

لديك مجموعة من كلمات المرور المخزنة بتنسيق مشفر. مهمتك هي فك تشفير كلمات المرور وتحليل قوتها.

مجموعة كلمات المرور (بشكل مشفر):

١. 5f4dcc3b5aa765d61d8327deb882cf99
٢. 6cb75f652a9b52798ee0e17941b2c76b
٣. d8578edf8458ce06fbc5bb76a58c5ca4

المهام:

١. قم بفك تشفير كلمات المرور المشفرة.
٢. حلل كلمات المرور المستخرجة من حيث قوتها. ما هي نقاط الضعف المحتملة؟
٣. اقترح أساليب لتحسين قوة كلمات المرور.

المهمة الأولى:

قم بفك تشفير كلمات المرور المشفرة

كلمة المرور المشفرة	كلمة المرور بعد فك التشفير
5f4dcc3b5aa765d61d8327deb882cf99	password
6cb75f652a9b52798ee0e17941b2c76b	123456
d8578edf8458ce06fbc5bb76a58c5ca4	qwerty

المهمة الثانية:

حلل كلمات المرور المستخرجة من حيث قوتها. ما هي نقاط الضعف المحتملة؟

- **كلمة المرور (password):** تعتبر هذه الكلمة من أكثر كلمات المرور شيوعاً. إن استخدام كلمة مرور بسيطة كهذه يجعلها عرضة للهجمات.
- **كلمة المرور (123456):** يعد استخدام التسلسل الرقمي من أكثر كلمات المرور شيوعاً، وهي تصدر قائمة الاستخدام عالمياً. إن استخدام كلمة مرور بسيطة كهذه يجعلها عرضة للهجمات.
- **كلمة المرور (qwerty):** تعتمد هذه الكلمة على نمط معين على لوحة المفاتيح، مما يسهل على المهاجمين تخمينها باستخدام هجمات الأنماط الشائعة.

المهمة الثالثة:

اقترح أساليب لتحسين قوة كلمات المرور.

- أ. **زيادة الطول والتعقيد**
 - ✓ استخدم كلمات مرور أطول يفضل أن تتراوح طولها بين ٩ إلى ١٦ حرفاً على الأقل.
 - ✓ أن تحتوي على الأحرف الكبيرة والصغيرة، والأرقام، والرموز الخاصة.
 - ✓ عدم استخدام كلمات معروفة أو متوقعة.
- ب. **استخدام مولدات كلمات المرور:** استخدم مولدات لإنشاء كلمات مرور قوية وعشوائية.
- ج. **تفعيل المصادقة الثنائية أو المتعددة:** تعد من التقنيات الممتازة لحماية البيانات مع تزايد التهديدات الإلكترونية.
- د. **التغيير الدوري لكلمات المرور:** الحرص على التحديث المنتظم لتغيير كلمات المرور بشكل دوري لضمان مستوى عال من الأمان.