Semester Break Challenge: Design • Deceive • Discover

Create an interlocking, multi-layer puzzle chain. Outsmart rival teams. Surface the group that sees the whole.

Overview

In this assignment, each team designs exactly one stage of a larger puzzle. You receive a defined *input* and a required *output*. Your stage must be solvable, auditable, and thematically coherent. Most importantly: stages depend on one another, forcing cross-team thinking.

You may embed deliberate red-herrings. However, every misleading element must be documented in your private design dossier and must not violate the **ethics rules**.

cryptography steganography OSINT curriculum design

Teams & Roles

Form self-selected teams of 3–6. Recommended roles: Puzzle Architect, Cryptography Lead, OSINT/Research, QA/Playtest, Documentation, DevOps (hosting, mirrors). Smaller teams may combine roles.

- Each team receives: (a) an **Input Artifact** (e.g., book page hash, image EXIF, GPS pair) and (b) a **Target Output** (e.g., a 43-char token).
- Teams know neither the upstream nor downstream stages. Design assuming adversarial interpretation.
- Your stage should be solvable within 2–6 hours by a capable group, assuming clean reasoning.
- Cross-team collaboration is not banned, but direct disclosure of private dossiers is prohibited.

Rules

- Single, verifiable solution for each stage; provide a grader script or step-by-step solution.
- Document any red-herrings; no doxxing, harassment, illegal access, or unsafe venues.
- Use only publicly accessible datasets or original content with clear attribution/license.
- No mass-messaging the public; any physical placement must be lawful and reversible.
- Silence policy: no public posts, videos, or write-ups until the debrief date.
- Accessibility: provide an alternate path or hint for color-blind or assistive tech users.

Task Specification

Your stage must include:

- Theme hook (e.g., poem line, historical inscription).

- Primary mechanic (e.g., Vigenère variant, image LSB stego, book cipher).
- Input contract and output contract (exact format, length, charset).
- At least one *signal* that distinguishes the correct path from attractive decoys.
- A **validation artifact** (checksum, signature, or verifier URL with rate-limit).
- A **private design dossier** (PDF/Markdown) with full rationale and solution.

Misdirection Case Studies (illustrative)

Below are example tactics teams historically used to nudge rivals onto elegant dead-ends. Use ethically; document all decoys.

Psychological Framing

Seed a quote that flatters a rival's known interests (e.g., occult lines) but hashes to the wrong book edition unless they checksum the source.

Signal vs. Noise

Hide a tiny checksum mismatch in a widely shared image; only careful solvers notice the EXIF time-zone offset that fixes the key.

Collaboration Trap

A clue that seems to demand many solvers (e.g., crowd OCR) but is solvable solo if one spots a monospace alignment cue.

Map Illusion

GPS looks like locations; actually it encodes a cipher key via lat/long deltas when sorted by UTC capture time.

Timeline

—	Milestones
Week 1	Kickoff, team forming, input/output contracts issued
Week 2–4	Design & prototyping, ethical review check-in
Week 5	Internal playtest with a blinded peer team

—	Milestones
Week 6	Finalize stage, submit dossier & verifier
Week 7–8	Integrated chain run, leaderboard, debrief prep
Week 9	Debrief (closed), postmortems published to class

Deliverables

Evaluation (100 pts)

Criterion	Description	Pts
Solvability & Rigor	Clear path, verifiable logic, no ambiguity	30
Interdependence	Meaningful links to other stages (inputs/outputs)	15
Creativity	Original theme/mechanics; elegant reveals	15
Ethics & Safety	Compliance with rules; responsible design	15
Misdirection Quality	Decoys are fair, documented, and avoid harm	10
Documentation	Dossier clarity, verifier quality, README	15

Tools & Resources

Suggested stacks (non-exclusive): Python (cryptography, Pillow), Go/Rust for verifiers, Git for versioning, image/audio editors, and safe hosting (Netlify, university servers).

- GitHub Classroom / GitLab groups; private repos during the silence window.
- Verifier templates: `Python/Flask`, `Go/Fasthttp`, `Rust/Actix`
- Checksum tools: `sha256sum`, `shasum`, `certutil`
- Media:

Ethics & Conduct

- No personal data harvesting, no stalking, no lock-picking, no trespass.
- No public panic: avoid misleading emergency symbols or sensitive sites.
- Credit authorship; observe licenses when embedding or linking media.
- Graceful failure: provide hint gates to prevent solver burnout.

FAQ

Can we collaborate across teams?

You may, but you must not share private dossiers or solutions verbatim. Collaboration should emerge from inference, not leakage.

Are physical clues required?

No. If used, they must be lawful, safe, and reversible with photos and coordinates documented.

What if a stage becomes unsolvable?

Provide a failsafe hint via the verifier after N incorrect attempts or after a time window.

What counts as a fair red-herring?

It should be attractive yet defeatable by method (checksums, provenance, units), not by luck. Document it.