



현대 전쟁사에서 유일하게 깨지지 않은 암호

# 나바호 코드 토크

고우종

[jstrane@gmail.com](mailto:jstrane@gmail.com)

# 목차

1. 나바호 코드 토크 소개
2. 영화 <윈드토크>
3. 암호 개발 배경
4. 언어적 특징
5. 암호적 특징
6. 암호 구성방식과 실제 예
7. 암호의 장단점
8. 정리

# 나바호 코드 토크란?

- 제2차 세계 대전 당시 미군이 고안해낸 자연어를 이용한 암호를 구사하는 암호병
- 북 아메리카 대륙의 원주민인 나바호 인디언들의 나바호어 사용
- “해독되지 않은 언어는 그 자체로 암호다.”

# 나바호 암호 소개

- 어족이 다른 언어의 생소한 음성을 듣고 이해하는 것은 굉장히 어려운 작업
- 로제타 석이라는 문자로 기록된 자료를 가지고도 수십 년에 걸친 노력이 필요했던 이 집트 상형문자의 해독과 유사
- 결과적으로 현대 전쟁사에서 유일하게 깨지지 않은 암호!

# 나바호 코드 토키 사진

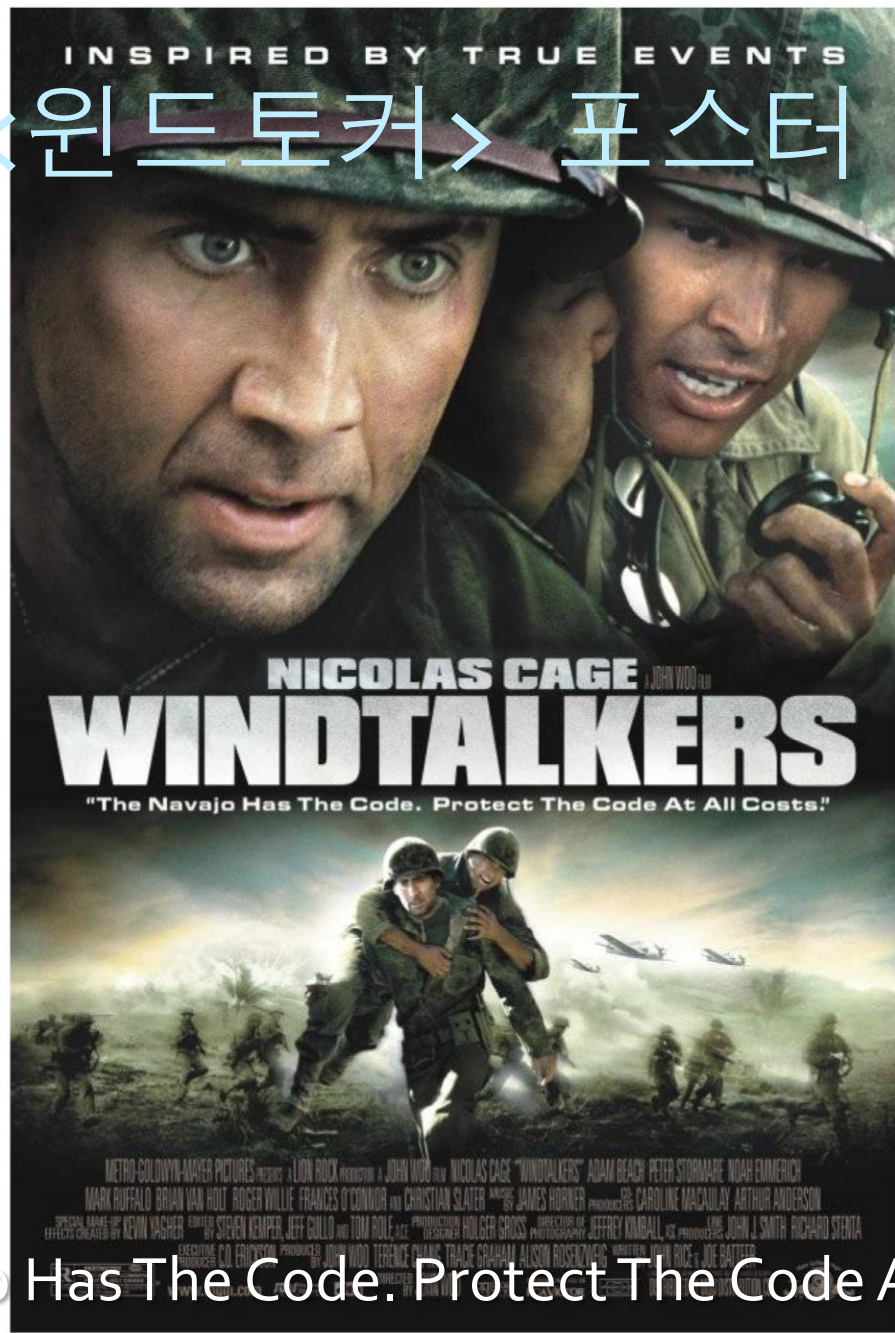


Original 29

# 영화 <윈드토키>

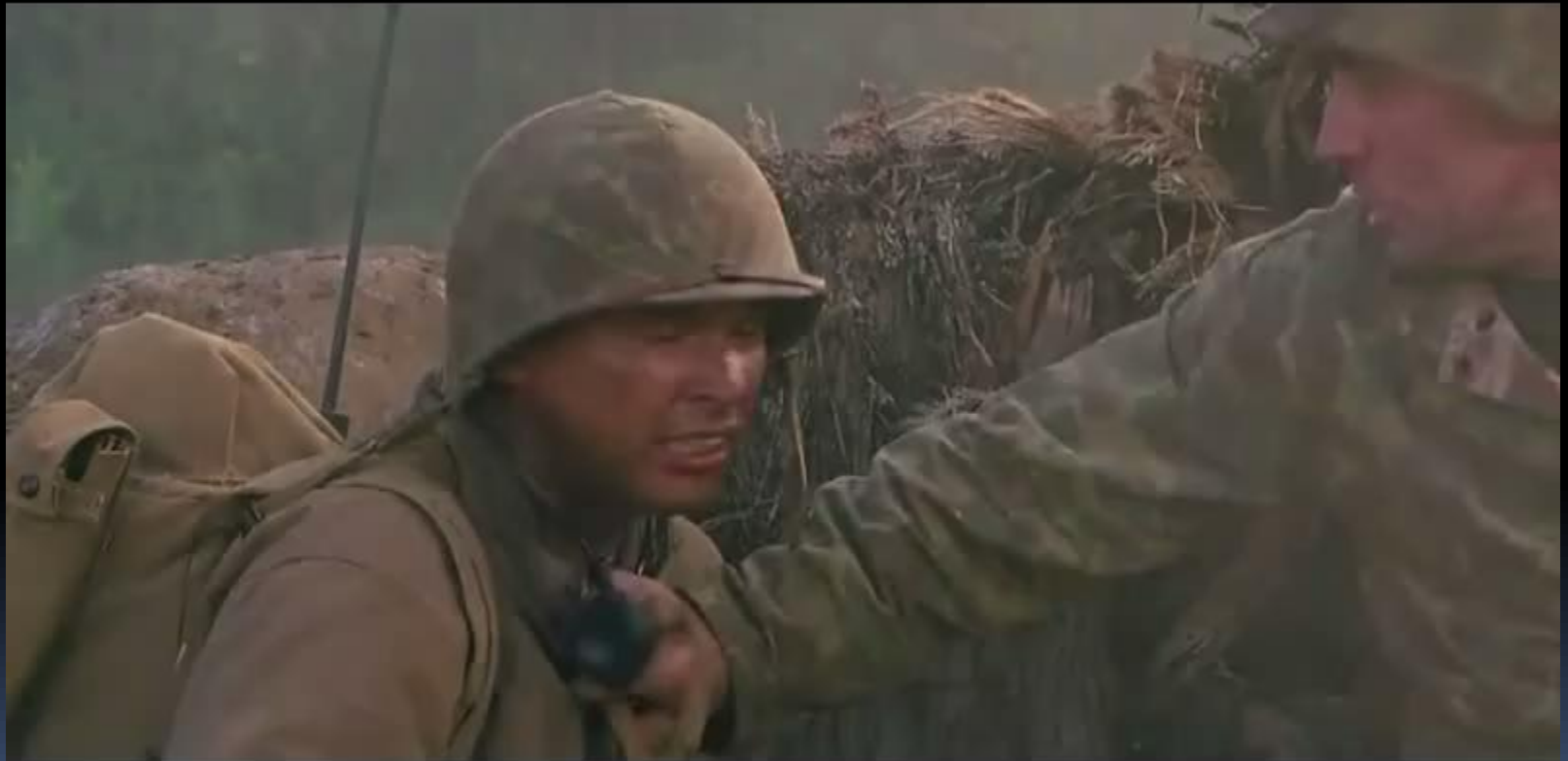
- 나바호 코드 토키들은 동양인과 비슷한 외모 때문에 종종 아군이 일본군으로 착각
- 체포될 때마다 아군임을 설명해야 했기에 백인 병사가 개인 경호를 맡음
- 하지만 유사 시에는 암호의 보호를 위해 이들을 없애도 좋다는 명령 → 영화화

영화 <윈드토키> 포스터



"The Navajo Has The Code. Protect The Code At All Costs."

# 영화 <윈드토키> 영상



# 나바호 암호 개발의 배경

- 일본군은 당시 미군이 사용했던 거의 대다수의 암호를 해독
- 해독 후 거짓 명령을 암호로 전송하여 동맹군에게 큰 피해 입힘
- 더욱 복잡한 암호를 도입하게 되면서 단문 암호화에도 2시간 이상 소요
- → 전혀 새로운 암호화 방식의 필요성 대두!

# 나바호어 기반 암호 제안

- 나바호 인디언 보호 구역에서 거주하던 **Phillip Johnston**
- 그는 당시 30명도 채 안 되던 나바호어에 통달한 외지인 중 한 명



# 나바호어 기반 암호 제안

- 나바호어에는 문자가 없고, 유아기에 습득하지 않으면 배우기가 거의 불가능임을 깨달음
- → 사령부에 나바호어를 암호로 사용하는 방안을 제안하여 수락됨



# 나바호어의 언어적 특징

- 이름 : Diné bizaad (디네 비자드)
- 사용 국가 : 미국 (애리조나 주, 뉴멕시코 주)
- 사용 지역 : 북아메리카
- 언어 인구 : 17만 8천 명
- 언어 계통
  - 나데네어족
    - 아타바스칸어족
      - 남 아타바스칸어족 (아파치)
        - 나바호어

# 나바호어의 언어적 특징

		양순음	치경음		치경 구개음	연구개음		성문음
			중앙음	측음		평음	순음화	
파열음	평음	b [p]	d [t]			g [k]		' [ʔ]
	기식음		t [tʰ]			k [kx]	kw [kx <sup>w</sup> ]	
	방출음		t' [t']			k' [k']		
파찰음	평음		dz [ts]	dl [tl]	j [tʃ]			
	기식음		ts [tsʰ]	tʃ [tʃʰ]	ch [tʃʰ]			
	방출음		ts' [ts']	tʃ' [tʃ']	ch' [tʃ']			
계속음	무성음		s [s]	ʃ [ʃ]	sh [ʃ]	h [x]	hw [x <sup>w</sup> ]	h [h]
	유성음		z [z]	l [l]	zh [ʒ]	gh [ɣ]	ghw [ɣ <sup>w</sup> ]	
비음		m [m]	n [n]					
접근음					y [j]		w [w]	

쇄두음				λ [l]		ʌ [ʌ]	
-----	--	--	--	-------	--	-------	--

# 나바호 암호의 암호적 특징

- 가장 큰 암호적 특징은 자연어 자체를 암호화 방식으로 사용했다는 것
- 다른 언어의 익숙하지 않은 소리들을 정확하게 구분하는 것이 거의 불가능
  - 언어별로 대립이 있는 음운이 서로 다름
  - 나바호어에는 일본어에는 없는 성조가 있음

# 나바호어가 암호로 적합한 이유

- 아시아나 유럽의 언어와 아무런 관련이 없는 나데네 Na-Dene 어족이기 때문
- 동사 중심 언어
  - 나바호어의 동사는 주어뿐만 아니라 목적어에 따라서도 변화

분리 접사					연속 접사						동사 어간
0	1a	1b	2	3	4	5	6	7	8	9	10
전치사 목적어	"제로 전치사"	부사어구- 어간형성모음	반복	복수	직접목적어	지시사	부사어구- 어간형성모음	범- 시제	주어	분류사	어간

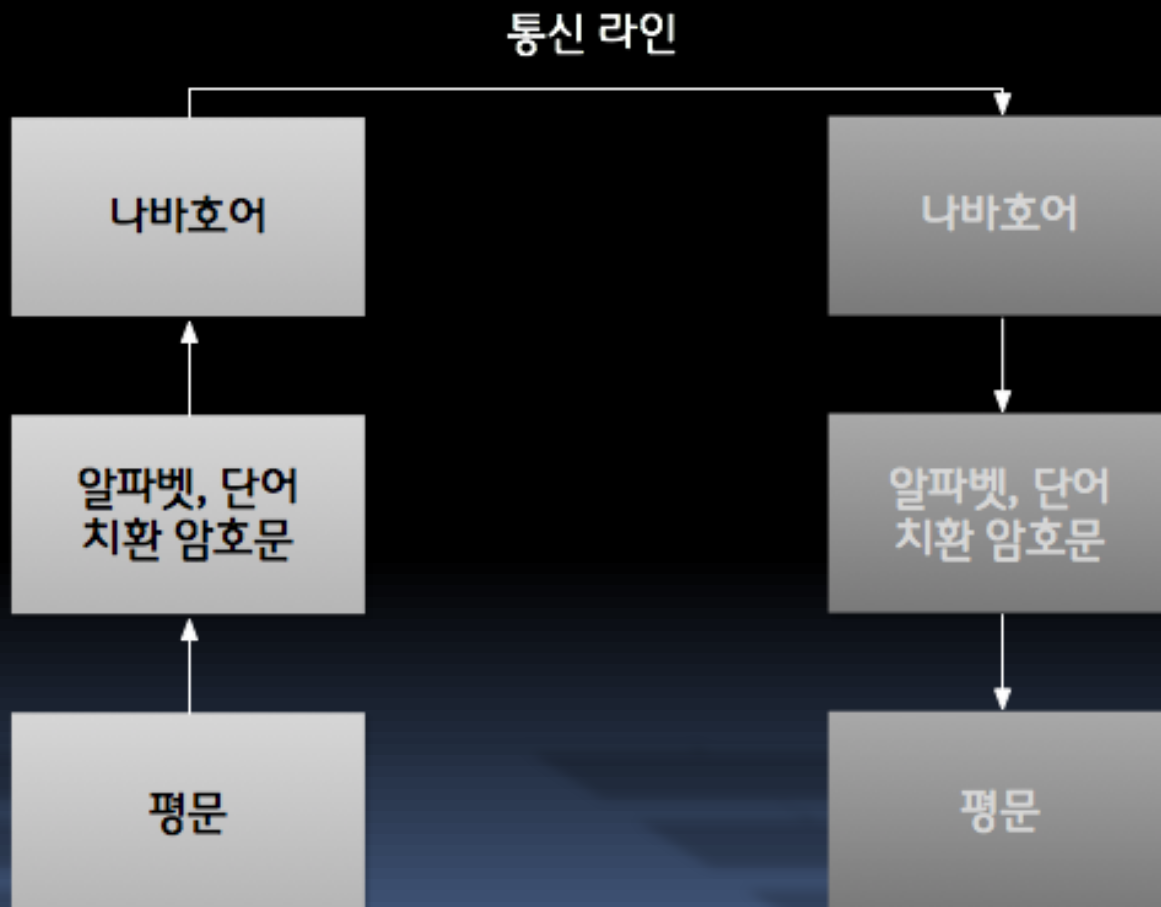
# 나바호어가 암호로 적합한 이유

- 아래와 같은 이유로 당시 나바호 인디언 외에는 이 언어를 배운 사람이 거의 없었다.
  1. 나바호어에는 문자가 없음
  2. 나바호어에 대한 책이 출판된 적 없음

# 나바호어가 암호로 적합한 이유

- P.199 미해군 소속 암호 해독가들은 나바호어로 된 암호문을 이렇게 표현했다. “괴상한 연구개음, 비음과 발음하기 힘든 여러 음절의 연속으로 이루어진 소리..... 해독은 커녕 받아적기도 힘들었다.”
- 네이티브 스피커와의 발음 차이 때문에 앞서 이야기한 거짓 명령 발송 가능성 차단
- + 추가적인 알파벳 암호화

# 나바호 암호 계층도



# 암호 구성 방식

- 나바호 단어들을 조합해 수백 개의 군사 용어에 해당하는 구체적인 암호를 구성
  - ▣ 해군 부서 → 나바호 씨족 이름
  - ▣ 선박 → 물고기 이름
  - ▣ 비행기 → 새 이름
- 철물고기 '베쉬-로' → 잠수함
- 벌새 '다-헤-티' → 전투기

# 암호의 실제 예

## 사물의 유사성을 이용한 암호화

영어 단어	나바호어 단어	뜻
급강하 폭격기	Gini	말뚝가리
탱크	chay-da-gahi	거북이
정찰기	Me-as-jah	올빼미
호주	Cha-yes-desi	말린 모자
독일	Besh-be-cha-he	강철 모자

## 메타포를 이용한 암호화

영어 단어	나바호어 단어	뜻
미국	Ne-he-Mah	우리들의 어머니

# 암호의 실제 예

지명, 인명 등을 위한 알파벳 암호화

영어 알파벳	나바호어 단어	뜻
A	Tse-nill	Ax
B	Shush	Bear
C	Moasi	Cat
D	Be	Deer
...	...	...

“BAD”를 암호화 한 예

B	A	D
Shush	Tse-nill	Be
Bear	Ax	Deer

# 장점

1. 빠른 암호화와 복호화 속도
2. 높은 정확도와 신뢰도
  - 사이판 전투 당시 48시간만에 혼자서 800개가 넘는 메시지를 단 한 건의 실수도 없이 전달
3. 뛰어난 보안성
  - 일본군 정보국장 세이조 아리스에 중장은 일본군이 미공군 암호해독에는 성공했지만, 나바호어 암호는 전혀 손도 댈 수 없었다고 나중에 고백

# 실제 戰史에 기록된 사례

- 사이판의 한 지역을 점령한 일본군이 후퇴한 뒤, 그 지역을 재점령한 미군 대대에게 갑자기 일제사격이 퍼부어졌다. 상황을 잘못 파악한 동료 미군 부대가 퍼부은 오인 사격이었다. 상황을 설명하는 영어 메시지를 송신했지만 일제사격은 그치지 않고 계속되었다.

# 실제 戰史에 기록된 사례

- 그 메시지가 미군을 속이려는 일본군의 작전이라고 오해되었기 때문이다. 급히 나바호어 메시지를 보낸 후에야 사격이 멈추었다. 나바호어 메시지는 절대 모방할 수가 없었으므로 어떤 상황에서도 신뢰할 수 있었기 때문이다.

# 단점

1. 나바호어에 능숙한 인력이 필요
  - 그에 반해 당시 독일군의 Enigma라는 암호화 기계는 대량 생산되어 거의 모든 부대에 보급
2. 사용자가 매우 적고 외부에 잘 알려지지 않은 자연어 필요
  - 미국은 또다른 전쟁 발발시 나바호 암호를 다시 사용하기 위해 나바호 코드 토키에 관한 모든 기록을 극비로 함

# 정리

- 자연 언어를 암호로 사용한 굉장히 희귀하면서도 효과적인 암호화 방식
  - 나바호어 외에도 초토우(Choctaw), 체로키, 코만치, 웨일즈, 바스크 어들을 사용한 코드 토크들 역시 존재
- 나바호 코드 토크들이 가장 전세에 미친 영향이 컸고 그리고 가장 대규모로 이루어진 사례이므로 이번 발표에서 다룸