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: it Navajo, just speaking back & forth. - everyone impressed speed/accuracy of communication.
Train 30 Navajo to work in a single "group".

Boot camp - (1) usual bootcamp stuff
(2) Develop the code.

- Initially all code words make substitutions that are easy to memorize
- Letter codes
  "a" → qpe, apple,...
  "b" → bacon

What about freq analysis?
Best Known Success of Navajo Code

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 1101 0110

XOR: \[ \begin{array}{c}
1100 \\
0101 \\
\hline
1001
\end{array} \]

AND: \[ \begin{array}{c}
1100 \\
1010 \\
\hline
1000
\end{array} \]

OR: \[ \begin{array}{c}
1100 \\
1100 \\
\hline
1110
\end{array} \]

\[ \neg 1100 = 0011 \text{ flips each bit} \]

ONE-TIME PAD

Message: 0110 1010 1110 0001

One-Time Pad: 01000 1110 0100 0110

Ciphertext \( \rightarrow \) 1110 0100 1011 0111

Input 1001 1110 perm = 5031264

Output 11010011