

Übungsaufgabe #1: GENPW

18.11.2009

In dieser Aufgabe soll ein Passworhash nach dem folgenden Muster erzeugt werden:

```
$syssec1$gcXj981u$hWP8hUh2K+xSYWdmxK1RnQ
```

Hierbei ist `syssec1` der Bezeichner des Hashalgorithmus, `gcXj981u` ist der Salt und `hWP8hUh2K+xSYWdmxK1RnQ` der Hash.

Der Hash wird erzeugt, indem ein MD5-Hash über `<Salt><Klartextpasswort>` gebildet und das Ergebnis als BASE64 ausgegeben wird. Im Gegensatz zu dem unter aktuellen Unix-Varianten eingesetzten MD5-Hashes soll der MD5-Algorithmus allerdings nur einmal angewendet werden. Der Salt besteht aus 6 Zeichen, welche auf 8 BASE64 kodierte Zeichen abgebildet werden, der Hash besteht aus 16 Zeichen, welche in 22 BASE64-Zeichen kodiert werden.

```
$ ./genpw
Enter Password: geheim
$syssec1$3wWnBd0/$056896/DNOxrKwkgDMNv2A
```

Für die Bearbeitung der Aufgabe soll die OpenSSL-Bibliothek genutzt werden, die Zufallszahlen, MD5-Funktionen und einen BASE64-Filter bereitstellt. Die zu verwendende Programmiersprache ist C.

Die Abgabe der bearbeiteten Aufgabe erfolgt in den Übungen am 25. oder 27.11. Die Bearbeitung kann in Gruppen zu zwei Personen erfolgen.