Messaggi segreti

Gli agenti Boris e Berta comunicano per mezzo di messaggi segreti, che nessuno tranne loro deve capire. Boris vuole mandare a Berta il seguente messaggio:

INCONTRABILLYALLE6

Boris scrive le lettere del testo una dopo l'altra, da sinistra a destra e riga dopo riga dall'alto verso il basso, in una tabella con 4 colonne e 5 righe. Se ci sono spazi vuoti nella tabella, ci scrive *. La figura qui a lato mostra il risultato.

I	N	C	O
N	T	R	A
B	I	L	L
Y	A	L	L
E	6	*	*

Poi crea il messaggio segreto prendendo le lettere dall'alto verso il basso, colonna per colonna da sinistra a destra, e le scrive su un nuovo foglio:

INBYENTIA6CRLL*OALL*

Berta utilizza lo stesso metodo per rispondergli. Il messaggio segreto che manda a Boris è:

VNSDCAEAIUBCRSREIOIO

Che risposta ha mandato Berta?

- ◯ VABENELOINCONTROIO
- ◯ VABENECISARODISICURO
- ◯ DACCORDOCOSIPERME
- ◯ VABENEORAPERINCONTRO

- Spiegazione -

La risposta corretta è "**VABENECISARODISICURO**" (con gli spazi e la punteggiatura diventerebbe "Va bene, ci sarò di sicuro!").

Per scoprire il messaggio originale, si può usare il procedimento inverso a quello usato per ottenere il messaggio segreto. Innanzitutto bisogna scrivere le lettere del messaggio segreto nella griglia, dall'alto verso il basso, colonna per colonna da sinistra a destra, ottenendo:

VABE
NECI
SARO
DISI
CURO

Il messaggio originale si ottiene leggendo la griglia riga per riga partendo dall'angolo in alto a sinistra.

Un trucco per scoprire il messaggio originale, avendo solo 4

alternative possibili, è partire da ciascuna delle quattro alternative, applicare a ciascuna il procedimento descritto nel quesito e verificare da quale si ottiene la frase "**VNSDCAEAIUBCRSREIOIO**".

Dal momento che la procedura descritta nel quesito cambia solo l'ordine delle lettere, anche un controllo sulla frequenza delle lettere (quante volte compaiono nel messaggio originale e quello segreto) poteva aiutare a trovare la risposta corretta. Ad esempio, "**VABENELOINCONTROIO**" si può escludere perché contiene una sola R.

- Anche questa è informatica -

Spesso vogliamo che un messaggio, se intercettato, non sia comprensibile e questo vale anche quando il messaggio viene inviato all'interno di reti informatiche, ad esempio se il messaggio che abbiamo inviato contiene una password o delle informazioni private. Per questo motivo, i messaggi possono essere **cifrati** ovvero trasformati in messaggi segreti. Affinché questo possa funzionare, il ricevente autorizzato deve essere messo in grado di **decifrare** il messaggio, ossia risalire al messaggio originale, cosa che invece non deve poter fare un potenziale avversario.

Un metodo per cifrare (e decifrare) messaggi è chiamato **cifrario**. Quello usato in questo quesito è un cifrario a trasposizione, in cui le lettere del messaggio sono spostate in posizioni diverse in base a uno schema prefissato. Esistono anche cifrari molto più complicati, spesso basati su proprietà matematiche non banali. La **crittografia** è l'area di studio che si occupa dei cifrari.

Parole chiave: codifica, crittografia, cifrario a trasposizione, cifrare/decifrare

- Informazioni sul quesito -

Il quesito è stato proposto dal gruppo Bebras Regno Unito (id: 2016-UK-06)