

التحدي الأسبوعي رقم 1 : تحليل كلمة المرور

كلمات المرور المعطاة مشفرة بخوارزم Md5

تُعد دالة هاش تشفيرية (Message Digest) من أكثر دوال الاختزال انتشارًا، وقد صُممت في نسختها الأولى (MD2) عام 1989م عن طريق الدكتور رونالد ريفست أستاذ الحاسب في معهد ماساتشوستس للتقنية (MIT)، وتم تطويرها إلى نسخة (MD5) عن طريق مطوّرها نفسه عام 1991م بعد أن تمّت دراسة خواصّ الأمن فيها وتغطية ثغرات سابقتها لفترة طويلة. تستخدم MD5 دالة ميركل ديمقارد (Merkle–Damgård construction)، وتقوم على اختزال رسالة ذات طول متغيّر إلى طول ثابت هو 128 بت بغضّ النظر عن طولها الأصليّ، حيث يتم تحويل الرسالة إلى حزم (blocks) طول كلّ منها 512 بت بغرض اختزالها في خطواتٍ لاحقة. من الجدير بالذكر أنّ أي تغيير مهما كان حجمه في النصّ الأصليّ يُنتج قيمة اختزال مختلفة تمامًا عن القيمة السابقة.

5f4dcc3b5aa765d61d8327deb882cf99	5f4dcc3b5aa765d61d8327deb882cf99 : password
Encrypt	Decrypt

Reverse hash decoder

Hash digest reverse lookup

Hash type	Search all types
Hash	6cb75f652a9b52798ee0e17941b2c76b

Enable mass-decrypt mode

Reverse decryption is failed. No match found. Try to search via "by all hash types" option, "Google-powered" search, or try later. Sorry... :(

d8578edf8458ce06fbc5bb76a58c5ca4	d8578edf8458ce06fbc5bb76a58c5ca4 : qwerty
Encrypt	Decrypt

✓ وجد:

5f4dcc3b5aa765d61d8327deb882cf99:password:MD5

d8578edf8458ce06fbc5bb76a58c5ca4:qwerty:MD5PLAIN

✗ متبقي:

التعرف على الهاشات ?

6cb75f652a9b52798ee0e17941b2c76b

بعد فك التشفير يتضح ان كلمات المرور المستخدمة ضعيفة حيث انها تستخدم كلمات بسيطة سهلة التخمين بطول (عدد الاحرف) صغير وجميع الأحرف المستخدمة صغيرة (Small)

ولضمان قوة كلمات المرور يجب إتباع النقاط او الملاحظات التالية معًا :

- 1- استخدام كلمات مرور طويلة (ذات عدد احرف كبير) بطول 12 حرف على الأقل
- 2- عدم استخدام كلمات مرور سهلة التخمين (مثل أسماء اشخاص او منتجات او مؤسسات)
- 3- استخدام مزيج من الاحرف الكبيرة و الصغيرة والأرقام
- 4- تعزيز قوة كلمات المرور باستخدام بعض الرموز الخاصة