

CRIPTOGRAFIA MILITAR E OS *CODE TALKERS* NAVAJOS

*Faça com que seus planos sejam obscuros e impenetráveis como a noite
e quando se mover caia como um relâmpago.*

Sun Tzu

JOÃO VICTOR NUNES DE SOUSA*
Engenheiro

SUMÁRIO

Introdução
Criptografia, Códigos e Cifras
A escolha do idioma Navajo
Preparação para o combate
Entrando em ação
Legado
Conclusão

INTRODUÇÃO

A comunicação sempre foi e ainda é fundamental para que governantes dirijam seus países e generais comandem suas tropas com eficiência. Tão importante quanto manter canais de comunicação eficientes é fazer com que as mensagens que circulam pelos mesmos sejam inacessíveis ao grande público,

em especial aos inimigos dos que trocam as mensagens, afinal, num conflito, um general inimigo teria enorme vantagem sobre outro conhecendo sua situação de estoque de munições, posicionamento de tropas e planejamentos futuros, assim como um país levaria enorme vantagem sobre outro se tivesse acesso às suas comunicações diplomáticas e estratégias comerciais.

* Mestre e Graduado em Engenharia Mecânica pela Universidade Federal de Campina Grande (PB). Perito Criminal da Polícia Civil do Estado de Pernambuco.

Esse medo de que comunicações sigilosas chegassem às mãos inimigas fez com que surgissem técnicas de mascaramento das mesmas por meio de códigos e cifras, que transformavam, quase que magicamente, mensagens perfeitamente entendíveis em monstros linguísticos, sem qualquer nexos, sendo essas mensagens entendidas apenas pelo destinatário.

Ao longo dos séculos, códigos e cifras eram criados, dando uma segurança temporária às comunicações, mas eram, depois de algum período, quebrados pelos inimigos dos que se correspondiam. Esses últimos criavam então novos códigos e cifras mais difíceis de serem quebrados e entravam em um ciclo que se mantém até hoje. O importante nesse ciclo é que há um período, curto ou longo, em que o código e a cifra são efetivos, ou seja, em que o conteúdo das mensagens trocadas de fato é secreto [1].

No âmbito militar, surgiu a ideia de usar como código para comunicações sigilosas idiomas muito específicos, com poucos falantes e que fosse virtualmente fora do alcance e conhecimento do inimigo. Os indivíduos que eram empregados nessa estratégia de comunicação ficaram conhecidos como *code talkers* (em português, “falantes em código”).

O uso oficial dos *code talkers* foi iniciado, mesmo que de forma bastante limitada, na Primeira Guerra Mundial, em que americanos usaram índios nativos do seu território para codificar mensagens trocadas por rádio ou telefone, sendo a tribo Choctaw pioneira nessa ação. Porém a aplicação mais maciça e marcante dessa estratégia se daria na Segunda Guerra Mundial, no teatro de operações do Pacífico, onde americanos utilizaram índios Navajo para codificar suas mensagens [2], ajudando a mudar o rumo de cada batalha naquelas selvas

e contribuindo para a vitória americana naquele conflito.

CRIPTOGRAFIA, CÓDIGOS E CIFRAS

O termo criptografia é derivado das palavras gregas *kriptos*, que significa “oculto”, e *graphein*, que significa “escrever”, podendo então ser entendido como “escrita oculta”. De fato, a criptografia tenta ocultar o significado da mensagem, não a existência da mesma, por meio de um processo chamado encriptação. Na prática, a encriptação consiste em misturar a mensagem seguindo um protocolo específico, só conhecido pelo emissor e pelo receptor.

Um código pode ser definido como um protocolo de substituição de uma palavra ou frase ou, de forma mais geral, de uma mensagem por uma palavra, uma frase, um número ou um símbolo desprovido de correlação com o significado real da mensagem. Um exemplo de código seria a substituição das palavras “ataque” por “sol” e “recue” por “lua”. Para quem desconhece o protocolo do código, que estaria descrito em um livro-código, a mensagem não teria o menor sentido.

Alternativamente aos códigos, existem as cifras, que são mais usuais e flexíveis. Na cifra, as letras da mensagem são substituídas por outras letras ou símbolos, que juntos são desprovidos de sentido. Para execução de uma cifra, define-se um protocolo de mistura (algoritmo) e como esse protocolo será usado (chave de cifra). Para decifrar a mensagem, é necessário conhecer tanto o algoritmo quanto a chave. Um exemplo de cifra simples seria a substituição de cada letra da mensagem por uma letra algumas posições à frente da mesma no alfabeto (algoritmo), sendo, no nosso exemplo, a

quantidade de posições de avanço igual a 1 (chave): “ataque” se tornaria “BUBRVF” e “recue” se tornaria “SFDVVF”.

A eterna batalha na ciência da criptografia consiste, então, na criação constante de códigos e cifras mais fortes (mais difíceis de serem quebrados) e, em paralelo, na tentativa de terceiros em decodificar e decifrar os mesmos.

A ESCOLHA DO IDIOMA NAVAJO

Enquanto os criptoanalistas britânicos quebravam a cifra da máquina alemã Enigma e alteravam dramaticamente o curso da guerra na Europa, seus aliados norte-americanos estavam envolvidos em acontecimentos igualmente relevantes no Pacífico ao decifrarem a cifra japonesa, conhecida como Púrpura (Figura 1).

Embora as cifras alemãs e japonesas acabassem sendo quebradas depois de algum tempo, elas forneceram um relevante nível de segurança para as comunicações ao serem implementadas, sendo um de-

safio real para os criptoanalistas aliados. Na verdade, se as máquinas de cifra fossem tivessem sido usadas de forma adequada, sem chaves repetidas, sem mensagens padronizadas e sem restrições nos seus ajustes, possivelmente não seriam decifradas durante a guerra. Um exemplo de cifra que foi usada de forma correta e não foi decifrada durante a Segunda Guerra é a SIGABA, que foi usada pelos americanos até meados dos anos 50.

Entretanto, mesmo dispondo de um sistema de cifras robusto e seguro, os comandantes militares se viam com um grande problema: o uso das máquinas de cifra era extremamente lento. As mensagens militares eram majoritariamente transmitidas via rádio, que era um meio rápido de comunicação, porém tinha a desvantagem de ter seu tráfego facilmente captado pelo inimigo, demandando que fosse feito algo para “embaralhar” as mensagens (ou, em termos mais técnicos, cifrá-las/codificá-las) e torná-las inúteis para os inimigos, porém perfeitamente inteligíveis e úteis para suas tropas¹. A

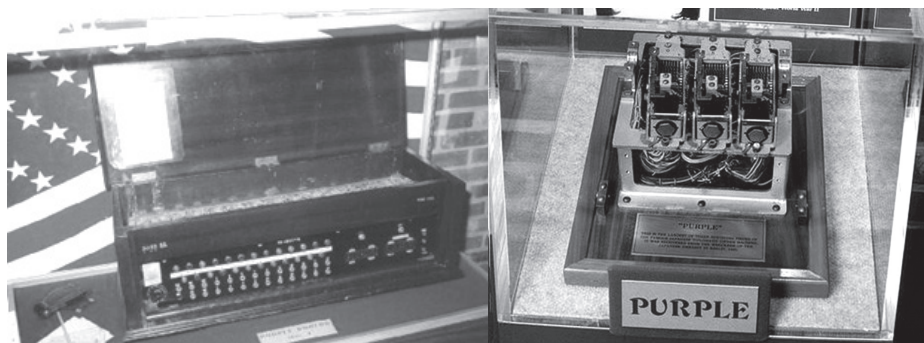


Figura 1 – Máquina de cifra japonesa Datilógrafo Alfabético '97 ou, como foi apelidada pelos norte-americanos, Púrpura, fechada (à esquerda) e com seu mecanismo interno exposto (à direita). Fonte: [3]

¹ Vale destacar que transmitir comunicações sigilosas em inglês estava totalmente fora de cogitação, visto que esse idioma era amplamente conhecido pelos japoneses, italianos e alemães, que dominavam inclusive os regionalismos e as gírias, pois muitos dos seus oficiais estudaram em universidades americanas antes da Segunda Guerra Mundial.

mensagem tinha que ser datilografada na máquina de cifragem, letra por letra. O texto cifrado, então, era anotado, letra por letra, e transmitido, letra por letra, pelo operador de rádio. Por sua vez, outro operador de rádio recebia a mensagem cifrada e a anotava cuidadosamente, letra por letra, e a passava para o especialista em cifras, que a datilografava na máquina de cifragem, letra por letra, decifrando-a. Esse processo exigia considerável tempo, além de um espaço mínimo adequado para o uso da máquina de cifras, não sendo problema para os centros de comando a bordo de navios ou quartéis, mas sendo totalmente inviável para os ambientes hostis e dinâmicos das selvas do Pacífico.

A solução para o problema estava surgindo no início de 1942, quando o engenheiro civil Philip Johnston começou a formular um sistema de códigos baseado na língua indígena Navajo. Johnston era filho de um missionário e cresceu nas reservas indígenas Navajo, no estado americano do Arizona, sendo uma das poucas pessoas fora da tribo a dominar o seu idioma. Johnston imaginou que um idioma indígena nativo americano seria um sistema de códigos ideal, em que cada unidade americana no Pacífico poderia usar um par de índios para prover comunicações seguras via rádio. Para se ter ideia, uma mensagem de três linhas que antes levava cerca de 30 minutos para ser transmitida de forma criptografada podia ser repassada em apenas 20 segundos usando os Navajos.

A língua Navajo equivalia a um código secreto e podia ser utilizada para comunicações militares rápidas e seguras

Após levar sua ideia ao Camp Elliott, base dos Fuzileiros Navais em San Diego, Califórnia, Johnston realizou uma magnífica demonstração da eficiência do método de comunicações que ele sugeria, e foi então aprovado um projeto-piloto baseado em sua ideia.

O primeiro passo do projeto-piloto era a seleção da tribo indígena nativa americana mais apta para a tarefa. Os requisitos básicos eram que a tribo pudesse fornecer grande quantidade de homens que fossem fluentes em seu idioma nativo e em inglês (falado e escrito) e que o idioma da tribo fosse totalmente desconhecido por alemães, italianos e japoneses. Em uma pré-seleção, foram escolhidas quatro tribos: Navajo,

Sioux, Chippewa e Pima-Papago.

Ao final, a grande escolhida foi a tribo Navajo, com sua língua de mesmo nome. O Navajo era a língua ideal, visto que era muito complexa, comple-

tamente incompreensível para todas as outras tribos americanas, não tinha raiz, nem similaridade estrutural com línguas europeias ou asiáticas, sendo totalmente incompreensível também para esses povos e não tinha forma escrita². Outro ponto importante era de que essa tribo não recebera visitas de estudantes de Antropologia alemães nos últimos 20 anos, como ocorrera com outras tribos, sendo sua língua, então, totalmente inacessível às potências do Eixo. De fato, a língua Navajo equivalia a um código secreto e poderia ser utilizada para comunicações militares rápidas e seguras.

² Atualmente o idioma Navajo possui uma forma escrita difundida e é falado por cerca de 170 mil pessoas.

PREPARAÇÃO PARA O COMBATE

Mesmo o nativo americano sendo um povo inferiorizado na década de 40 nos Estados Unidos da América (EUA), não foi difícil encontrar uma grande quantidade de candidatos a *code talkers* Navajos. A primeira turma de Navajos no curso de comunicações militares do Corpo de Fuzileiros Navais dos EUA foi formada quatro meses após o ataque japonês a Pearl Harbor (7 de dezembro de 1941), composta por 29 indivíduos (Figura 2).

Um dos problemas que tinham de ser resolvidos antes de se adotar o uso do idioma Navajo como código para comunicações residia no fato de não existir em Navajo palavras ou expressões equivalentes aos modernos termos militares. Os militares americanos, com ajuda dos índios, montaram então um dicionário que relacionava termos Navajos com palavras/expressões inglesas de referências militares. Assim, *Da-he-tih-hi* (pronúncia de “beija-flor”

em Navajo) se tornaria “avião de caça”; *lo-tso* (pronúncia de “baleia” em Navajo), “encouraçado”; e assim por diante. Esse dicionário continha inicialmente 274 palavras e fora ampliado para 508 palavras no transcorrer da guerra.

Mesmo com o dicionário, havia ainda a necessidade de se traduzirem nomes menos usuais e previsíveis, tais como nomes de lugares e pessoas. Para isso, foi criado um alfabeto fonético para soletração (Figura 3). Por exemplo, “Guam” seria soletrado em inglês como *goat* (cabra), *ute* (tribo), *ant* (formiga), *mouse* (rato), sendo codificado em Navajo como *klizzie, no-da-ih, wol-la-chee, na-as-tso-si*.

Visando dificultar uma eventual quebra do código Navajo pelos japoneses, os americanos fortaleceram o alfabeto fonético de soletração criando homófonos. Por exemplo, a palavra “Saipan” seria soletrada com repetição do termo Navajo equivalente ao “a”, que seria *wol-la-chee*, o que permitiria aos japoneses deduzir que aquele som repetido poderia corresponder ao som de uma letra repetida. Com uma



Figura 2 – Primeira turma de *code talkers* Navajos. Na foto há três instrutores não-indígenas. Fonte: [4]

análise de frequências³ bem feita, seria possível, em algum tempo, deduzir todo o alfabeto fonético codificado. Assim, os americanos introduziram homófonos para letras mais comuns; por exemplo, “a”

poderia ser soletrado também como *apple* (maçã) ou *axe* (machado), ou, em Navajo, *be-la-sana* e *tse-nihl*, respectivamente. Isso dificultava, ou mesmo inviabilizava, a análise de frequências.

CONFIDENTIAL ALPHABET					
A- (Wol-la-chee)	Ant	N- (Nesh-chee)	Nut		
B- (Shush)	Bear	O- (Ne-ahs-jah)	Owl		
C- (Moesi)	Cat	P- (Bi-so-dih)	Pig		
D- (Se)	Deer	Q- (Ca-yailth)	Quiver		
E- (Dseh)	Elk	R- (Gah)	Rabbit		
F- (Ma-e)	Fox	S- (Dibsh)	Sheep		
G- (Klizzio)	Goat	T- (Than-zie)	Turkey		
H- (Lin)	Horse	U- (No-da-in)	Ute		
I- (Tkin)	Ice	V- (A-keh-di-glini)	Victor		
J- (Tkele-cho-gi)	Jackass	W- (Gloe-ih)	Weasel		
K- (Klizzio-yazzie)	Kid	X- (Al-an-as-dzoh)	Cross		
L- (Dibsh-yazzie)	Lamb	Y- (Tesh-as-zih)	Yucca		
M- (Na-as-teo-si)	Mouse	Z- (Besh-do-gliz)	Zino		

Names of various organizations					
Corps	Din-neh-ih	Clan			
Division	Ashi-hi	Salt			
Regiment	Tabaha	Edge Water			
Battalion	Techuene	Red Soil			
Company	Nakia	Mexican			
Platoon	Ket-olish-nih	Mud			
Section	Yo-ih	Bees			
Squad	Debeh-li-zini	Black Sheep			
COMMUNICATION					
Telephone	Besh-hal-ne-ih	Telephone			
Switchboard	Ya-ih-e-tih-ih	Central			
Wire	Besh-ah-ah-ih	Copper			
Telegraph	Besh-ah-ah-ih-beh-hane-ih	Comm. by copper wire			
Semaphore	Dah-na-a-tah-ih-beh-hane-ih	Flag Signals			
Blinker	Coh-nil-kol-ih	Fire Blinder			
Radio	Nil-chi-hal-ne-ih	Radio			
Panel	As-kad-be-ha-ne-ih	Carpet Signals			
OFFICERS- A-la-jih-na-zini (Headmen)					
Major General	So-na-kih	Two Stars			
Brigadier General	So-s-la-ih	One Star			
Colonel	Atah-besh-le-gai	Silver Eagle			
Lieutenant Colonel	Che-chil-be-tah-besh-legal	Silver Oak Leaf			
Major	Che-chil-be-tah-ola	Gold Oak Leaf			
Captain	Besh-legal-na-kih	Two Silver bars			
1st Lieutenant	Besh-legal-a-lah-ih	One Silver bar			
2nd Lieutenant	Ola-alah-ih-ni-ahi	One Gold bar			
Airplanes-No-tah-de-ne-ih (Air Force)					
Dive Bomber	Gini	Chicken Hawk			
Torpedo Plane	Tas-chizzie	Swallow			
Observation Plane	Ne-as-jah	Owl			
Fighter Plane	Da-ne-tih-hi	Humming Bird			
Bomber	Jay-sho	Buzzard			
Patrol Plane	Ga-gin	Crow			
Transport	Atash	Eagle			

Figura 3 – Página da apostila de treinamento em comunicações militares usada pelos Navajos. Fonte: [5]

3 Análise de frequências é uma técnica utilizada por criptoanalistas que pode ser definida, de forma simplificada, na correlação dos percentuais de aparições das letras do texto criptografado com os percentuais médios de aparições das letras em textos de um determinado idioma. Por exemplo, se sabemos (ou supomos) que o texto criptografado está em inglês e verificamos que o termo “wol-la-chee” consiste em 8% das aparições em uma mensagem longa ou em um conjunto de mensagens curtas, podemos supor com razoável certeza que ele se refere à letra “a”, que consiste em 8% das aparições em textos em inglês. A análise de frequências foi criada no século IX pelo cientista e filósofo árabe Abu Yusef Ya’qub ibn Is-haq as-Sabbah ibn omran ibn Ismail al-Kindi.

Após oito semanas de curso, formou-se a primeira turma de militares Navajos, que memorizaram todo o dicionário e o alfabeto fonético para soletração, dispensando a necessidade de uso de livros-código no campo de batalha. Os Navajos tinham excelente memória, visto que seu povo não tinha linguagem escrita, fazendo com que essa qualidade fosse uma característica comum entre eles. Enfim, os Navajos estavam prontos para o combate.



Figura 4 – Fuzileiros americanos descansando na selva de Guadalcanal. Fonte: [6]

ENTRANDO EM AÇÃO

Os Navajos fizeram seu batismo de fogo junto à Primeira Divisão de Fuzileiros, em 7 de dezembro de 1942, na invasão americana de Guadalcanal, uma das Ilhas Salomão, na época colônia britânica (Figura 4). Rapidamente, campanha após campanha, os Navajos mostravam eficiência no desempenho de suas funções (Figura 5). Mensagens



Figura 5 – Militares Navajos operando rádio na Ilha de Bougainville, hoje território de Papua-Nova Guiné. Fonte: [4]

eram transmitidas com velocidade e clareza, além de serem consideradas imunes a falsificações. Os japoneses não conseguiam sequer transcrever os sons produzidos pelos Navajos, quanto mais reproduzi-los. Toda a comunicação que circulava em Navajo era entendida automaticamente pelos americanos como autêntica.

Há que se destacar a postura dos militares Navajos diante da batalha. Eram

conhecidos por serem extremamente calmos, mesmo sobre condições críticas, como em um ataque inimigo⁴, errando pouquíssimo em suas transmissões. Além disso, em prol do cumprimento do dever como militares, os índios passavam por cima de suas próprias crenças. Os Navajos acreditavam que os espíritos dos mortos habitavam o local de sua morte até que uma cerimônia fosse realizada no corpo.

⁴ Vale ressaltar que operadores de rádio, como os *code talkers* Navajos, oficiais e socorristas eram alvos preferenciais nos ataques japoneses. Esses militares corriam um risco de morte maior que o restante da tropa.

Enquanto isso não acontecia, o local onde esse corpo se encontrava era tido como impuro. Obviamente, as condições de combate nas selvas das ilhas do Pacífico não permitiam enterros de imediato, e muitas vezes os índios tinham que passar longos períodos ao lado de cadáveres, executando suas funções, mesmo diante do desrespeito a uma tradição tribal. Os Navajos colocaram seu dever para com a pátria acima de suas tradições seculares.

LEGADO

Ao final da Segunda Guerra Mundial, foram empregados 420 *code talkers* Navajos. Seu emprego como codificadores militares foi definido como informação classificada pelo Alto-Comando americano. O público só foi ter conhecimento sobre sua contribuição para a vitória na guerra em 1968 quando o código Navajo foi desclassificado. Em 1982, o governo americano batizou o dia 14 de agosto como o Dia Nacional dos Codificadores Navajos.

Anos depois de findada a guerra, os japoneses admitiram que conseguiram de-

cifrar alguns códigos usados pelos americanos, mas não avançaram nada na quebra do código Navajo. Sem dúvida, podemos dizer que a cultura, sob a forma de sua língua, daquelas tribos isoladas nos rincões dos Estados Unidos, muitas vezes marginalizadas e inferiorizadas, foi fundamental para a vitória em muitas batalhas no Pacífico. O povo americano tem uma dívida eterna com o povo Navajo (Figura 6).

CONCLUSÃO

Conforme exposto, o uso do idioma Navajo para codificação de mensagens militares na Segunda Guerra Mundial foi fundamental para a vitória americana no Pacífico, impondo aos japoneses a surpresa.

De fato, uma guerra se torna dramaticamente mais fácil de ser vencida se você tem pleno acesso às comunicações do seu adversário, conhecendo seus planos e acompanhando em tempo real sua situação, enquanto mantém as suas próprias comunicações blindadas contra os ouvidos do seu inimigo.



Figura 6 – Monumento em homenagem aos *code talkers* Navajos em Window Rock, Arizona, EUA. Fonte: [4]

📁 CLASSIFICAÇÃO PARA ÍNDICE REMISSIVO:
<INFORMAÇÃO>; Código; Criptografia;

REFERÊNCIAS

- [1] SINGH, S. *O Livro dos Códigos*. 12ª edição. Rio de Janeiro: Editora Record, 2020.
- [2] *Navajo Code*. Disponível em: <https://navajocodetalkers.org>. Acesso em: 9 de fev. 2021.
- [3] *Cipher Machines*. Disponível em: <https://ciphermachines.com/purple>. Acesso em: 18 de fev. 2021.
- [4] *AZ Central*. Disponível em: <https://www.azcentral.com/story/news/local/arizona/2018/07/11/navajo-code-talker-facts-unbreakable-code/460262002/>. Acesso em: 8 de fev. 2021.
- [5] *Northern Arizona University Digital Library*. Disponível em: <http://archive.library.nau.edu/digital/collection/cpa/id/44806>. Acesso em: 22 de fev. 2021.
- [6] *Guadalcanal Campaign*. Disponível em: https://en.wikipedia.org/wiki/Guadalcanal_campaign. Acesso em: 18 de fev. 2021.