Projektarbeit Brute-Force

1. Theorie

MD5 ist eine Hash-Funktion, die verwendet wird, um Eingaben beliebiger Längen in einen fixen 128-Bit langen Wert zu verwandeln. Dieser Wert, oft als Hashwert oder MD5-Summe bezeichnet, kann mithilfe eines Algorithmus berechnet werden, der für jede Eingabe immer das gleiche Ergebnis liefert. Die Funktion spielt eine wichtige Rolle bei der Datensicherheit, insbesondere im Zusammenhang mit Schlüsselwerten.

Die MD5-Funktion ist eine einseitige Funktion. Das bedeutet, dass es zwar relativ einfach ist, einen Hashwert aus einer Eingabe zu berechnen, die Umkehrung dieser Berechnung jedoch nicht möglich ist.

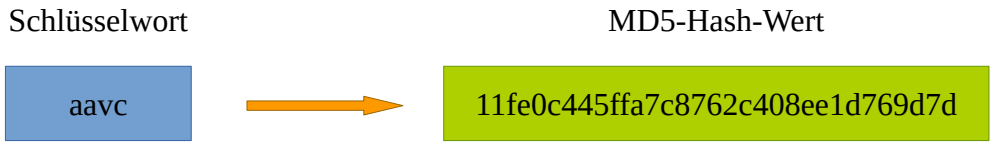
Mit anderen Worten: Wenn Sie den Hashwert einer Eingabe kennen, können Sie daraus die ursprüngliche Eingabe nicht eindeutig rekonstruieren. Es gibt keine direkte Möglichkeit, rückwärts vom Hashwert zur ursprünglichen Eingabedatei zurückzugehen. Diese Eigenschaft machen Hash-Funtkionen besonders nützlich für die sichere Speicherung von sensiblen Daten wie Passwörtern, da selbst wenn ein Angreifer den Hashwert stiehlt, er das ursprüngliche Passwort nicht wiederherstellen kann.

Es gilt jedoch zu beachten, dass MD5 inzwischen als unsicher angesehen wird und es bessere Hash-Funktionen gibt, wie z.B. SHA256. Dennoch bleibt MD5 in einigen Anwendungen noch verbreitet, weil sie einfach zu implementieren ist und eine vergleichsweise schnelle Berechnungszeit hat.

2. Auftrag

Im Rahmen eines Projekts wurden innerhalb des Unternehmens kurze Schlüsselwörter mit Gross- und Kleinbuchstaben erzeugt. Diese enthalten keine Umlaute (Beispiel: „aavc“ oder „FdUzg“).

Es kam zu einem Fehler, wodurch die Schlüsselwörter als kryptografische Hash-Werte in einer Datenbank gespeichert wurden. Dabei wurde die MD5-Hash-Funktion verwendet. Diese Funktion ist eine Einwegfunktion, d.h. aus den gehashten Werten können die ursprünglichen Schlüsselwörter nicht direkt rekonstruiert werden.



Ihr Auftrag ist es nun der Projektleitung ein Tool zu programmieren, welche die Werte herausfinden kann. Dazu sollen Sie die sogenannte Brute-Force-Methode („rohe Gewalt“) verwenden:

Die Brute-Force-Methode ist ein grundlegender Angriff auf kryptografische Systeme, bei dem alle möglichen Einträge systematisch getestet werden, bis der korrekte gefunden wird. Stellen Sie sich vor, Sie haben ein Zahlenschloss und wissen nur, dass die richtige Kombination aus drei Ziffern besteht. Bei der Brute-Force-Methode würden Sie jede mögliche Kombination aus Zahlen von 000 bis 999 versuchen, bis das Schloss aufspringt. Ihr Programm soll somit alle möglichen Schlüsselwörter mit der MD5-Hash-Funktion umwandeln und testen, ob der gleiche Wert erzeugt wird. Ist dies der Fall, so haben Sie das entsprechende Schlüsselwort gefunden.

Der Benutzer soll dabei folgende Eingaben tätigen können:

- Eingabe Hash-Wert
- Anzahl Stellen des Schlüsselwortes angeben. Dabei soll Ihr Programm bis zu 8 Stellen unterstützen.
- Ob es sich um Kleinbuchstaben oder um Klein- und Grossbuchstaben im Schlüsselwort handelt

Zudem soll Ihr Programm die Anzahl an möglichen Versuchen, je nach Eingabe des Benutzers, anzeigen. Sollte das Programm keinen Schlüssel nach einem kompletten Brute-Force-Versuch finden, soll eine entsprechende Nachricht ausgegeben werden.

3. Zusatzinformation

Für die Berechnung der Hash-Funktion können Sie die Beispiel-Datei *hash.py* beziehen. Dort wird mit der Hilfe der *hashlib*-Library MD5-Werte generiert. Beachten Sie, dass Sie diese Library in der Web-Tigerjython-Umgebung nicht vorhanden ist. Sie können jedoch die Tigerjython- oder Standart-Python-Umgebung verwenden.