CIS 3362 9/18/24

1. Transposition + Double Transposition Explanation
2. Code Trans. (with functions)
3. Quiz 2 Info

Transposition

Keyword: YELLOW

6 1 2 3 4 5
T O D A Y I
S W E D N E
S D A Y S E
P T E M B E
R E I G H T
E E N T H

MSG:

TODAYIS
WEDNESDAY
SEPTEMBER
EIGHTEENTH

35 letters

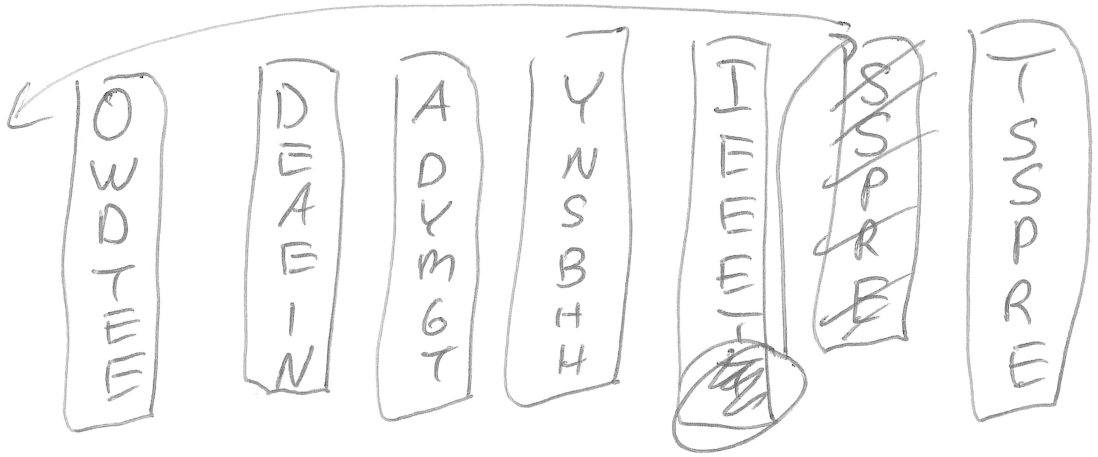
Ciphertext: Read columns in numerical order.
Column Labeled 1, followed column labeled 2, etc.

OWDTEE DEAEIN ADYMGT YNSBHH IEEBTT SSPRE

C1 C2 C3 C4 C5 C6

To break: Step 1 - Guess keyword length

Imagine we guess 6 keyword length



Double transposition is apply a new key word to the output from the 1st keyword.

Key 2: ~~CA~~ F R O G

1 4 3 2

O W D T

E E D E

A E I N

A D Y M

G T Y N

S B H H

I E E E

T T S S

P R E

OWDTEE

DEAEIN

ADYMGT

YNSBHH

IEEET

TSSPRE

Double Trans: OEAAGSITP TENMNIHES DDIYYIHESE

C1 C2 C3

WEEDTBETR

C4

Quiz 2 Topics

Playfair
Hill
ADFGVX
Enigma
Navajo Code
Transposition

Playfair

how to encrypt/decrypt with key and also if I tell you a different padding char.

- Repeat letters in keyword
- I/J
- Padding char
- Double letters in plaintext

Hill

key matrix (gen n×n matrix)
2×2 for exam

encrypt/decrypt with key

2×2 (Give you encryption key ask find decryption key
↳ 26 (look up chart), not 26 ⇒ EEA (extended Euclidean Algorithm)

2 pairs of matching plain/cipher text set up mod equations to solve for ~~# of po~~ possible keys.

ADFGUX

about a portion of encryption or decryption OR maybe conceptually how a part of it works.

Enigma

Read typed notes story...

Itigh level design of machine

DAY CODE → published "book" for year.

MSG CODE → encrypted twice for each msg.

3 scramblers → 5 scrabbers : added # configuration

How allies broke it → weather report, Rejewski analyzing the cycles in the permutations, operators who used same msg code over + over again.

Navajo Code

Itistory - why, who proposed it, how the code works. Anything covered in the typed notes.

Transposition

By hand encrypt or decrypt given the key.