Brute force

Cifrare un messaggio non lo rende illeggibile al 100%, la chiave infatti ha in alcuni casi un limite di grandezza, ad esempio si possono usare solo un numero limitato di caratteri o come per il *Cifrario di Cesare* è limitato al numero di caratteri presenti su un alfabeto.
È possibile quindi per un attaccante, colui che vuole scoprire il contenuto del messaggio cifrato senza che abbia avuto la nostra autorizzazione, di provare tutte le combinazioni possibili della chiave. Ovviamente gli ci andrà molto tempo per farlo usando determinati cifrari ma non con il *Cifrario di Cesare*!

Attività - Brute force distribuito

Preparazione: preparare 25 bigliettini di carta scrivendo su ciascuno un numero da 1 a 24. Piegare poi i bigliettini in modo che non sia possibile leggerne il numero scritto e porli all'interno di una ciotola. Fornire ad ogni studente una tavoletta e lettere magnetiche per scrivere.

Ieri, i nostri soldati sono riusciti ad intercettare dei messaggi che stavano trasportando dei messaggeri romani, ma sembra che questi messaggi contengano del testo non comprensibile. Fortunatamente i nostri esperti sono riusciti a scoprire l'algoritmo che utilizzano per rendere i loro messaggi incomprensibili, il cifrario di Cesare, ma non conosciamo la chiave con cui questi messaggi sono cifrati. Siccome potrebbero contenere informazioni importanti per non farci catturare dobbiamo fare in fretta a decifrare questi messaggi. Assegnerò ad ognuno di voi un numero e proverete a decifrare il messaggio.

1. l'insegnante scriva su una lavagna il seguente testo: "TRLWWTLEELNNSPCPXZLWWLACZDDTXLWFYLATPYL";
2. far estrarre ad ogni persona/gruppo un bigliettino con un numero;
3. dire ai ragazzi di decifrare il messaggio facendo lo spostamento delle lettere con il numero che hanno estratto.
4. appena hanno finito fategli leggere ad alta voce il testo decifrato per capire se la chiave utilizzata era quella giusta.

Lo spostamento era di 11 posizioni ed il contenuto del messaggio originale è : "I GALLI ATTACCHEREMO ALLA PROSSIMA LUNA PIENA".