8/22/2022

CIS 3362

Arup Guha

Course Webpage

Course Organization

1) Classical Crypto (before computers)

2) Modern Private Key Crypto (computers, 2 people share a secret key)

3) Modern Public Key Crypto (computers, 2 people don't have to meet, keys are used)

4) Odds + Ends (group key management, quantum crypto, hash functions)

Caesar Cipher

HELLO

+3 KHOOR

numerically each letter is assigned a number 0-25.

A=0, B=1, C=2, ... Z=25

$f(x) = (x+3) \bmod 26$ → equivalence relation

% → operators single answer

mod is remainder, so $27 \bmod 26 = (1) \rightarrow B$

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

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

$$E \quad f_k(x) = (x + k) \bmod 26$$

$$D \quad f_k^{-1}(x) = (x - k) \bmod 26$$