Prüfungsvorleistung zum Modul Informationssicherheit

Hallo Gabriel Kai Pechstein!

Schreiben Sie bitte ein C-Programm, das die unten folgende Aufgabe für Sie erledigt. Die dafür benötigten Dateien finden Sie hier. Bitte beschränken Sie sich auf eine Quelltextdatei s88752.c. Ihr Programm soll Zwischenergebnisse im Arbeitsspeicher halten. Es darf zur Lösung der Aufgabe keine eigenen Zwischenergebnisse aus Dateien lesen. Bei der Formatierung des Quelltextes orientieren Sie sich bitte am Linux kernel coding style, den ich hier für Sie in deutscher Sprache zusammengefasst habe. Die Aufgabenstellung wurde gestestet mit dem openssl-Paket, das im dritten Praktikum übersetzt wurde (siehe ~westfeld/30-isprak).

Aufgabe

1. Entschlüsseln Sie bitte zunächst jeweils die Daten in den Dateien s88752-cipher1.bin und s88752-cipher2.bin. Beide Dateien wurden mit dem gleichen Verfahren verschlüsselt. Der Typ dieses Verfahrens CAMELLIA-192-CFB wird von der Funktion EVP_camellia_192_cfb128( ) in libcrypto zurückgegeben. Die Länge der benötigten Parameter können Sie mit den Funktionen EVP_CIPHER_key_length( ) und EVP_CIPHER_iv_length( ) aus dem Typ ermitteln. Der Schlüssel und danach ggf. der Initialisierungsvektor liegen, unmittelbar aufeinanderfolgend, in der Datei s88752-key1.bin vor.
2. Zu einem der beiden Klartexte passt die digitale Signatur in der Datei s88752-sig.bin. Die digitale Signatur basiert auf dem Hashverfahren SHA3-512, dessen Typ die Funktion EVP_sha3_512( ) zurückgibt. Prüfen Sie bitte mit dem Signaturprüfschlüssel aus der Datei dsapub.pem, zu welchem der Klartexte die Signatur passt. Verwerfen Sie die Daten der anderen Datei, zu denen sie nicht passt.
3. Am Anfang der entschlüsselten Daten (Klartext) finden Sie einen Text, der, einem Beispiel von Joachim Ringelnatz folgend, festlich angepasst wurde — leider für das falsche Fest (Ostern). Deshalb machen Sie diese Anpassung bitte rückgängig. Der angepasste Text endet mit einem Nullzeichen ('\0'), der Klartext endet dort jedoch nicht. Lassen Sie bitte den übrigen Klartext unverändert. Zusammen werden der angepasste Text und die unveränderten Daten im Folgenden *bereinigte Daten* genannt.
4. Verschlüsseln Sie bitte die bereinigten Daten mit dem Verfahren AES-128-OFB. Der Typ des Verfahrens wird von der Funktion EVP_aes_128_ofb( ) in libcrypto zurückgegeben. Der Schlüssel und ggf. der Initialisierungsvektor liegen, unmittelbar aufeinanderfolgend, in der Datei s88752-key2.bin vor. Speichern Sie bitte das von Ihnen erzeugte Chiffrat in einer Datei namens s88752-result.bin.

Senden Sie eine E-Mail an andreas.westfeld@htw-dresden.de (am besten den elektronischen Verweis nutzen)

- mit dem Betreff »Einreichung IS-Beleg«,
- (mindestens) der Zeile »s88752 Gabriel Kai Pechstein«,
- Ihrem Quelltext s88752.c und
- der Datei s88752-result.bin als Anlage

(bitte *nicht* als zip o. ä. verpacken und *nicht* mit PGP/GPG verschlüsseln; S/MIME-Verschlüsselung ist zulässig).

Spätester Termin für die Abgabe ist im Zweifel **Montag, der 20. Januar 2025, 24 Uhr (MEZ)**.

Ständig aktualisierte Hinweise/Antworten zu dieser Prüfungsvorleistung finden Sie hier.

Andreas Westfeld