MATHEMATICS 4440/5440
CRYPTOSYSTEM ORGANIZER

Cryptosystem: Caesar Cipher

Plaintext space: $(\mathbb{Z}/26\mathbb{Z})^* =$ strings of integers mod 26

Ciphertext space: $\mathbb{Z}/26\mathbb{Z}$ (same)

Key space (and its size): $\mathbb{Z}/26\mathbb{Z} = \{0, 1, \ldots, 25\}$

Encryption:

If key $= k$, encryption is character-by-character

$$x \bmod 26 \longmapsto x + k \bmod 26$$

Decryption:

If key $= k$, decryption

$$x \bmod 26 \longmapsto x - k \bmod 26$$

Example: see slides

Ciphertext only attacks:

Known plaintext attacks:

Chosen plaintext attacks:

Chosen ciphertext attacks: