

aspal

agenzia sarda pro su traballu
agenzia sarda per le politiche
attive del lavoro



REGIONE AUTONOMA
DE SARDEGNA
REGIONE AUTONOMA
DELLA SARDEGNA

Generatore di numeri casuali per estrazioni Linee Guida





Sommario

1	INTRODUZIONE.....	2
2	FUNZIONAMENTO DEL SOFTWARE	2
3	ORDINE CRONOLOGICO OPERAZIONI DI ESTRAZIONE	4
4	ESEMPIO ESTRAZIONE BASATA SULL'ESTRAZIONE SUPERENALOTTO N.131 DEL 03/10/2023	5
5	DETTAGLI ALGORITMO E SOFTWARE UTILIZZATO PER L'ESTRAZIONE	6

Data documento: 20/10/2023

File:

Versione/Edizione: 01.00

Redazione: Fabio Musio

Validazione: Andrea Matta

Approvazione/
rilascio: Andrea Alimonda



1 INTRODUZIONE

L'obiettivo di queste linee guida è quello di consentire l'utilizzo di un generatore di numeri casuali per poter effettuare delle estrazioni che rispettino i principi di trasparenza, pubblicità, imparzialità e ripetibilità.

Un generatore di numeri casuali è un software basato su un algoritmo che, tramite una variabile numerica imprevedibile da inserire nello stesso, genera una sequenza di numeri avente le stesse proprietà statistiche di una sequenza di numeri casuali.

Agli effetti pratici, la sequenza generata ha lo stesso valore di una sequenza realmente casuale, ma il fatto che si utilizzi un algoritmo garantisce di ricreare la stessa sequenza fornendo all'algoritmo la stessa Variabile numerica.

La Variabile numerica è la variabile che cambia il risultato dell'estrazione: inserendo la stessa Variabile Numerica nel generatore è possibile ripetere l'estrazione ed ottenere i medesimi risultati garantendo la ripetibilità.

Una Variabile numerica, quindi, è una sequenza di numeri casuali non prevedibili, e questa casualità deve essere certificata dallo Stato.

Nello specifico l'algoritmo, per la generazione di numeri pseudo-casuali, che verrà utilizzato per il sorteggio è chiamato generatore congruenziale moltiplicativo, anche detto Generatore di Lehmer, il quale è molto conosciuto. La teoria sulla quale poggia è semplice da capire e da implementare; inoltre risulta vantaggioso dal punto di vista computazionale. Il funzionamento dell'algoritmo è spiegato al capitolo 5.

L'algoritmo è stato implementato in un software reso disponibile gratuitamente e pubblicamente dalla Regione Emilia-Romagna ([LINK](#)).

Per rispettare i principi di trasparenza, pubblicità, imparzialità e ripetibilità, si è scelto di utilizzare, per ottenere una generazione causale di numeri, un variabile numerica composta dai primi quattro numeri estratti di una determinata estrazione del Superenalotto (stabilita in anticipo e dopo aver assegnato i rispettivi numeri ai partecipanti) in quanto di pubblico dominio e certificata come "non prevedibile in anticipo" dall'Agenzia delle Dogane e dei Monopoli.

Nella pratica, verrà generata un'estrazione basata sulla casualità ricavata da un'altra estrazione che verrà certificata dallo Stato (Agenzia delle Dogane e dei Monopoli) come casuale.

Nei capitoli successivi verrà spiegato nel dettaglio il funzionamento del software di estrazione e la procedura da seguire in ordine temporale per effettuare tale operazione, garantendo i principi di trasparenza, pubblicità, imparzialità e ripetibilità.

2 FUNZIONAMENTO DEL SOFTWARE

In questo capitolo verrà illustrato come utilizzare una Variabile Numerica certificata e di pubblico dominio per generare un'estrazione che sia ripetibile.

Come già spiegato nel capitolo precedente, il software che verrà utilizzato implementa l'algoritmo che genera l'estrazione di un insieme definito di numeri. Tale algoritmo necessita di una variabile numerica imprevedibile la quale, una volta definita e inserita nel software, andrà a generare la sequenza di numeri estratti.

Agli effetti pratici, la sequenza generata ha lo stesso valore di una sequenza realmente casuale, ma il fatto che si utilizzi un algoritmo garantisce la possibilità di ricreare la stessa sequenza, fornendo all'algoritmo la stessa Variabile Numerica.

Quindi quest'ultima è la variabile che cambia il risultato dell'estrazione: inserendo la stessa Variabile Numerica nel generatore è possibile ripetere l'estrazione ed ottenere i medesimi risultati garantendo la ripetibilità.

Una Variabile Numerica, quindi, è una sequenza di numeri casuali non prevedibili, e questa casualità deve essere certificata dallo Stato.

Il software utilizzato chiama questa variabile numerica "**Seme generatore**".



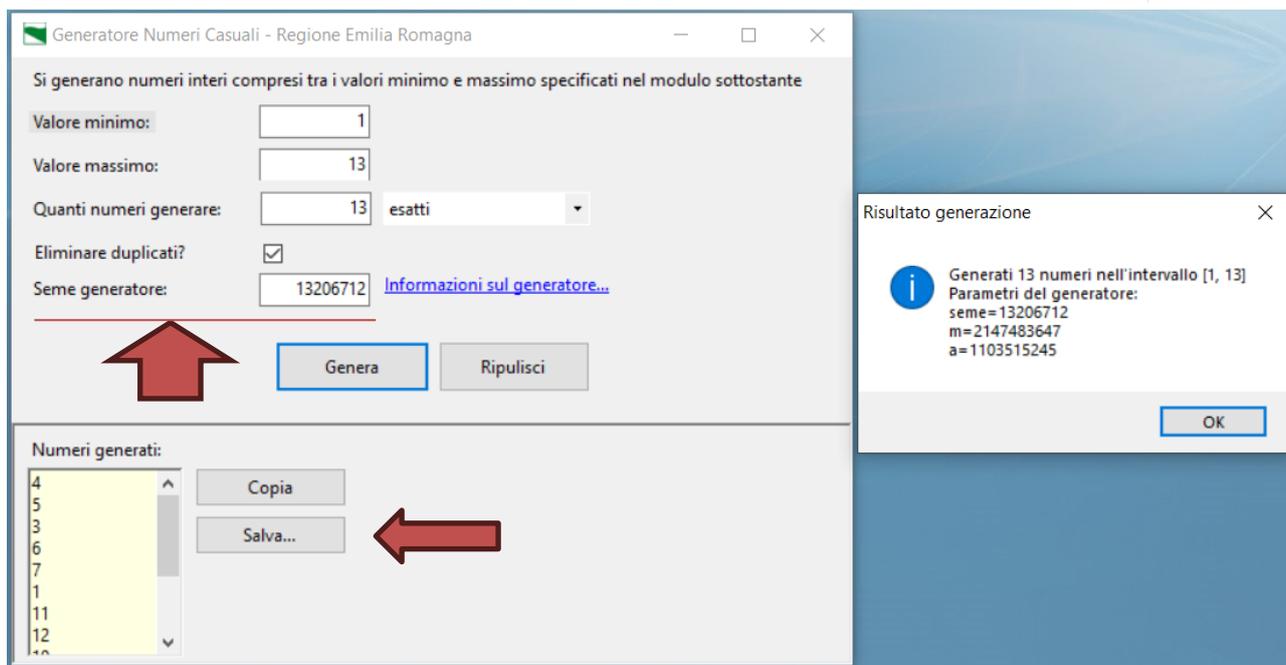


Immagine 1: interfaccia software di estrazione Windows



Immagine 2: interfaccia software di estrazione Sito Web Regione Emilia-Romagna

Nel software andranno inseriti i seguenti valori:

- Valore minimo** sempre impostato a 1, in quanto verrà assegnato ai partecipanti il proprio numero partendo da 1.
- Valore massimo** è il numero totale dei partecipanti, il quale corrisponderà al numero assegnato all'ultimo partecipante. Ad esempio, se saranno presenti 13 partecipanti, all'estrazione verrà assegnato agli stessi un numero che va da 1 a 13 (in questo caso il valore massimo da inserire nel software è 13). NB Il valore massimo supportato è superiore al milione.

- c) Tramite **“Quanti numeri generare”** sarà possibile selezionare due opzioni chiamate “Esatti” e “in % sul totale”:
Se verrà selezionata l’opzione “Esatti”, dovrà essere inserito lo stesso valore di “valore massimo” per estrarre tutti i partecipanti. In questo caso il “valore massimo” non può superare 999.
Se verrà selezionata l’opzione “in % sul totale” dovrà essere impostata la % dei partecipanti da estrarre riferita al “valore massimo” sopra. Per ottenere il 100% dei partecipanti estratti, quindi il 100% di “valore massimo” dovrà essere impostato il valore 100. Questa opzione può risultare utile quando i candidati da estrarre sono più di 999. Attualmente l’opzione “in % sul totale” è stata testata con 100.000 partecipanti.
- d) Dovrà essere spuntata l’opzione **“Elimina duplicati?”** come nell’immagine sopra, al fine di evitare di estrarre lo stesso numero più di una volta.
- e) Nel campo **“Seme generatore”** verrà inserita la variabile numerica che genera la casualità come specificato al capitolo 3 nel punto 2 e 3 (inserendo la stessa variabile numerica otteniamo la stessa estrazione).
- f) Per generare l’estrazione si dovrà cliccare su **“Genera”** e salvare l’estrazione appena effettuata cliccando su salva.

Nota: Tutti i partecipanti sono in grado di ripetere l’estrazione in qualsiasi momento in quanto avranno a disposizione in quanto sarà di dominio pubblico, non solo il software e la relativa configurazione usata, ma lo sarà anche la variabile numerica casuale generata dai primi quattro numeri estratti (da una predeterminata estrazione del superenalotto).

3 ORDINE CRONOLOGICO OPERAZIONI DI ESTRAZIONE

Di seguito sono indicati i passaggi in ordine cronologico per effettuare un’estrazione che rispetti i principi di trasparenza, pubblicità, imparzialità e ripetibilità:

- 1) Verrà assegnato un numero da **“1 a X”** ad ogni partecipante all’estrazione, dove “X” corrisponde al numero totale di partecipanti.
- 2) Verrà comunicato, Congiuntamente al numero assegnato ad ogni partecipante, anche la variabile numerica che verrà utilizzata: in particolare andrà specificato anche che la variabile numerica corrisponderà ai primi 4 numeri del superenalotto (vedi punto 3), inseriti come unico numero senza virgole e senza punti e in ordine cronologico dal primo estratto fino al quarto compreso. (i numeri da 1 a 9 sono inseriti nell’algoritmo senza lo zero).
- 3) Verrà comunicato il numero progressivo dell’estrazione del superenalotto scelta, specificando “il numero progressivo dell’estrazione” che non dev’essere ancora avvenuta nel momento in cui viene comunicata (dev’essere successivo a quello della comunicazione di cui al punto 1 e 2). Tramite il sito web dell’[Agenzia delle Dogane e dei Monopoli \(LINK\)](#) è possibile visionare le estrazioni già effettuate ed il relativo numeri della giocata.



Immagine 3: [Sito Web – Agenzia delle Dogane e dei Monopoli](#)



Esempio: Dovrà essere scelto un numero di un'estrazione non ancora avvenuta : se nel sito web dell'[Agenzia delle Dogane e dei Monopoli \(LINK\)](#) compare una situazione simile a quella dell'immagine sopra, significa che l'estrazione N.139 è avvenuta e non può essere utilizzata. In questo caso si dovrà comunicare ai partecipanti, che verrà utilizzata la variabile numerica relativa all'estrazione N.140 (o superiore) in quanto non ancora avvenuta al momento della comunicazione.

- 4) Nella stessa comunicazione, Verrà indicato il software che sarà utilizzato per effettuare l'estrazione ([LINK](#))
- 5) Verranno trasmesse le presenti linee guida per l'utilizzo del software di estrazione e il relativo algoritmo.
- 6) Una volta effettuata l'estrazione N.xxx scelta tra le estrazioni del superenalotto (nell'esempio del punto 3 la n. 140), si otterrà la "variabile numerica" da inserire nel software per l'elaborazione della estrazione.
- 7) Per effettuare l'estrazione, l'amministrazione dovrà:
 - i) inserire la configurazione software in base al numero dei partecipanti, definendo, in ordine, "valore massimo", quanti numeri generare uguale a valore massimo con opzione "Esatti", e spuntare "elimina duplicati".
 - ii) inserire i valori della Variabile numerica nel software di generazione, i quali corrispondono ai primi 4 numeri estratti dall'estrazione N.xxx del superenalotto (nell'esempio del punto 3 la n. 140)
 - iii) Salvare l'estrazione effettuata cliccando sul tasto salva.
- 8) Verrà comunicato ai partecipanti il risultato dell'elaborazione dell'estrazione.

4 ESEMPIO ESTRAZIONE BASATA SULL'ESTRAZIONE SUPERENALOTTO N.131 DEL 03/10/2023

Presupponendo che siano state già comunicate ad ogni partecipante le informazioni definite nel capitolo precedente verrà simulata un'estrazione.

Nel presente esempio verrà effettuata un'estrazione tra **13 partecipanti**. Ad ogni partecipante è stato comunicato il **02/10/2023** il relativo **numero assegnato da 1 a 13** la variabile numerica scelta tra le estrazioni del superenalotto, nello specifico l'estrazione **N.131 del 03/10/2023** (N.B. la data dell'estrazione è successiva rispetto alla comunicazione per garantire il requisito dell'imprevedibilità).

Si può visionare la Variabile Numerica, cioè i primi 4 numeri estratti dell'estrazione **N.131 del 03/10/2023** sul sito web dell'Agenzia delle Dogane e dei Monopoli ([LINK](#)):

Il **04/10/2023** avviene l'elaborazione dell'estrazione da parte dell'amministrazione inserendo i seguenti dati nel software:

1. Dal sito dell'Agenzia delle Dogane e dei Monopoli ([LINK](#)), estrapoliamo i primi quattro numeri estratti.

ADM
AGENZIA DELLE DOGANE E DEI MONOPOLI
<https://www.adm.gov.it/portale/monopoli/>

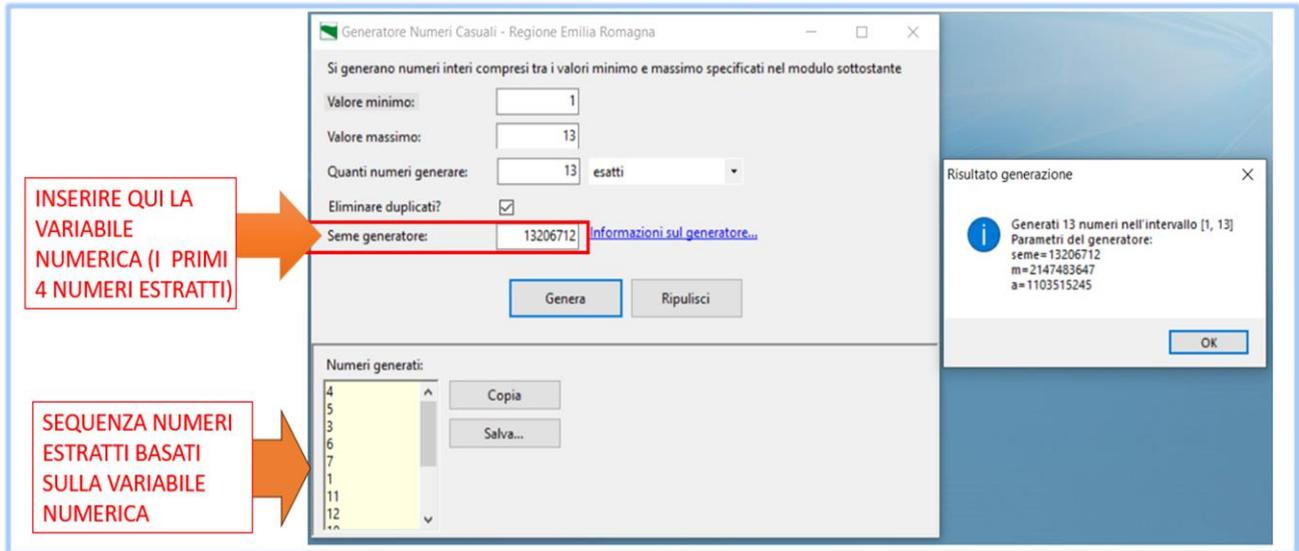
Estrazione
Superenalotto n. 131 del 03/10/2023

Combinazione Vincente
13 20 67 12 54 84

COPIARE I PRIMI 4 NUMERI ESTRATTI IN ORDINE CRONOLOGICO SONO LA VARIABILE NUMERICA CERTIFICATA DALLO STATO DELL'ALGORITMO

2. Nel software saranno inserite le seguenti configurazioni e procederemo come indicato nel capitolo 2.





3. Salvare i risultati dell'estrazione facendo clic su salva, i numeri più in alto corrispondono ai primi estratti.

4. Verrà comunicato ai partecipanti il risultato dell'estrazione.

Nota: Ogni partecipante può in autonomia ripetere l'estrazione e verificarne la correttezza.

5 DETTAGLI ALGORITMO E SOFTWARE UTILIZZATO PER L'ESTRAZIONE

È necessario specificare, preliminarmente, che un computer, in quanto macchina assolutamente priva di arbitrio (ovvero deterministica), non è in grado di generare dei numeri casuali nel senso letterale del termine.

Quello che si può fare è realizzare un algoritmo che generi una sequenza di numeri avente le stesse proprietà statistiche di una sequenza di numeri casuali.

Sostanzialmente la sequenza generata ha lo stesso valore di una sequenza realmente casuale, ma il fatto che si utilizzi un algoritmo, implica che è possibile ricreare la stessa sequenza fornendo all'algoritmo lo stesso valore iniziale (Chiamato variabile numerica o seme del generatore).

L'algoritmo che si utilizzerà per il sorteggio è chiamato generatore congruenziale moltiplicativo, anche detto "Generatore di Lehmer", un algoritmo per la generazione di numeri pseudo-casuali vecchio e molto conosciuto. La teoria sulla quale poggia è semplice da capire e da implementare; inoltre ha il vantaggio di essere computazionalmente leggero.

L'algoritmo, a partire dal seme identificato con X_0 , è definito in termini ricorsivi nel seguente modo:

$$X_{k+1} = (aX_k + c) \bmod m, k > 0$$

I numeri generati appartengono all'intervallo $[0, m-1]$.

m è un numero intero.

a e c sono numeri interi maggiori o uguali a 0 e minori di m .

È di particolare importanza per la bontà della sequenza è la scelta dei valori di a , c e m , i valori scelti sono stati tratti dalla letteratura e sono: $m=2147483647$ ($2^{31}-1$), $a=1103515245$, $c=0$.

L'implementazione deve gestire i casi di overflow che possono capitare durante la moltiplicazione aX_k . Dato che dopo la moltiplicazione si esegue una operazione di modulo, l'overflow può essere evitato distribuendo la moltiplicazione su più parti ed eliminando i termini più significativi (ovvero le cifre più a sinistra).

Il software scelto per implementare l'algoritmo sopra è fornito dalla Regione Emilia-Romagna, sia come software Windows che, come Web App, entrambi disponibili gratuitamente all'indirizzo HTML indicato nei riferimenti sotto.

Riferimenti:

<https://wwwservizi.regione.emilia-romagna.it/generatore/Note.aspx>

<https://wwwservizi.regione.emilia-romagna.it/generatore/Default.aspx>