

Esame di TEORIA DEI SEGNALE

Quesito A5

Si vuole riservare l'accesso a un certo servizio a $M = 100$ utenti a ciascuno dei quali viene assegnata una diversa password formata da n cifre decimali.

- Si trovi il valore minimo di n (lunghezza della password) che garantisca una probabilità P minore di 10^{-2} che una persona non autorizzata riesca ad accedere al servizio eseguendo $k = 10$ tentativi casuali.

Quesito A5 (soluzione)

Sia $N = 10^n$ il numero totale di stringhe - Se solo M di queste sono password la probabilità di trovare una password scegliendo una stringa a caso (un tentativo) è: $p = \frac{M}{N}$, infatti lo spazio si può assumere uniforme date le condizioni del problema - Naturalmente la probabilità di non trovare una password facendo un tentativo è il complemento ossia: $q = 1 - p = 1 - \frac{M}{N}$.

La probabilità che si vuole mantenere minore di 10^{-2} è la probabilità di trovare almeno una password facendo k tentativi (supposti indipendenti) che si può esprimere così:

$$P = 1 - \Pr\{\text{non trovare alcuna password in } k \text{ tentativi}\} = 1 - q^k$$

Si cerca quindi il minimo valore di N (e quindi di n) che soddisfi la seguente:

$$P = 1 - q^k < 10^{-2}$$

ossia:

$$1 - \left(1 - \frac{M}{N}\right)^k < 10^{-2} \rightarrow N > \frac{M}{1 - (1 - 10^{-2})^{\frac{1}{k}}} = \frac{100}{1 - 0,99^{\frac{1}{10}}} = 0,99 \cdot 10^5 \approx 10^5 \rightarrow \boxed{n \geq 5}$$

Le password devono essere di almeno $n = 5$ cifre decimali -