CIS 3362 9/20/21

1. OH today VIRTUAL 3-4pm (9/20)
2. Navajo Code
3. Transposition
4. Give you more letters for playfair

Generated 274 code words.
Training - 30 code talkers
Initially confusion because of poor planning!
Contest - race between 2 Navajo + the usual machine system.

1942-1945 420 Code Talkers
Most Important Battle: Iwo Jima Feb/March 1945

Japanese admitted they had broken most of the US codes, but not the Navajo.

Neat CS Connections via language

- Chomsky Normal Form (context free grammars)
  - Earliest posited idea of a Universal Grammar.
- Information Theory - Entropy (measure of disorder)

Transposition

(1) Permutation Cipher (precursor)

keyword: COMPUTER → 0 3 2 4 7 6 1 5

perm: 6,2,1,5,3,7,4,0

Plaintext: ITISVERY|HOTOUTSI|DETODAYX|

→ ISIVYRTEHOTUISOTDOTDXYEA

permutation tells me which letter to grab in the block

---

(2) Single Transposition

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

C O M P U T E R

0 3 2 4 7 6 1 5

I T I S V E R Y

H O T O U T S I

D E T O D A Y

I H D R S Y I T T T O E S O O Y I E T A V U D

0 1 2 3 4 5 6 7

0 3 2 4 7 6 1 (5) ← short

I T I S V E R Y

H O T O U _ S I

D E T O D A Y .

msg len = 23

key len = 8

7 cols long

1 short

How to break

Guess keyword length write out columns out of order

try to reorder columns to form word at top.