Program Name- To generate a One Time Password or Unique Identification URL

Project Category- Strings

What is a One Time Password (OTP) ?-

A **one-time password** (**OTP**) is a password that is valid for only one login session or transaction, on a computer system or other digital device.

For more details go to - https://en.wikipedia.org/wiki/One-time_password

Applications-

OTPs are widely used in websites like- Facebook, Google Sign-in, Wifi – accessing, Railways Portal Login etc.

Algorithm-

We randomly pick characters from our all possibilities and generate a string of the desired length from it. OTPs are generally 6-7 characters long as randomness in 6-7 characters almost guarantees a secure way of logging in.

Time Complexity-

O(N) , where N = number of characters in our OTP

Auxiliary Space-

Apart from the string having all possible characters we require O(N) space to hold the OTP, where N = number of characters in our OTP

An Interesting Fact on Unique Identification URL-

Even the G4G IDE (http://code.geeksforgeeks.org/) has a unique string for all the codes compiled through it.

For example, http://code.geeksforgeeks.org/Ks84Ck has the unique string – "Ks84Ck" at the end which is unique for this code only.

How would you think this would have been generated ?

Well it is a great possibility that it uses the same algorithm as an OTP is generated. If by chance (very rare) the unique string generated is already been generated before and has been associated with a different code then another random string is used.

As per now it seems that only six character strings are generated randomly for a unique identification of all codes. A time will come when all the possible six character strings will get exhausted (It is very possible as G4G IDE is a very popular one).

So yes even the web-related stuffs also heavily relies on randomness.

Probability of collision of two OTPs -

The length of OTP is 6 and the set size of all possible characters in the OTP is 62. So the total number of possible sets of the pair of OTPs are- 62^{12}.

Some of them are – [{aaaaaa, aaaaaa}, {aaaaaa, aaaaab},.....{456789, 456788}, {456789, 456789}]

But the possible sets of equal pair of OTPs are - 62^{6}.

Some of them are- [{aaaaaa, aaaaaa}, {aaaaab, aaaaab},.....{456788, 456788}, {456789, 456789}]

Hence the probability of collision of two OTPs is-
$62^{6} / 62^{12} = 1 / 62^{6} = 1 / 56800235584 = 1.7605561^{-11}$

So the probability of two OTPs colliding are as less probable as the existence of your life on earth (Ratio of the number of years you will live to the number of years from the start of the universe and everything in existence)

So yes OTPs are way more secure than static passwords !

References-

https://en.wikipedia.org/wiki/One-time_password