¿Cómo elegir una buena contraseña?

Lo primero que tenemos que hacer es leer la siguiente lista con las 40 contraseñas más comunes e inseguras.

- **0**
- **1234**
- **12345**
- **111111**
- **123123**
- **123456**
- **654321**
- **1234567**
- **12345678**
- **abc123**
- **2000**
- **696969**
- **admin**
- **admin1234**
- **america**
- **ashley**
- **bailey**
- **baseball**
- **bonita**
- **contraseña**
- **dragon**
- **estrella**
- **football**
- **iloveyou**
- **letmein**
- **mariposa**
- **master**
- **michael**
- **monkey**
- **passw0rd**
- **password**
- **qazwsx**
- **qwerty**
- **shadow**
- **sunshine**
- **superman**
- **tequiero**
- **trustno1**
- **mustang**
- **harley**

En Segundo lugar revisar las contraseñas que **NO DEBEN** usarse porque son fáciles de conocer o hackear.

Nombres Propios *(alejandra, alberto, juan carlos, roberto, etc...)*

Palabras Típicas de los 80's (sexo, amor, dios, dinero, muchas veces se combinan con números para cumplir el mínimo de caracteres exigido)

Nombre de la Página/ Sitio / Servicios (si la clave es de facebook, la clave será facebook, lo mismo con gmail, hotmail, o correo si es la del correo electrónico)

Nº de Documentos o Celular (son muy utilizados y dan sensación de seguridad, pero esta información se puede conseguir fácilmente)

Gustos Personales (equipos de fútbol, artistas o grupos musicales, nombres de actores o películas, etc…)

Tercero utilizar alguna técnica para generar contraseñas difíciles y complejas, y que a su vez sean fáciles de recordar. Ya que la cantidad de contraseñas que debemos de recordar nos lleva a usar a veces el mismo password (o un par de ellos) para los todos los servicios que usamos. Y claro, seleccionamos contraseñas fáciles de aprenderse y por lo tanto de adivinar.

Técnica HayStack.

El inventor de este método es **Steve Gibson**, un verdadero experto en seguridad. En su página viene mucho mejor explicado. https://www.grc.com/haystack.htm

Romper contraseñas por fuerza bruta se basa en el hecho de probar "n" combinaciones posibles de contraseñas, empezando por las más comunes y posteriormente "**armar**" posibles contraseñas utilizando herramientas de software que automatizan la labor.

Es posible generar contraseñas robustas pero fáciles de recordar si se tiene en cuenta el tamaño del "**search space**" o **espacio de búsqueda** según nos lo explica Steve.

Es posible por lo tanto generar una contraseña fácil de recordar y volverla robusta al completarla con caracteres ("**padding**"); de esta manera hacemos que el espacio de búsqueda o "search space" se amplíe considerablemente haciendo un hackeo por fuerza bruta excesivamente tardado. Asimismo se puede complementar esta técnica al introducir mayúsculas y números de tal forma que por ejemplo :

"**teclado**" queda compuesto como: **T3clado……**

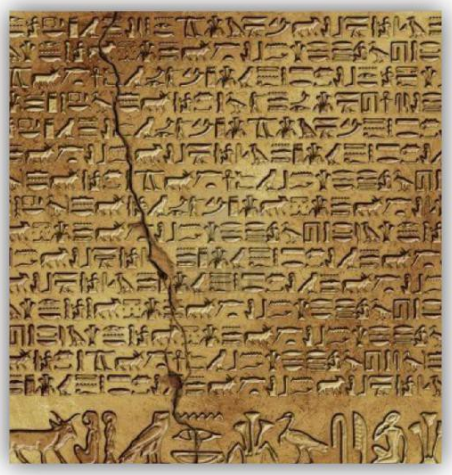
Vemos la "T" mayúscula, un "3" en lugar de "e" con diez puntos "." y según la calculadora del sitio ya mencionado, esta contraseña tardaría varios millones de años en descubrirse por un método de fuerza bruta/exhaustivo

Otros ejemplos:

E5tract0%%%%%%%%%%%

Rut3ador!!!!!!!!!!!!

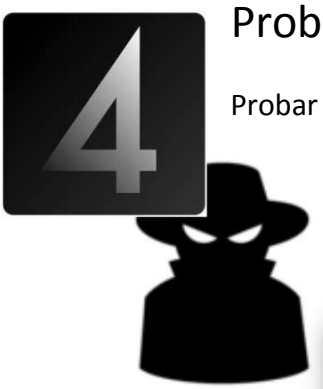
G4to********



Técnica basada en Frases.

Existen varias maneras de crear una "passphrase" en lugar de un "**password**". Si buscas en Google "create passphrase" encontrarás varias sugerencias. Por ejemplo una la propone Microsoft:

Iniciamos con una frase que te sea fácil de recordar: **"Oid mortales el grito sagrado"**. Le quitamos los espacios en blanco "Oidmortaleselgritosagrado". Sustituimos algunas letras por números (se recomienda siempre sustituir los mismos números por las mismas letras para no hacerse bolas), por ejemplo "1" en lugar de "i": "O1dmortaleselgr1tosagrado".



Probar cuan seguro es nuestra contraseña

Probar en **HOW SECURE IS MY PASSWORD?** (http://howsecureismypassword.net) cuan segura en nuestra contraseña y poder comprobar cuan fácil que resulta descubrir una contraseña con un ordenador doméstico y un programa de **craqueo** por diccionario y/o fuerza bruta.