Introduzione – Lezione - Raccontarsi dei segreti

I computer per comunicare tra di loro si scambiano dei messaggi attraverso dei mezzi di trasporto in comune. Siccome ai mezzi di comunicazione possono accedere tutti i computer, o non potrebbero inviare e ricevere messaggi, potrebbe accadere che i computer più curiosi si mettano a leggere i messaggi di altri senza il consenso del mittente e del destinatario. Come possiamo evitare che solo chi spedisce il messaggio e lo riceve possano leggere il messaggio? Cercare di usare delle strade segrete o poco trafficate non è una buona strategia in quanto potrebbe accadere che si venga a conoscenza della strada che viene utilizzata e si ritorni al punto di partenza. Possiamo invece provare a rendere illeggibile il contenuto del messaggio così che se anche qualche computer riesce ad impossessarsi del messaggio, non possa capirne il significato. Questa operazione si fa attraverso la crittografia.

Domande di ragionamento:

Provate a chiedere agli studenti come potrebbero scrivere del testo in modo da renderne illeggibile il contenuto.

Sostituzione monoalfabetica

La sostituzione monoalfabetica consiste nel sostituire una lettera con un'altra lettera. Questa sostituzione sarà sempre uguale per tutto il testo, ad esempio possiamo decidere che al posto della lettera A scriveremo sempre la lettera X, al posto di B scriveremo F e così via per tutte le lettere dell'alfabeto facendo attenzione a non ripetere le lettere.

Il cifrario di Cesare

Il cifrario di Cesare fa parte dei *cifrari a sostituzione monoalfabetica*.
Un modo molto semplice per nascondere il testo è quello di utilizzare un algoritmo crittografico molto antico, risalente all'epoca dell'antica Roma, il Cifrario di Cesare che prende il nome da Giulio Cesare.
Il suo funzionamento si basa nel sostituire una lettera con un'altra lettera per mezzo di uno spostamento di un numero di posizioni fisse all'interno dell'alfabeto. Storicamente Cesare faceva effettuare uno spostamento di 3 posizioni. Gli spostamenti vanno intesi sempre come spostamenti in avanti.
Per cercare di capire meglio prendiamo l'alfabeto inglese e proviamo ad effettuare la sostituzione monoalfabetica effettuando uno spostamento di 2 elementi, avremo:

Alfabeto Inglese	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto con spostamento di 2 elementi	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b

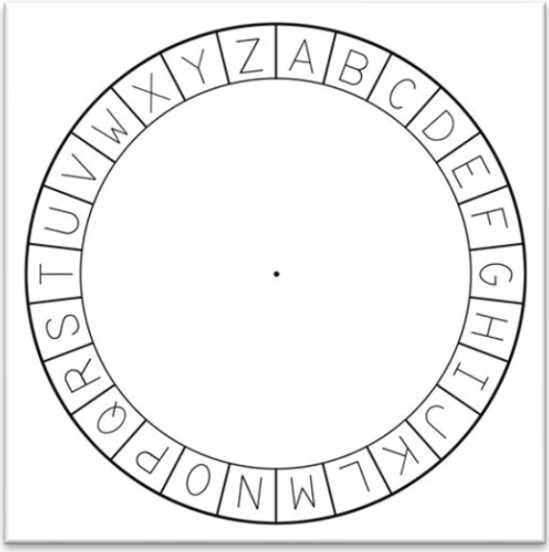
Per Cifrare non ci resta che scrivere in chiaro la parola o frase che vogliamo nascondere e andare a sostituire ciascuna lettera con la lettera corrispondente dell'alfabeto permutato, ad esempio:

Testo da cifrare: "Buongiorno"
Testo cifrato: "Dzqpimqtpq"

Per Decifrare basta fare il procedimento inverso e andare a sostituire le lettere del testo cifrato con le lettere corrispondenti dell'alfabeto originale.

Domanda per gli studenti: *L'alfabeto inglese è composto da 25 lettere. Cosa succede secondo voi se proviamo cifrare una parola effettuando uno spostamento di 25 elementi?*

Se proviamo ad effettuare lo spostamento di 25 posizioni ci ritroveremo con l'alfabeto di partenza. Va da sé quindi che con questo algoritmo possiamo avere solo 24 tipi di alfabeti diversi, se proveremo con uno spostamento di 26 elementi otterremo lo stesso alfabeto ottenuto con uno spostamento di 1 posizione. Si può provare ad immaginare questa operazione come un orologio dove al posto dei numeri che indicano le ore abbiamo le lettere dell'alfabeto [6]. Posizioniamo la lancetta delle ore e dei minuti sulla lettera che vogliamo cifrare e spostiamo la lancetta dei minuti avanti in senso orario di tante posizioni quante sono quelle scelte per lo spostamento, ottenendo così la lettera cifrata.



Domanda per gli studenti: *Come si potrebbe provare a decifrare il testo senza conoscere il numero della permutazione o la tabella?*

Essendoci solo 24 alfabeti possibili è molto facile scoprire il numero della permutazione, basta procedere per tentativi fino a che non si trova una parola o frase di senso compiuto, molto probabilmente quel numero usato per gli spostamenti sarà la chiave per decifrare il testo.

Cifrario a trasposizione

Un altro possibile metodo di cifratura è quello che basa il suo funzionamento su quello che è chiamato cifrario a trasposizione. Questo tipo di cifrario consiste nello scambiare di posizione i caratteri che compongono il testo, spazio e numeri compresi, secondo un determinato schema. Il testo cifrato sarà quindi costituito da quella che viene chiamata una *permutazione del testo in chiaro.*

Vediamo un esempio:

Testo in chiaro:	N e v e	P i o g g i a
Testo cifrato:	e N e v	g i g P o a i

Domanda per gli studenti: *Cosa rende più difficile intuire il contenuto del messaggio cifrato?*

Più è lungo il testo da cifrare e maggiore sarà la sicurezza del testo cifrato!

Attività – Cifrario di Cesare:

Questa attività verrà scritta in due versioni e utilizzerà il cifrario di Cesare, una adatta a dei ragazzi più grandi e l'altra, assistita, adatta a bambini o ragazzi piccoli. La versione assistita può essere usata anche come introduzione o esempio nel caso i ragazzi fossero in difficoltà con la versione standard. I passi sono numerati in modo che si possa notare quali passaggi hanno in comune le due versioni affinché sia possibile passare da un momento all'altro alla versione assistita in caso di difficoltà elevata per i ragazzi.

[6] Immagine reperita da: https://projects.raspberrypi.org/it-IT/projects/secret-messages/1 e distribuita secondo licenza: https://creativecommons.org/licenses/by-sa/4.0/

VERSIONE STANDARD

1 - Distribuire a ogni studente una tavoletta magnetica e delle lettere affinché sia possibile scrivere delle parole di uso comune.

2a - L'insegnante dovrà scegliere e comunicare a voce, o scrivendolo su una lavagna, una parola semplice da far cifrare ai ragazzi, che riporteranno sulla parte superiore della tavoletta. Dovrà anche decidere un numero da 1 a 25

3a -Chiedete agli studenti di scrivere nella parte bassa della tavola magnetica una parola semplice come ad esempio il nome di un frutto o di un animale. Lo studente dovrà poi cifrare il messaggio.

Nota: se vedete gli studenti in difficoltà suggeritegli come primo passo quello di scriversi su un foglio una tabella in cui si abbia l'alfabeto inglese e l'alfabeto risultante dallo spostamento.

VERSIONE ASSISTITA

1 - Distribuire a ogni studente una tavoletta magnetica e delle lettere affinché sia possibile scrivere delle parole di uso comune.

2b – l'insegnante dovrà comunicare a voce il numero 7 e scrivere sulla lavagna una tabella composta da due righe e 26 colonne e dovrà scrivere nella prima riga l'alfabeto inglese.

3b – far vedere ai ragazzi come vengono ottenute le lettere permutate delle lettere 'A', 'L' e 'V', indicare con la mano 7 spostamenti come indicato qui sotto:

	1	2	3	4	5	6	7
A	-> B	-> C	-> D	-> E	-> F	-> G	-> ***H***
L	-> M	-> N	-> O	-> P	-> Q	-> R	-> ***S***
V	-> W	-> X	-> Y	-> Z	-> A	-> B	-> ***C***

Successivamente lavorare insieme ai ragazzi per completare la tabella.

Il risultato dovrà essere così:

Alfabeto Inglese	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto con spostamento di 7 elementi	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g

4b – far scrivere sulla parte superiore della tavoletta la parola "BUONGIORNO", chiedete ora ai ragazzi di provare a cifrare questa parola lasciandogli utilizzare la tabella. Il risultato dovrà essere "IBVUNPVYUV"

5b – Chiedere agli studenti di decifrare la frase "MYHAYLNPVYUPHAALJJOLYLTVPNHSSP" sapendo che è stato effettuato uno spostamento di 7 lettere.

Se vedete i ragazzi in difficoltà ricordategli che per decifrare bisogna effettuare lo stesso procedimento fatto per la cifratura ma leggendo la tabella dal basso verso l'alto. Dalla decrittazione otterremo: "FRATREGIORNIATTECCHEREMOIGALLI". Dopo aver fatto decifrare la frase è sufficiente leggerla per capire dove vanno inseriti gli spazi.