Beleg zum Modul Informationssicherheit SS16

Liebe(r) Markus Klemm!

Die benötigten Dateien für Ihre personalisierte Aufgabenstellung finden Sie in diesem Archiv.

Entpacken Sie das Archiv (im aktuellen Verzeichnis) mit dem Kommando

```
unzip s70357.zip
```

Schreiben Sie danach ein C-Programm, das die folgenden Aufgaben 1. bis 4. für Sie erledigt. Beschränken Sie sich auf eine Quelltextdatei s70357.c. Bei der Formatierung des Quelltextes orientieren Sie sich bitte am Linux kernel coding style.

1. Entschlüsseln Sie das Chiffrat s70357-src-cipher.bin mit Hilfe des gestörten Schlüssels s70357-corrupt-src-key.bin. Falls ein Initialisierungsvektor nötig ist, so ist dieser im Anschluss an den Schlüssel in dieser Datei abgelegt. Der Klartext wurde mittels des Verfahrens 2K-3DES-EDE-CBC verschlüsselt. (Der Typ des Verfahrens wird übrigens durch die Funktion EVP_des_ede_cbc() der OpenSSL-Bibliothek implementiert). Das Byte Nummer 11 (gezählt ab 0) des Schlüssels wurde 'versehentlich' auf 0 gesetzt. Der Klartext ist ein Dokument im PDF.
2. Bilden Sie einen kryptografischen Hash über dem entschlüsselten Klartext. Nutzen Sie das Verfahren DSS, das durch die Funktion EVP_dss() der OpenSSL-Bibliothek implementiert wird.
3. Verschlüsseln Sie den Hash mittels des Verfahrens DES-ECB und dem Schlüssel s70357-dest-key.bin und speichern Sie das Chiffrat in der Datei s70357-dest-cipher.bin. (Der Typ des Verfahrens wird durch die Funktion EVP_des_ecb() in der OpenSSL-Bibliothek implementiert).
4. Senden Sie die Dateien s70357-dest-cipher.bin und s70357.c als Attachment per Mail an robert.baumgartl@htw-dresden.de. Bitte schreiben Sie '[IS] Beleg sxxxxx' in das Subject der Mail.

Letztmöglicher Einreichungstermin ist der 1.7.2016, 23:59:59 CEST (UTC+2).

Viel Spaß!