

## 1.2 Lesson 1 : Codes and ciphers

Cryptography is the practice and study of techniques for **securing communications** from unauthorized access. Codes and ciphers are two ways of changing the message systematically to confuse anyone who intercepts it.

### 1.2.1 Examples of codes

A code is a way of changing the message by replacing each word with another word that has a different meaning. For example, “Burn the City” could become “Take the rubbish” where the word “burn” is represented by the codeword “take”, and similarly for “city” and “rubbish”. Using codes requires a codebook which acts like a dictionary for all codewords.

**Exercise 1** — 🗣️ **The code talkers.** Let us watch an excerpt from National Geographic’s documentary “Untold Stories of the Second World War”. <https://youtu.be/LN2oKqa1o04>

1. Watch part 1 (until 4’14”) and pay attention to:

- What war is it about ?.....
- In what part of the world ?.....
- What tribe is it about ?.....

2. Fill in the gaps in the following text while watching Part 2 (from 4’14” until 9’33”).

Japan’s attack on \_\_\_\_\_ crippled the pacific fleet. As American forces fought back, they discovered that the enemy could \_\_\_\_\_ and read battlefield messages almost at will. A new, \_\_\_\_\_ . Convinced that \_\_\_\_\_ signalmen would baffle Japan’s best \_\_\_\_\_, The Marine Corp turned to the Reservation for \_\_\_\_\_.

“When you become a Marine you have to. The sergeant tells you to jump in the lake, you jump in the lake”. “You can’t say simplified; all we speak.”

Keith Little and Sam So have met to share memories and Navajo frybread. Many traditions still \_\_\_\_\_, but the Navajo tongue, like \_\_\_\_\_, is \_\_\_\_\_ generations.

“When you first joined the Marines, did you guys know you’d become \_\_\_\_\_?”

“Well, for me I didn’t have any idea that I would be joining the Marines at all. All I know is I get \_\_\_\_\_”

“My birthday was on March 4th, and when the March 4th came, I became a 17 years old and “absolutely marine corps recruiting stationed”.

On the reservation, Navajo men, young and old, were lining up to fight for America \_\_\_\_\_.

“All I know was that his is our land. When I heard it was being bombed, being attacked by some enemy, then that doesn’t set too well with me.”

In all, nearly \_\_\_\_\_ Navajo left the world of the Reservation to join a world at war. Some \_\_\_\_\_ would serve as \_\_\_\_\_ with the US Marines. From Guadalcanal to Okinawa, the Navajo signalmen strung phone lines; they hauled field radios and fought on the front lines. Yet of all their duties, none was more crucial than \_\_\_\_\_. Subtle tones and \_\_\_\_\_ make Navajo \_\_\_\_\_.

On the battlefield it made an unbreakable code. The marines’ warrior language started with \_\_\_\_\_. Common Navajo words stood for individual letters, and the code talkers simply \_\_\_\_\_

“We sent it as a code and then it would be received on the other end as a regular message. I guess Sam, if I talk to him from here and my commanding officer gives me a message “a plane” in this message and I said it in Navajo, in Navajo code, and Sam would write it down on the other end as “plane” English as I got it from for my commanding officer”.

“If it is Navajo, the other guy was saying “message for Arizona”, that means that they want a \_\_\_\_\_ to receive the message”.

To confuse \_\_\_\_\_, they played \_\_\_\_\_ and used \_\_\_\_\_

“What we called rockets (LESZ-YIL-BESHI), ground boiler, when they hit the ground it like ground is boiling. This is a rock flying all around. Hand grenade: (NI-MA-SI) potatoe, (DA-HE-TIH-TI) means Hummingbird in English. We used to call the fighter plane. ”

Hummingbird and Iron fish, ground boiler and potatoes. On an island called Iwo Jima, Navajo would be \_\_\_\_\_.

3. Answer the following questions. If necessary, clues can be found in the text.

- a) What were the two forces in the Pacific War?.....
- b) What event made the US enter the Pacific War? .....

- c) When did it happen?.....
- d) What was the name of the new US weapon? .....
- e) What was the strength of this code, and why was it so difficult to be broken?.....

4. Unscramble the following words: “bi-sodih, wol-la-chee, moasi,tkin, ma-e, tkin, moasi”...

5. Cipher the sentence “Bombs will fall on Guadalcanal”

The Navajo alphabet code								
A	Ant	Wol-la-chee	J	Jackass	Tkele-cho-gi	S	Sheep	Dibeh
B	Bear	Shush	K	Kid	Klizzie-yazzi	T	Turkey	Than-zie
C	Cat	Moasi	L	Lamb	Dibeh-yazzi	U	Ute	No-da-ih
D	Deer	Be	M	Mouse	Na-as-tso-si	V	Victor	A-keh-di-glini
E	Elk	Dzeh	N	Nut	Nesh-chee	W	Weasel	Gloe-ih
F	Fox	Ma-e	O	Owl	Ne-ahs-jsh	X	Cross	Al-al-as-dzoh
G	Goat	Klizzie	P	Pig	Bi-sodih	Y	Yucca	Tsah-as-zih
H	Horse	Lin	Q	Quiver	Ca-yeilth	Z	Zinc	Besh-do-glitz
I	Ice	Tkin	R	Rabbit	Gah			

Navajo codewords for planes and ships					
Fighter plane	Hummingbird	Da-he-tih-ti	Observation plane	Owl	Ne-as-jah
Torpedo plane	Swallow	Tas-chizzie	Bomber	Buzzard	Jay-sho
Dive-bomber	Chickenhawk	Gini	Bombs	Eggs	A-ye-shi
Amphibious vehicle	Frog	Chal	Battleship	Whale	Lo-tso
Destroyer	Shark	Ca-lo	Submarine	Ironfish	Besh-lo

**Table 1.1:** Elements of the Navajo code book. Codebooks can become quite large, making the use of codes rather cumbersome. However, sometimes it is enough to encode key words in a message.

**Exercise 2** — 🕒 **Marlo’s clocks.** Simple codes can be very effective, since even if the message is intercepted, the code reads as an innocent or unrelated topic. In the crime tv show “The Wire”, ruthless gang leader Marlo Stanfield is trying to keep the police from having probable cause when investigating. Watch the video clip and answer the following questions :

1. What do Marlo and his crew send each other when hiding a message ? .....
2. What does each of the second hand, the hour hand and the minute hand indicate? .....

- .....
- .....
3. How do members of the crew know the time of the meeting ? .....
- .....
4. What can members of the crew say to the police if the message is intercepted ? .....
- .....

### 1.2.2 Examples of ciphers

Unlike codes, ciphers convert the message by a rule, known only to the sender and recipient, which changes each individual letter (or groups of letters). A message encrypted using a cipher is going to look like a random string of letters or symbols. Ciphers are easier to use than codes, since the users only have to remember a specific algorithm to encrypt the message, and not a whole dictionary of codewords.

**Exercise 3** Ciphers that use a method of jumbling the order that the letters of the plaintext are written are called **Transposition Ciphers**.

1. What does *transposition* mean? .....
2. What does this message say : "KCATTA" ? How has it been enciphered? .....
- .....
- What is bad about this method of enciphering? .....
- .....

3. A *Scytale* (rhymes with *Italy*) was an ancient tool used by the Spartans to send secret messages during military campaigns. The sender of the message would wrap a long thin piece of leather around his Scytale, and write the message in rows. When the leather was removed from the Scytale, it had a long



list of letters running down it, in no particular order. The receiver would reveal the original message by wrapping the leather around his Scytale (of the same length and diameter).

Encipher the message "attack tomorrow" with a Scytale wrapped 5 times, with 4 letters per turn : .....

.....

How secure is the Scytale? .....



