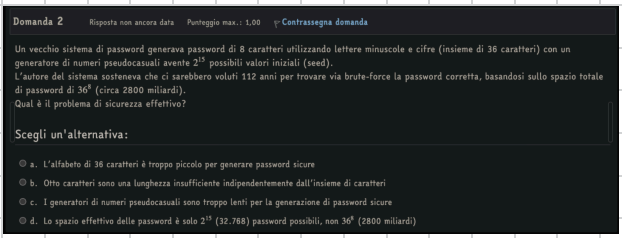
DETERMINARE LO SPAZIO DELLE PASSWORD

IN: - d dimensione delle password

- D alfabeto (# di caratteri usabili)
- s combinazioni del seed (Opzionale)

OUT: $\min\{D^d, s\}$

EX



Domanda 2 — Risposta non ancora data — Punteggio max.: 1,00 — Contrassegna domanda

Un vecchio sistema di password generava password di 8 caratteri utilizzando lettere minuscole e cifre (insieme di 36 caratteri) con un generatore di numeri pseudocasuali avente 2^{15} possibili valori iniziali (seed).
L'autore del sistema sosteneva che ci sarebbero voluti 112 anni per trovare via brute-force la password corretta, basandosi sullo spazio totale di password di 36^8 (circa 2800 miliardi).
Qual è il problema di sicurezza effettivo?

Scegli un'alternativa:

- a. L'alfabeto di 36 caratteri è troppo piccolo per generare password sicure
- b. Otto caratteri sono una lunghezza insufficiente indipendentemente dall'insieme di caratteri
- c. I generatori di numeri pseudocasuali sono troppo lenti per la generazione di password sicure
- d. Lo spazio effettivo delle password è solo 2^{15} (32.768) password possibili, non 36^8 (2800 miliardi)

- $D = 36 \quad d = 8 \quad s = 2^{15}$

$= \min\{D^d, s\}$

DETERMINARE TEMPO D'ATTACCO: SENZA FEEDBACK

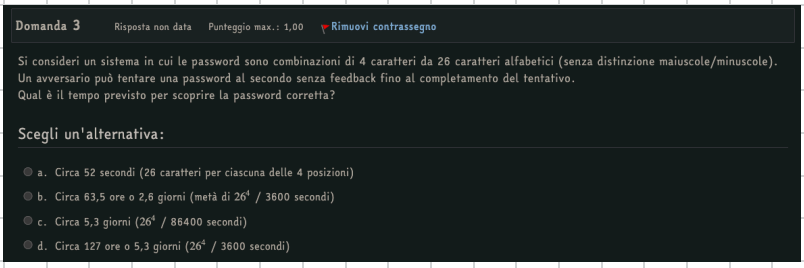
IN: - d: dimensione della password

- D: alfabeto (# di caratteri usabili)
- t: Tempo impiegato per risolvere 1 password.

OUT:

- $t \cdot D^d$: Nel caso peggiore
- $\frac{t \cdot D^d}{2}$: Nel caso medio in brute force

EX:



Domanda 3 — Risposta non data — Punteggio max.: 1,00 — Rimuovi contrassegno

Si consideri un sistema in cui le password sono combinazioni di 4 caratteri da 26 caratteri alfabetici (senza distinzione maiuscole/minuscole).
Un avversario può tentare una password al secondo senza feedback fino al completamento del tentativo.
Qual è il tempo previsto per scoprire la password corretta?

Scegli un'alternativa:

- a. Circa 52 secondi (26 caratteri per ciascuna delle 4 posizioni)
- b. Circa 63,5 ore o 2,6 giorni (metà di 26^4 / 3600 secondi)
- c. Circa 5,3 giorni (26^4 / 86400 secondi)
- d. Circa 127 ore o 5,3 giorni (26^4 / 3600 secondi)

- $D = 26, \quad d = 4, \quad t = 1s$

- $T_{peggiore} = t \cdot D^d = 1s \cdot 26^4 = \frac{26^4 s}{3600 s/h} \text{ (in ore)} \simeq \boxed{\text{127 h}}$

- $T_{medio} = \frac{t \cdot D^d}{2} = \frac{26^4 s}{2} = \frac{228 \text{ ore}}{3600} \simeq \boxed{63.5 \text{ h}}$

NB: Tempo previsto = T. medio

DETERMINARE TEMPO D'ATTACCO: CON FEEDBACK PER CHAR

IN:
- d: dimensione della password
- D: alfabeto (# di caratteri usabili)
- t: Tempo impiegato per risolvere 1 password.

OUT:
- T. peggiore: $D \cdot d \cdot t$
- Tmedio: $\frac{D \cdot d \cdot t}{2}$

EX:

Domanda 4 Risposta non data Punteggio max.: 1,00 Rimuovi contrassegno

Un sistema utilizza password di 4 caratteri da 26 caratteri alfabetici (senza distinzione maiuscole/minuscole). Un avversario può tentare una password al secondo.
Il sistema fornisce feedback immediato segnalando un errore non appena viene inserito ogni carattere errato (come facevano alcuni vecchi sistemi).
Qual è il tempo previsto per scoprire la password corretta?

Scegli un'alternativa:

a. Circa 52 secondi (in media 13 tentativi per posizione, 4 posizioni totali)
b. Circa 127 ore (tutti i 26^4 tentativi / 3600 secondi)
c. Circa 63,5 ore (metà di 26^4 tentativi / 3600 secondi)
d. Circa 104 secondi (26 caratteri per posizione, 4 posizioni totali)

- $T_{medio} = \frac{D \cdot d \cdot t}{2} = \frac{26 \cdot 4^2 \cdot 1s}{2} = \boxed{52s}$

DETERMINARE POPOLAZIONE: CON PATTERN

IN:
- Serie di sub alfabeti S_A S_B...
- Pattern con cui combinare le lettere: ABA

OUT: $= \prod_{l \in \{A,B,C\}} S_A^l$ Usa quanto sai di combinazioni

EX:

Domanda 5 Risposta non data Punteggio max.: 1,00 Rimuovi contrassegno

Un generatore di password fonetiche crea password utilizzando il pattern CVC (consonante, vocale, consonante) per ogni segmento, scegliendo due segmenti casualmente per formare password di sei lettere.
Dato: $V = \{a, e, i, o, u\}$ (5 vocali) e $C = \{b, c, d, f, \dots\}$ (21 consonanti)
Qual è la popolazione totale di password?

Scegli un'alternativa:

a. $(21 + 5 + 21)^6 = 47^6$ password
b. $21 \times 5 \times 21 \times 2 = 4.410$ password
c. $21^3 \times 5^3 = 1.157.625$ password
d. $(21 \times 5 \times 21)^2 = 2.205^2 = 4.862.025$ password

popolazione: $21^2 \cdot 5^2 \cdot 21^2 = D$