

9/30/19 (1)

Navajo Code

Philip Johnston - military aware
Navajo language (brought up idea of
using Navajo).

- Navajo was chosen as there was
no proof any Germans knew Navajo
(but there was for the other possibilities)

Staged demo: 4 Navajo, just speaking
back & forth. - everyone impressed
speed/accuracy of communication.

Train 30 Navajo to work in a single
"group".

Bootcamp - (1) usual bootcamp stuff

(2) Develop the code.

- Initially 211 code words
make substitutions that
are easy to memorize
- Letter codes

"a" → ape, apple, ...

"b" → bacon

What about freq analysis?

Summer
1942

Best Known Success of Navajo Code 9/30/19 ②

Iwo Jima (early 1945)

discuss how in the 1st 24 hrs

Code Talkers sent over 800 messages.

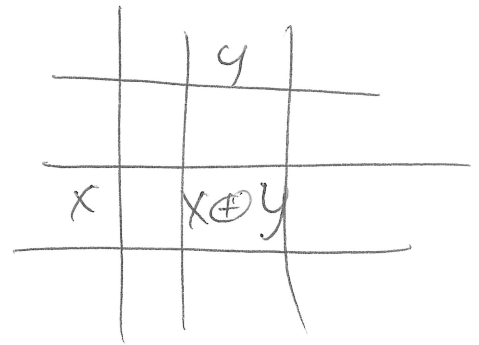
- Some generals say that the Allies would not have won Iwo Jima w/o the code talkers.
- Even though a lot of people died, it's estimated that the battle ultimately saved lives as it hastened the end of the war.

Bitwise Operators

Most modern plaintext will be bits.

Plaintext: 1001 0101 95
1101 0110 D6

XOR: $\begin{array}{r} \text{code} \\ \downarrow \\ 1100 \\ \oplus \text{books} \rightarrow 10101 \\ \hline 1001 \end{array}$ $\begin{array}{r} C \\ \oplus 5 \\ \hline 9 \end{array}$



and $\begin{array}{r} \downarrow \\ 1100 \\ \& 1010 \\ \hline 1000 \end{array}$ $\begin{array}{r} C \\ A \\ \hline 8 \end{array}$

or $\begin{array}{r} \downarrow \\ 1100 \\ | 1010 \\ \hline 1110 \end{array}$ $\begin{array}{r} C \\ 1A \\ \hline E \end{array}$

$\sim 1100 = 0011$ Flips each bit

ONE-TIME PAD

Message: 0110 1010 1110 0001

1Time Pad: $\oplus$ 1000 1110 0101 0110

Cipher $\rightarrow$ 1110 0100 1011 0111

Input $\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ \uparrow \uparrow \uparrow \uparrow & \uparrow \uparrow \uparrow \uparrow \end{array}$

perm = (5)(2)(3)(1)(2)(8)(4)(6)

Output 11010011