CIS 3362  9/20/21

1. OHT today VIRTUAL 3-4 pm (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.

Next CS Connections via languages

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
   - perm: 6, 2, 1, 5, 3, 7, 4, 0
   - Plaintext: IT IS VERY HOT OUTSIDE TODAY
   - ISIVYRTEHOTUISOTDOTOXYEA
     permutation tells me which letter to grab in the block

2. Single Transposition
   - COMPUTER
   - 0 3 2 4 7 6 1 5
   - IT IS VERY HOT OUTSIDE TODAY
   - IHORSYITTOESOXYETAVUD
     0 1 2 3 4 5 6 7
     0 3 2 4 7 6 1 5
     IT IS VERY HOT OUTSIDE TODAY
     msg len = 23
     key len = 8
     7 cols long
     1 shot
How to break

Guess keyword length, out of order:

```
 H  S  T  o  I  T  U
 D  Y  T  E  O
   ↑
guess
shot
```

Write out columns, try to reorder columns to form word at top.