

ALGORITMOS DE CREACIÓN DE CONTRASEÑAS

Trabajo de Alejandro Sainz Sainz

SISTEMAS
INFORMÁTICOS
24-25

INTRODUCCIÓN	3
BREVE COMIENZO	4
Longitud y tipos de caracteres	4
Inclusión de información personal o palabras existentes	5
Uso repetido de la misma contraseña	5
Pequeño resumen	7
ALGORITMOS DE GENERACIÓN DE CONTRASEÑAS	8
Hashing	8
Criptografía y Encriptado	10
CONCLUSIÓN Y REFLEXIÓN	11
BIBLIOGRAFIA Y ENLACES	12

TABLA DE FIGURAS

1 Tiempo requerido para romper una contraseña según su composición.....4

2 Si es que a veces nos lo ganamos a pulso.....6

3 Funcionamiento básico del hashing9

INTRODUCCIÓN

Con el auge de las nuevas tecnologías, de las aplicaciones como servicio, de la autenticación sobre servidores de aplicaciones o programas, y con la necesidad de mejorar la seguridad en todos esos ámbitos, apareció la necesidad también de asegurar una forma en la que cada usuario se pudiese identificar de forma única y segura. De esta necesidad surge como solución la aplicación de contraseñas.

Como contrapartida a lo comentado anteriormente, surgen prácticas, algunas de ellas ilícitas para apropiarse de esas credenciales, de las cuales la contraseña es la que tiene un mayor valor, por lo que se desarrollan una serie de normas para crear contraseñas más seguras, más difíciles de detectar o de romper mediante fuerza bruta. Estas normas o buenas prácticas hacen, nuevamente, que vuelva a evolucionar la forma es que estas son conseguidas de manera ilícita o por descuido de los propios usuarios.

En este ciclo constante, de actualización de ambas partes, vuelve a generar un cambio, que ya venía de épocas anteriores, el cuál es la aplicación de la criptografía y encriptación de estas claves, que pueden ser vitales para proteger nuestros datos. Se actualizan las buenas prácticas, y sobre todo, surgen algoritmos de generación de estas claves que las hacen mucho más complicadas a la hora de ser descubiertas, quebradas o descriptadas.

BREVE COMIENZO

Para comenzar con este tema de una forma más ligera, comenzaremos comentando brevemente algunas de las políticas más comunes a la hora de generar contraseñas seguras, para luego pasar a hablar de los algoritmos de generación de contraseñas propias.


Longitud y tipos de caracteres

La primera y más común de todas, la longitud.

Una contraseña muy corta puede llegar a ser muy fácil de romper o descubrir, incluso a mano. El bajo número de combinaciones que se pueden formar con una longitud baja, digamos 4 o 5 por ejemplo, hace que, aunque pueda llevar algo de tiempo, por medio de ensayo o error, se puedan romper simplemente por insistencia. Vamos a ver un pequeño ejemplo gráfico.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

 [Learn how we made this table at hivesystems.io/password](https://hivesystems.io/password)

1 Tiempo requerido para romper una contraseña según su composición.

Como podemos observar en la tabla 1, dependiendo de la longitud, y por ahora sólo estamos hablando de longitud, podemos ver que, a menor longitud, el tiempo de ruptura es instantáneo, independientemente de la composición. Una vez comenzamos a aumentar la longitud, empieza a aumentar, de forma exponencial, la dificultad de atravesar la seguridad de nuestra clave.

Alejandro Sainz Sainz

Siguiendo la progresión de nuestra tabla, podemos comenzar ahora a hablar de la composición de nuestra contraseña. Una clave sólo compuesta por números es un sistema muy simple (miedo me dan los pines de la tarjeta de crédito, o los del móvil), pero a medida que añadimos elementos diversos a nuestro sistema, vamos proporcionando mayor complejidad y seguridad y, por lo tanto, aumentando mucho la cantidad de tiempo necesaria para bypassear nuestra pass.

Inclusión de información personal o palabras existentes

Otras de las buenas prácticas a la hora de generar nuestra clave es evitar la inclusión de datos personales como parte de la misma, véase fechas de nacimiento, nombres de familiares, nombre del perro, etc. Esos datos pueden ser accesibles desde el exterior y ser probados como clave pudiendo tener fatales consecuencias.

En cuanto a palabras existentes nos referimos al no uso de palabras que existan en nuestro diccionario, que pueden ser usadas en nuestra contra, ya que con el afán de crear una clave que nos sea fácil de recordar tendemos a usar palabra que son de uso cotidiano y al final pueden jugar en nuestra contra.

Uso repetido de la misma contraseña

Como cada vez crece más el número de contraseñas que tenemos que usar, se habla en algunos artículos de incluso unas cien por persona, tendemos a usar la misma en muchos sitios distintos, a veces exactamente igual y otras con pequeñas variaciones. Eso puede provocar que una vez comprometida la contraseña en una plataforma o sistema, puedan quedar comprometidas en otros.

Alejandro Sainz Sainz

Y para ejemplo de lo dicho anteriormente, un botón.

Vamos a ver una pequeña tabla de contraseñas usadas con asiduidad y el tiempo de ruptura asociado.

RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	password	< 1 Second	4,929,113
2	123456	< 1 Second	1,523,537
3	123456789	< 1 Second	413,056
4	guest	10 Seconds	376,417
5	qwerty	< 1 Second	309,679
6	12345678	< 1 Second	284,946
7	111111	< 1 Second	229,047
8	12345	< 1 Second	188,602
9	co1123456	11 Seconds	140,505
10	123123	< 1 Second	127,762
11	1234567	< 1 Second	110,279
12	1234	< 1 Second	106,929
13	1234567890	< 1 Second	105,189
14	000000	< 1 Second	102,636
15	555555	< 1 Second	98,353
16	666666	< 1 Second	91,274
17	123321	< 1 Second	83,241
18	654321	< 1 Second	81,231
19	7777777	< 1 Second	74,233
20	123	< 1 Second	60,795

2 Si es que a veces nos lo ganamos a pulso

Pequeño resumen

Para afianzar todo esto que hemos comentado hasta ahora, vamos a realizar un par de menciones.

<https://www.welivesecurity.com/la-es/2023/05/04/consejos-crear-politica-contrasenas-empresa/>

Si seguimos este link, vamos a una de las muchas páginas que hay por internet, en la que se nos indica y se nos anima a seguir ciertas prácticas para mejorar el nivel de seguridad de nuestras claves. Y en la que se nos muestran ciertos casos en el pasado que nos muestran que no hacemos ningún caso.

Que sepamos también que el ingeniero Bill Burr escribió en 2003 un estándar para la seguridad de las contraseñas. Un estándar que se ha seguido y se ha actualizado desde entonces.

<https://pages.nist.gov/800-63-3/>

Después de varios años de esta implementación el propio Bill Burr comentaba lo siguiente:

“Simplemente vuelve loca a la gente y no eligen buenas contraseñas sin importar lo que hagas”.

También encontramos alguna que otra reflexión curiosa:

"A través de 20 años de esfuerzo, hemos capacitado con éxito a todos para usar contraseñas que son difíciles de recordar para los humanos, pero fáciles de adivinar para las computadoras".

A parte de todo esto que hemos comentado se han creado infinidad de sistemas, como el 2FA (Two Factor Authenticator) que es un sistema de autenticación en dos pasos, los CAPCHA que son sistemas que nos hacen elegir entre una serie de opciones o introducir textos o números adicionales para comprobar que somos “humanos”, e incluso las contraseñas de una sólo uso, generadores de passwords limitados a un solo uso que nos crean una clave, para así, dadas nuestras costumbre, que no usemos una variante de nuestra clave favorita.

ALGORITMOS DE GENERACIÓN DE CONTRASEÑAS

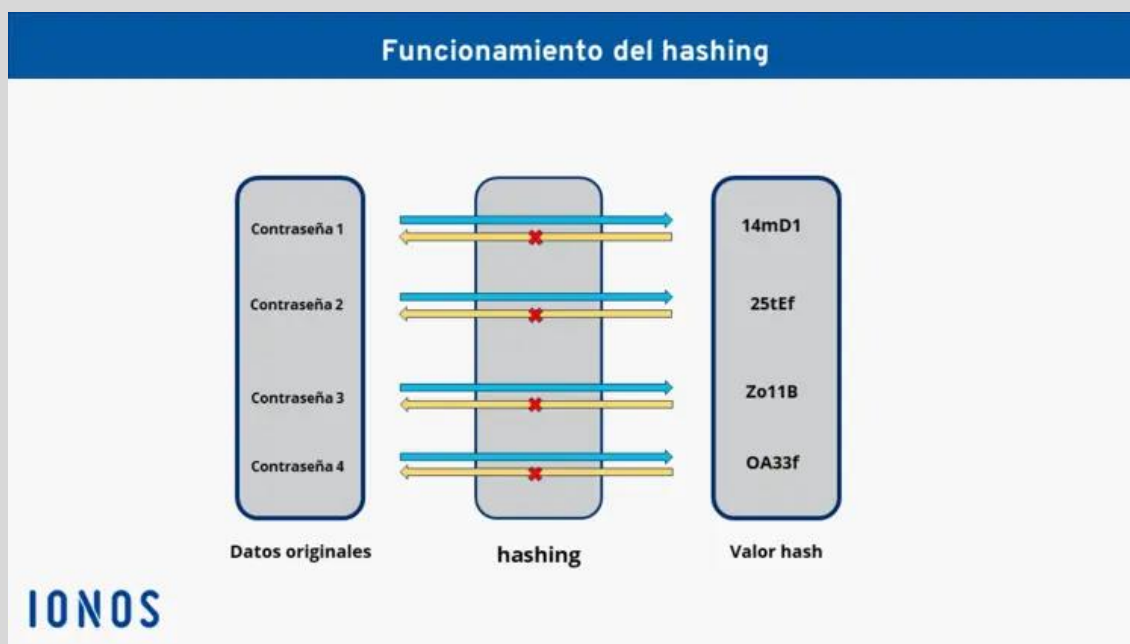
A raíz de todo lo comentado con anterioridad, surge la necesidad, sobre todo en el ámbito profesional, de crear un sistema que nos cree claves más complejas, he incluso que sea el propio sistema el que las administre.

Esto también viene dado por el aumento de la capacidad de los ordenadores, cuya capacidad de proceso y la ingente cantidad de cálculos que pueden realizar por segundo, tengan más capacidad para descubrir o romper las claves que usamos y generamos.

En este caso sólo voy a hablar de dos sistemas en concreto, no de las diferentes variantes de los mismos que existen actualmente, tanto sistemas de código abierto como sistemas propietarios creados por diferentes compañías.

Hashing

Pues, intentando explicarlo con mis propias palabras, el hashing es un sistema mediante el cual transformamos una cadena de texto y la convertimos en otra totalmente diferente, la cual no puede ser revertida a su valor original salvo que se tenga la clave o fórmula con la que fue creada. Es un sistema para que la información, en el caso que nos atañe, las contraseñas, no se almacenen ni transmitan en forma de texto plano.



3 Funcionamiento básico del hashing

El hashing, cómo indica el título de nuestra tarea, es una suerte de algoritmo de encriptado que transforma fragmentos de texto plano en otros totalmente diferentes, y que siempre tienen la misma longitud. Estos nuevos caracteres suelen ser caracteres hexadecimales cuya longitud y valor depende del algoritmo usado.

Estos valores se almacenan en tablas hash, que son más compactas y livianas. Esta cadena final no es legible de la forma tradicional y a ser posible estas cadenas no pueden ser revertidas a su forma original aun conociendo el algoritmo usado. En lo referente a las contraseñas estos es lo que nos importa.

Si hemos seguido algunas de las indicaciones del capítulo anterior, y luego hemos sometido nuestra contraseña a este proceso, generaremos una nueva cadena completamente ilegible, más fácil de guardar y casi imposible de descifrar.

Existen diferentes algoritmos de hashing que se pueden aplicar a los diferentes datos, cada uno de ellos produce un resultado diferente, ya sea en la longitud de la cadena generada como en la forma en la que agrupan los diferentes caracteres para transformarlos en otros.

<https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/hashing/>

Criptografía y Encriptado

La criptografía, de forma muy general, es la transformación de la información o de los caracteres, en otros siguiendo un patrón o método, que sólo conocen una serie de elementos para luego volver a recuperar la cadena original aplicando el método inverso en la cadena modificada. Los métodos modernos generan claves de longitudes que pueden llegar hasta los 256 caracteres, lo que genera una cantidad de posibilidades enormes en número de combinaciones y limita mucho la posibilidad de ser descubierta esa cadena mediante fuerza bruta.

En el campo de la criptografía encontramos el mayor número de algoritmos distinto, siendo uno de los primeros en el campo informático el llamado DES (Data Encryption Standard) desarrollado por IBM en la década de los 70.

En el ámbito histórico, por ejemplo, podemos encontrar el método Cesar, usado por Julio Cesar, que permutaba las posiciones de las letras del mensaje original por otras a tres posiciones de distancia, o las máquinas enigma, que dependiendo del rotor que se aplicaba generaban un mensaje que sólo podía ser descifrado por otra máquina enigma que escribiese el mensaje modificado usando la misma configuración de la máquina.

Estos algoritmos criptográficos se basan en tres sistemas diferentes:

El simétrico, el asimétrico y el sistema híbrido.

Para diferenciarlos diremos que:

El sistema simétrico usa una clave común para las dos partes; en el sistema asimétrico cada parte genera un par de claves, una propia y una común, y trabaja en base a las dos; por último, en el sistema híbrido, como se puede suponer, se usa una mezcla de los dos anteriores.

Todos estos sistemas, con la evolución de los mismos protocolos que los componen, han ido evolucionando a lo largo del tiempo.

Podemos contar con el DES, DES3d, AES, MD-5 en cuanto a encriptación y, en cuanto a códigos HASH algunos ejemplos son el Argon 2, Bcrypt, SHA-256 y otros muchos.

Tener en cuenta que cada uno de ellos simplemente lo que hace es cambiar su funcionamiento y los métodos con los que realizan su labor. Algunos agrupan los bits originales en grupos de 8, otros de 16, algunos realizan un solo encriptado y luego un cifrado adicional, mientras que otros realizan triple cifrado y luego una función hash. Las combinaciones son casi infinitas, eso sin tener en cuenta que mucho de los nuevos lenguajes de programación permiten

Alejandro Sainz Sainz

que los desarrolladores creen sus propios algoritmos de hash o de encriptación, por lo que una palabra sencilla, como puede ser nuestro password, puede acabar convirtiéndose en una cadena hexadecimal prácticamente indescifrable, o que en caso de ser descifrada será dentro de muchos años, cuando ya ni estemos aquí para necesitarla.

<https://www.ionos.es/digitalguide/servidores/seguridad/todo-sobre-los-metodos-de-encriptado/>

CONCLUSIÓN Y REFLEXIÓN

Como hemos visto a lo largo de este tema, aunque reconozco que, de forma muy general, vemos que la forma de mejorar nuestros sistemas de protección de la información, por medio de claves, ha evolucionado tanto como el propio tratamiento de la información.

Partiendo siempre de claves que sólo nosotros conocemos, apoyado por formas de convertir esas claves en otras muy diferente mediante, de nuevo, otras claves que sólo nosotros conocemos, hemos ido mejorando nuestros sistemas de seguridad en torno a los datos, tanto los nuestros como aquellos que manejamos en nuestros propios entornos de trabajo.

Los diferentes sistemas evolucionan siempre basándose en sistemas matemáticos y en ciertas operaciones, como por ejemplo el XOR (que estoy empezando a pensar que va a estar en el centro del universo), debido a que las diferentes variaciones que podemos obtener mediante el uso de las diferentes operaciones matemáticas son casi infinitos.

Todo ellos, para que al final, como he podido leer en algunos de los artículos, acabemos utilizando 123456 y nos acabe dando igual todo.

BIBLIOGRAFIA Y ENLACES

<https://www.welivesecurity.com/la-es/2023/05/04/consejos-crear-politica-contrasenas-empresa/>

<https://pages.nist.gov/800-63-3/>

<https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/hashing/>

<https://www.ionos.es/digitalguide/servidores/seguridad/todo-sobre-los-metodos-de-encryptado/>

<https://learn.microsoft.com/en-us/dotnet/standard/security/generating-keys-for-encryption-and-decryption>