



Falko Dressler Tobias Limmer

Netzwerksicherheit WS 2007/08

3. Übungsblatt

20.11.2007

Symmetrische Verschlüsselungsalgorithmen können auf verschiedene Arten auf Daten angewendet werden. In dieser Aufgabe werden Sie verschiedene Betriebsmodi von kryptographischen Algorithmen programmieren. Dazu wird Ihnen von uns eine Funktion für die blockweise symmetrische Verschlüsselung zur Verfügung gestellt.

Auf der Webseite der Vorlesung finden Sie die Dateien `netsec_des.(c|h)`, welche die Funktion `netsec_des_crypt` bereitstellen. Diese Funktion verschlüsselt jeweils 8-Byte-Blöcke mit Hilfe des DES Algorithmus.

Ihre Aufgabe ist nun, die Betriebsmodi ECB, CBC, CFB und OFB auf Basis dieser Funktion zu implementieren. Folgende Punkte gibt es dabei zu beachten:

- Alle Werte werden in der Little-Endian Bytereihenfolge gespeichert. Falls Sie auf i386 Rechnern arbeiten, müssen Sie sich also nicht um Bytekonvertierung kümmern.
- Bei blockweise operierenden Betriebsmodi müssen Quelldaten eventuell mit zufälligen Zeichen aufgefüllt werden, falls der letzte Block nicht komplett gefüllt ist.
- Die ursprüngliche Länge kann bei blockweise operierenden Betriebsmodi nach der Verschlüsselung nicht mehr festgestellt werden. Deswegen wird dem unverschlüsselten Text *immer* ein 4 Byte `unsigned int` vorangestellt, welcher die Anzahl der Bytes der Quelldaten enthält. Die Länge und die Quelldaten werden nun gemeinsam verschlüsselt. Somit ist der verschlüsselte Text mindestens um 4 Byte länger als der Quelltext.
- Stromchiffrierende Betriebsmodi werden byteweise auf Daten angewendet.
- Als Grundlage für die Programmierung der Betriebsmodi können die Folien der Vorlesung verwendet werden. Bei Stromchiffren wird auf das Shift-Register die „shift left“-Operation angewendet.
- Achten Sie auf Buffer Overflows!

Aufgabenstellung:

1. Programmieren Sie in einem ersten Schritt alle Betriebsmodi und testen Sie sie. Stellen Sie dazu ein kleines Skript bereit, das nacheinander in jedem Betriebsmodus einen Text verschlüsselt und danach wieder entschlüsselt. Es muss dabei sichtbar sein, dass der Text wieder erfolgreich entschlüsselt wurde.
2. Auf der Webseite der Vorlesung befinden sich zwei verschlüsselte Dateien mit den Namen `blockcipher(1|2).enc`. Diese wurden mit dem Schlüssel 12345 und, falls benötigt, dem Initialisierungsvektor ABCDEFGH verschlüsselt. Entschlüsseln Sie diese Texte in dem in der vorigen Aufgabe erstellten Skript.

Technische Hinweise:

- Die Aufgaben sind in C/C++ zu erstellen.
- Der Code muss auf dem Betriebssystem Debian/Linux im CIP-Pool der Informatik mit der dort installierten Version des GNU C/C++-Compilers kompilieren und lauffähig sein.
- Es ist ein Makefile oder ein ausführbares Skript zu bereitzustellen, welches temporäre Daten löschen (Target „clean“) und eine Binärdatei (Target „all“) erstellen kann.
- Es ist eine Dokumentation im ASCII-Format zu erstellen, welche einen typischen Programmstart dokumentiert und über Besonderheiten des Programms berichtet.
- Bei Kompilierung/Linkvorgang des Programms muss die OpenSSL-Bibliothek eingebunden werden. Dazu muss gcc der Parameter `-lssl` übergeben werden.

Abgabe der Lösungen per Mail an `tobias.limmer@informatik.uni-erlangen.de` bis Montag, den 26.11.2007 als *Archiv* im Format `.tar.(gz|bz2)` oder `.zip`. Als Betreff der Mail `Netsec Übung 3, Gruppe X` angeben.