.
node lab.mjs assemble	Assembles the supplied header, payload and issuer signature into issuer.ticket, and verifies that signature.
node lab.mjs verify	Reports that the issuer signature is valid. Read the expiry information.
node lab.mjs tamper	Writes tampered.ticket by changing a claim without changing the issuer signature. The original remains intact.
node lab.mjs verify tampered.ticket	Enter this as ONE command. It must fail with SIGNATURE INVALID. This expected failure demonstrates tamper detection; continue with the original ticket.
node lab.mjs sign	Countersigns the original issuer ticket with your local key and creates character-access.ticket.

6. Unlock Character Forge. Return to its home page and upload character-access.ticket in the character-access panel. Confirm that course access is verified. Keep this exact file for the final Gradescope submission. Uploading it again does not add generation rounds.

What the signatures demonstrate

The course issuer signs the access claims using **ML-DSA-65**. Your script verifies that signature, then adds your own signature over the original ticket. You are assembling and countersigning an existing authorization, not creating course permission yourself. The website also checks your signed-in account, current access record, expiry and quota.

A signature detects changes; it does not hide the readable claims. Your signature demonstrates possession of your local private key, not independent proof of enrollment. A legacy topic claim may be empty and does not reserve a presentation seat. Keep a local note of why the tampering test failed; no separate report is required for this assignment.

4. Design and generate your character

7. Complete Identity. Choose your course alias, fictional character name, sex, race/species, role and form. Keep your real name and student number out of the character imagery and story. A role describes how the character approaches problems.

8. Complete Backstory. Select the presentation topic matching your separate signup choice. Choose a former occupation, motivation, **meaningful keepsake** and **personal limitation**. The last two are required: they help the later combat animation express your character's behavior and setbacks. Use the choices, Random/Shuffle, or Customized by myself; review the resulting text.

Set **Force, Guard, Insight, Agility and Charm** from 1 to 20 each, totaling **exactly 55**. The defaults are 11 each. These starting attributes are narrative/cosmetic settings, not self-awarded combat power. Your topic dropdown is a declaration, not a seat reservation.

9. Complete Appearance. Choose the broad body, hair, clothing and face details, palette and optional signature accessory. All candidates use the course's common visual style. There is no Research Plan step; prepare the actual presentation separately.

10. Review your choices. Open **Review & export**, read the character background, resolve missing fields and confirm the review checkbox. Do not include real credentials, private messages or other people's personal information in the prompt.

5. Use Character Studio

11. Generate your first batch. Click **Submit & generate five candidates**. Each candidate is one reference sheet containing front, back and right-side views of the same character. Wait for completion; if the status is uncertain, use Refresh status and contact the TA before attempting another request.

12. Compare and revise. Inspect the full-size images and each candidate's background. You may generate **one initial batch plus up to three additional batches**: at most four rounds of five candidates (20 total). You do not need to use every round.

All completed candidates are saved automatically with your course account. New batches preserve earlier images and their backgrounds. Use the Saved image gallery and batch shortcuts to revisit them, including after signing in again. You can choose an image from any saved batch.

You may return to any settings page before the next batch. Use Edit Identity, Edit Backstory or Edit Appearance, or the step navigation at the top. Make changes, return to Review & export, check the details, and generate again. Earlier images are not changed by edits to the current form.

13. Finalize one candidate. Click Choose this candidate, inspect all three views for a consistent face, outfit, limbs and asymmetric details, tick the final-confirmation checkbox, then click **Confirm final character**. Final confirmation locks the selection and ends further generation. Do not confirm until you have compared the candidates you want to consider.

14. Download the matching artifacts. Under **Your character is ready to download**, use **Download three-view PNG** and **Download character background**. Also save **Download reference details** (JSON) locally for your records. Use the finalized character's exports, not text from a later edited draft or another batch.

6. Submit Project 1 on Gradescope

15. Prepare these three files. Rename the exported image/background for clarity as shown below. Do not edit or reformat the ticket contents.

Filename	Final check
character-access.ticket	This is the file produced by node lab.mjs sign and accepted by the website, not issuer.ticket or tampered.ticket.
character.png	The original finalized PNG contains all three character views. Submit the image file, not a screenshot of the website.
character-background.txt	The exported text belongs to the exact same finalized candidate and includes its character background, keepsake and limitation.

16. Upload privately. Submit all three files to the **Project 1** assignment using your own enrolled Gradescope account. If its upload interface requires a single archive, put only these three files in project1.zip. Reopen the submission and verify that all files are present and readable.

17. Keep your originals. Retain your ticket, finalized PNG, background TXT and optional reference JSON. The image and story will be used together as character references for later combat simulation/video production. Reusing another student's ticket, image or story is not permitted.

Never submit: student-secret.json, passwords, API keys, the entire lab folder, or the instructor's ticket register. Do not post access tickets or private key material on the public course website or Piazza. The required character-access.ticket is submitted only through the designated private Gradescope assignment.

Completion criteria

Your submission must contain a valid course-account access ticket with your countersignature, one finalized three-view image, and its matching background text. Complete the verification and deliberate-tampering steps yourself. No separate written report or additional screenshots are required. Follow the Project 1 rubric and deadline published on Gradescope; this sheet does not introduce a new course-grade weighting.

Troubleshooting

Problem	Action
Ticket parts or image service unavailable	Check that your account is activated and read the course announcement. Contact the TA if the service is not enabled; do not buy personal API access to bypass it.
SIGNATURE INVALID for tampered.ticket	Expected. Keep issuer.ticket unchanged and continue with node lab.mjs sign. If the original fails, stop and ask the TA.
File exists / EEXIST	Commands refuse overwrites. Preserve your existing outputs and keys; use a new private folder for a fresh attempt rather than overwriting originals.
Ticket rejected or generation uncertain	Use the same activated account and current unexpired packet. Refresh status and contact the TA; do not create accounts to reset quotas.
Wrong image/background pair	Download both again from the finalized character's download area. Do not use the current form's draft background instead.

Help: use Piazza for general questions and the course's private channel for account-specific problems. Follow the course academic-integrity rules when using AI or external resources.