DTTF/NB479: Dszquphsbqiz Day 7

- Announcements:
  - Matlab tutorial linked to in syllabus
- Questions?
- Today:
  - Substitution ciphers
  - Matrix inverses
  - Hill ciphers

Block Ciphers

- So far, changing 1 character in the plaintext changes ___ character(s) in the ciphertext.

- Shannon outlined qualities of good ciphers:
  - *Diffusion:* Changing one character of the plaintext changes _____ characters in the ciphertext
    - **Makes frequency analysis much tougher!**
  - *Confusion:* Each character of the ciphertext interacts with several parts of the key

- ***Block ciphers*** have both qualities:
  - DES (64 bits), AES (128 bits), Hill ciphers (smaller; today)

Hill Ciphers

- Lester Hill, 1929. Not used much, but is historically significant: first time linear algebra used in crypto
- Use an *n* x *n* matrix M. Encrypt by breaking plaintext into blocks of length *n* (padding with x's if needed) and multiplying each by M (mod 26).
- Example: Encrypt "hereissomeonetoencrypt" using M

$$M = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{bmatrix}$$

- **her eis som eon eto enc ryp txx**
- (7, 4, 17) (4, 8, 18) … (19, 23, 23)

$$\begin{pmatrix} 7 & 4 & 17 \end{pmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{bmatrix} \equiv \begin{pmatrix} 2 & 5 & 25 \end{pmatrix} \bmod 26$$

- (2, 5, 25) (0, 2, 22) … (0, 22, 15)
- **cfz acw yga vns ave anc sdd awp**
- **"CFZACWYGAVNSAVEANCSDDAWP"**

Decrypting

- Reverse the process, multiplying each block by M inverse (mod n)

- *Theorem:* If a matrix M is invertible mod n, then gcd(det(M), n) = 1
- Proof on board

Modular matrix inverse (§3.8)

- The Hill cipher requires us to invert a matrix mod 26.
- For a 2x2 matrix, this is easy.
- Many numerical packages allow us to invert a matrix, but using floating point numbers.
- How do we combine the two?
  - Demo of my code

How to break via known plaintext?

- Answering Q7 preps you to do 2.13 #14 on HW2 if you want to earn an early day
- You may leave when done