Game: number stations

An intriguing activity to learn about the encoding and decoding of secret messages, and to get introduced to the mysterious world of radio espionage.

Learning targets: Get familiar with the techniques of ciphering and deciphering of messages - get familiar with Morse code or NATO/ICAO alphabet.

Material:

- PMR/CB or mobile phone with internet connection, one for each group/patrol
- Paper and pen.

Time and preferred place: 1-2 h. Open countryside.

Description: Patrols receive a ham radio frequency or CB/PMR channel to listen to, together with a deciphering key (one for each patrol). At a certain hour, the patrols must listen to a message, transmitted in Morse code or in NATO/ICAO alphabet. Using their own key, the patrols can decipher the message and they must execute the orders contained in it (go to a specific place, attack another patrol to steal them a specific object, etc.). Multiple orders can be transmitted. The last of them is to listen to a specific frequency at a given hour. In this way, the patrol will listen to a real number station, used in real espionage activities.

A list with stations and times to listen to number stations is available here:
https://priyom.org/number-stations/station-schedule

Number stations are radio stations that transmit, at given frequencies and hours, encrypted Morse or voice messages. Everyone can listen to them, but only few people can understand their messages: spies! This method of communication, particularly active during the Cold War, is really effective because it’s totally impossible to find traces of the person able to decode the message. The only way to understand a message is to catch the spy with his/her deciphering keys.

Several information on the topic can be found over the Internet. Here are some examples of number stations:
https://youtu.be/GUQUD3IMbb4
https://youtu.be/0Xfc4LjKi1w
https://youtu.be/QnXPqUU6fI0
https://youtu.be/tFm7Q9-17w0

How to cypher/decipher a message

The easy way

Each letter is numbered according to the alphabet:

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

The numbering may be optionally extended to include numbers, a word separator, punctuation, etc. In this way, any message can be converted in a sequence of numbers. For example, DOG is 3 - 14 - 6.

Now, let's say that the key is a letter, for example P (that equals to 15). To encrypt DOG, 15 is added to the number of each letter, and the final numbers are converted back to letters. If the above table is used and the sum exceeds 25, 26 must also be subtracted.
D(3) + P(15) = S(18)
O(14)+P(15) =29 → 29-26=D(3)
G(6)+P(15) =V(21)
So DOG becomes SDV. To decrypt the message, the inverse operations must be performed:
S(18)-P(15) =D(3)
D(3)-P(15) =-12 → -12+26= O(14)
V(21)-P(15) =G(6)

An easy way to perform these actions without arithmetics is using the Alberti disk (https://en.wikipedia.org/wiki/Alberti_cipher). Two disks, pinned on a common center, have the alphabet letters indicated on their circumference. By rotating one disk over the other, it's quite easy to find the correspondence of original and encrypted letters.

The less easy way

The encryption method described above can be easily broken: all the same letters give the same final letters, so that knowing the language (the most recurring letters, words with 1-2 letters, etc.) it is possible to guess the letters as in an encrypted crossword. In any case, not more than 25 attempts are necessary to find the correct key.

To make the encryption practically unbreakable, the key must be composed of at least as many letters as the message. The letters of the key are chosen randomly. The first letter of the message is encrypted with the first letter of the key using the method described above, and so for all the following letters. If the key is random, a 100 letters message may become any, literally any message of 100 letters, using an ad hoc key. This is called the Vernon cyphrary. Each message has a separate key (the equivalent of an OTP, one time password), which is given in advance to the spy, so that no relation can be established between messages.