Course Organization

1) Classical Crypto (before computers)
2) Modern Private Key Crypto (computers share a key)
3) Modern Public Key Crypto (computers don't have to meet, keys are used)
4) Odds + Ends (group key management, quantum crypto, hash functions)

Caesar Cipher

HELLO +3 KHOOR

\[ f(x) = (x + 3) \mod 26 \]

Numerically, each letter is assigned a number 0-25. A=0, B=1, C=2, ..., Z=25.
mod is remainder, so $27 \mod 26 = 1 \rightarrow B$

To decrypt, $f(x) = (x - 3) \mod 26$

Shift Cipher → instead of adding 3, we add the secret key, $k$, $0 \leq k \leq 25$, but $k=0$ would be pretty silly!

E: $f_k(x) = (x + k) \mod 26$

D: $f_k^{-1}(x) = (x - k) \mod 26$