#Description: Course notes

Smart Contract Design Principles (Securitywise)

- less Code == less bugs
- Move complexity offchain wherever possible
    - less gas
    - less things to directly worry about
- avoid for/while loops
- Limit Expected Inputs
    - think of possible edge-cases and eliminate/handle them
    - be explicit about what users are allowed to do
- handle all cases despite having precautions in place
- AVOID parallel data structures
    - Use 1 data structure to track 1 thing

External Call Safety

BEST CASE:

- Only made to trusted addresses
- Only made by trusted Roles
- Inputs not Arbitrarily controlled by users

ALWAYS

- Think About
    - Reentrancy
        - CEI
        - Add nonReentrant whereever possible
        - think about Read-Only Reentrancy
        - Think about multiple contract Read-Only Reentrancy
        - Think of how it works if someone builds on top of this contract (composability)
    - DoS
        - Fails
        - Forced Reverts
    - Return Values
        - Check for all possible values(Unexpected bytes)
        - DO NOT copy return data from untrusted calls (Return bombs)
    - Gas
        - If not trusted forward limited gas

Post Checks

Checking state of contracts after external calls can also lead to thier own complications.