VISIT MATH

Cofinanziato dall'Unione europea

Programmazione

Argomento	Algoritmi
Obiettivi di apprendimento	Conoscere i diversi modi di codificare e imparare a decodificare
Fascia d'età	12-16 anni (da adattare in ogni paese)
Durata stimata	45 min
Attività	Crittografare e decrittografare
Visite correlate	Parigi

Conoscenze pregresse richieste

Non sono richiesti particolari prerequisiti.

Passo dopo passo: la sequenza in aula

Passaggio 1: presentazione dell'argomento

Breve presentazione degli elementi del patrimonio in questa sequenza

La crittografia è una scienza a metà strada tra matematica e informatica, ma con applicazioni molto pratiche. Il suo scopo è proteggere le informazioni, di solito facendole sembrare incomprensibili, mescolandole e trasformandole secondo un metodo particolare.

Esiste anche una tecnica crittografica chiamata steganografia, che viene utilizzata per nascondere un messaggio in testo o immagini apparentemente innocui. Questi messaggi possono essere inviati nel pubblico dominio senza preoccuparsi di essere intercettati o scoperti, anche accidentalmente.

Un po' di storia

- Dall'800 a.C. al 200 a.C.: gli Spartani usavano le scitale
- Circa 600 a.C.: Nabucodonosor usava teschi rasati
- Intorno al 480 a.C.: Demarato (un greco), isolato in Persia, usa tavolette di cera per avvertire il suo paese dei piani di Serse (Persia)
- 100 a.C. / 44 a.C.: Cifrario di Cesare (spostamento alfabetico)
- I secolo: comparsa di inchiostro invisibile (fluidi organici ricchi di carbonio)
- 1580: Cifra mediante sostituzione di simboli (nomenclatura del codice) - Mary Stuart
- 1586: Trattato sui cifrari: cifrario di Vigenère
- 1930: macchina enigma
- Fine del XX secolo: comparsa della crittografia a chiave pubblica – RSA

Definizione di codifica:

Criptologia: la scienza della crittografia e della crittoanalisi.

Crittografia: scienza della creazione di crittogrammi.

Crittoanalisi: scienza dell'analisi dei crittogrammi al fine di decifrarli.

Crittogramma: messaggio crittografato.

Crittografa / Cifra / Cripta: trasforma un testo o un'informazione sostituendo le lettere (o le parole da codificare) in uno script composto da segni predefiniti.

Decifra / Decodifica: trasforma un messaggio crittografato in un messaggio chiaro conforme all'originale.

Decifra: trova il cifrario utilizzato nel crittogramma.

Testo in chiaro: messaggio originale prima della crittografia.

Testo cifrato: testo ottenuto dopo la crittografia.

Chiave: Elemento (parola o numero) che trasforma l'applicazione del metodo di cifratura e/o decifratura.

Classificazione dei codici

Cifrario di sostituzione: sistema crittografico in cui ogni lettera del messaggio è sostituita da un altro carattere, ma mantiene il suo posto nel messaggio.

Cifrario di trasposizione: sistema crittografico in cui ogni lettera del messaggio rimane invariata, ma viene spostata in un altro punto del messaggio.

Monosostituzione alfabetica: Cifrario di sostituzione in cui l'alfabeto crittografato rimane lo stesso per tutta la crittografia. Sostituzione con lettere, simboli, cifre o numeri, ecc.

Sostituzione poli-alfabetica: Cifrario di sostituzione in cui l'alfabeto cifrato cambia durante la crittografia. Questa modifica viene eseguita secondo una chiave.

Codice nomenclatura: questo tipo di cifrario combina una semplice sostituzione (ogni lettera è sostituita da un simbolo) e un codice di repertorio (alcune parole sono anche sostituite da un simbolo, così come simboli dirompenti).

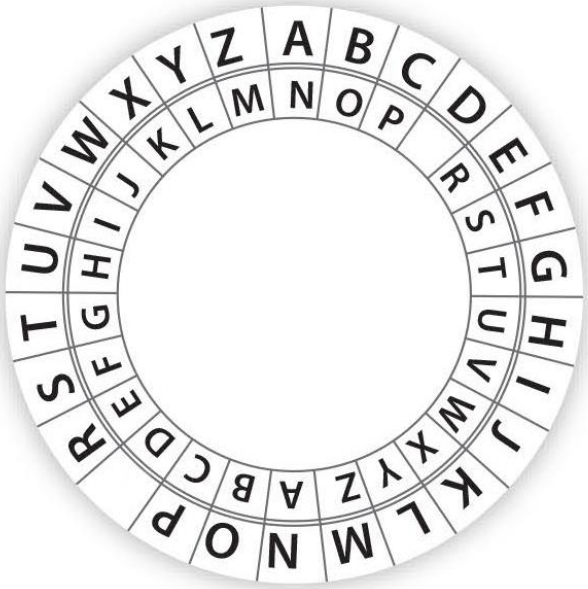
Fase 2: Attività in classe

Esempio dei sistemi di codifica più noti

1. Cifrario di Cesare o codice di Cesare

Per importanti comunicazioni al suo esercito, Cesare criptò i suoi messaggi. Ciò che è noto come cifrario di Cesare (sostituzione mono-alfabetica) è uno spostamento delle lettere di rango 4: per crittografare un messaggio, **A diventa D**, **B diventa E**, **C diventa F**, ecc.

Per tenere conto di tutte le lettere dell'alfabeto, è più saggio rappresentare l'alfabeto su una ruota.



Crediti: Fermat Science

Per decifrare il messaggio

DOHD LDFWD HVW

tutto quello che devi fare è spostare le lettere nella direzione opposta: D è decodificato come A, E come B, ecc.

Il messaggio decodificato è quindi:

ALEA IACTA EST

Decritta i seguenti 3 messaggi:

WKH URPDQV

YLFWRUB

HPSHURU

2. Il cifrario di Vigenère

Il cifrario di Vigenère è un algoritmo di sostituzione polialfabetica.

Invece di corrispondere circolarmente le lettere, ogni lettera è ora associata a un'altra lettera (in nessun ordine fisso o come regola generale).

Ad esempio:

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
F	Q	B	M	X	I	T	E	P	A	L	W	H	S	D	O	Z	K	V	G	R	C	N	Y	J	U

Per crittografare il messaggio

TO BE OR NOT TO BE THAT IS THE QUESTION

guarda la corrispondenza e sostituisci la lettera E con la lettera X, poi la lettera T con la lettera G, poi la lettera R con la lettera K...

Il messaggio crittografato è quindi:

GD QX DK SDG GD QX GEFG PV GEX ZRXVPDS

Per decifrarlo, conoscendo le sostituzioni, facciamo l'operazione inversa.

Decritta i seguenti 3 messaggi:

HFGE PV IFSGF VGPB

OWFJ NPGE SRHQX KV

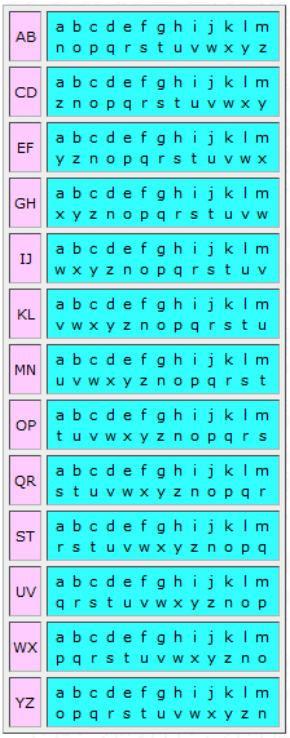
FSDGEXK PMXF IKDH HFGEV

3. Il sistema di cifratura Porta

Porta è stato un fisico e inventore italiano del primo sistema letterale a doppia chiave, ovvero il primo cifrario per il quale l'alfabeto cambia ad ogni lettera.

Questo sistema polialfabetico era estremamente robusto per l'epoca, tanto che molti considerano Porta il “padre della moderna crittografia”. Giovanni Della Porta inventò il suo sistema di cifratura nel 1563, e fu utilizzato con successo per tre secoli.

Ecco un esempio della tabella di crittografia Porta:



AB	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
CD	a b c d e f g h i j k l m z n o p q r s t u v w x y
EF	a b c d e f g h i j k l m y z n o p q r s t u v w x
GH	a b c d e f g h i j k l m x y z n o p q r s t u v w
IJ	a b c d e f g h i j k l m w x y z n o p q r s t u v
KL	a b c d e f g h i j k l m v w x y z n o p q r s t u
MN	a b c d e f g h i j k l m u v w x y z n o p q r s t
OP	a b c d e f g h i j k l m t u v w x y z n o p q r s
QR	a b c d e f g h i j k l m s t u v w x y z n o p q r
ST	a b c d e f g h i j k l m r s t u v w x y z n o p q
UV	a b c d e f g h i j k l m q r s t u v w x y z n o p
WX	a b c d e f g h i j k l m p q r s t u v w x y z n o
YZ	a b c d e f g h i j k l m o p q r s t u v w x y z n

Crediti foto – apprendre-en-ligne.net

Per cifrare utilizzando uno di questi alfabeti, si sceglie la lettera opposta nella tabella per sostituire la lettera nel testo normale. Ad esempio, se si esegue la crittografia utilizzando l'alfabeto AB, si sostituirà a per n, b per o, q per de così via.

Ad esempio, se la parola chiave **è** STEEL, gli alfabeti S, T, E, E, L, S, T, E, E, L, ecc. vengono utilizzati successivamente per crittografare il messaggio. Se crittografiamo la frase "**Porta cipher**" con la **chiave** STEEL, otteniamo:

Cancella	p	o	r	t	a	c	i	p	h	e	r
Chiave	**S**	**T**	**E**	**E**	**L**	**S**	**T**	**E**	**E**	**L**	**S**
Codificato	L	K	G	I	V	T	Z	E	S	Z	A

Il cifrario Porta fu utilizzato dalla regina Maria Antonietta per modificare e migliorare la PORTA cifrata da utilizzare nella sua corrispondenza. In particolare, aggiunse la caratteristica di codificare solo ogni altra lettera.

Fase 3: compiti a casa e idee di sviluppo

Che ne dici di una sfida? Passa messaggi in codice ai tuoi compagni di classe in modo che possano decifrarli.
Ad esempio, scegli un metodo di codifica e crittografa il tuo messaggio, quindi trasmettilo senza rivelare il metodo utilizzato.
Aggiungi un po' di suspense, assegnando un limite di tempo o una ricompensa.

Puoi anche creare la tua ruota di decodifica, che è facile da trovare su Internet:
https://www.youtube.com/watch?v=0Xuv58Uwu9o

Materiale necessario per il tour

Gli alunni che partecipano al tour dovranno avere matita, gomma e carta per trovare il codice giusto.

VISIT MATH

Cofinanziato dall'Unione europea

Il progetto è finanziato con il sostegno della Commissione europea. Questo progetto è stato finanziato con il sostegno della Commissione Europea. Questa pubblicazione riflette solo le opinioni dell'autore e la Commissione non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in essa contenute.

Codice progetto: 1-FR01-KA220-SCH-00027771

Scopri di più su Visit Math su: https://visitmath.eu

FERMAT SCIENCE
Une autre idée des maths

5th High School
Agrinio·Greece

Istituto Statale "E. Montale" Pontedera

LogoPsyCom.

ZS 31

YuzuPulse