MATHEMATICS 4440/5440
CRYPTOSYSTEM ORGANIZER

Cryptosystem: Affine Cipher

Plaintext space: $(\mathbb{Z}/26\mathbb{Z})^{str}$

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

Key space (and its size): $(\mathbb{Z}/26\mathbb{Z})^{*} \times \mathbb{Z}/26\mathbb{Z}$ these are α's that have inverses

size $= 12 \cdot 26 = 312$

Encryption:

key $= (\alpha, \beta)$

$p \longmapsto \alpha p + \beta \pmod{26}$

Decryption:

key $= (\alpha, \beta)$ figure out α^{-1}

$c \longmapsto \alpha^{-1}(c - \beta) \pmod{26}$

$= \alpha^{-1} c + (-\alpha^{-1}\beta)$ ← decryption is encryption w/ key $= (\alpha^{-1}, -\alpha^{-1}\beta)$ "decryption key"

Example: → see notes

Ciphertext only attacks: exhaustive search (312 keys)

frequency analysis (permutation of histogram bars)

Known plaintext attacks: → see hmwk.

Chosen plaintext attacks: Choose plaintext $AB = (0\ 1)$

$0 \longmapsto \alpha \cdot 0 + \beta = \beta$

$1 \longmapsto \alpha \cdot 1 + \beta = \alpha + \beta$

$\beta =$ ciphertext(0)

$\alpha =$ ciphtxt(1) − ciphtxt(0)

Chosen ciphertext attacks:

Choose $AB = (0,1)$ as ciphertext.

Same analysis: get decryption key