Aufgabenblatt 3
Sicherheit digitaler Systeme

Institut: Berliner Hochschule für Technik
Dozent: Prof. Dr. Christian Forler
Url: `https://lms.bht-berlin.de/`
Email: `cforler(at)bht-berlin.de`
Wintersemester 23/24

Aufgabe 1 AES

a) Vor der ersten Runde wird bei AES einmal die Operation AddRoundKey ausgeführt. Warum wird dieses gemacht?

b) In jeder Runde werden die Operationen ShiftRows und MixColumns hintereinander ausgeführt. Wird die Sicherheit von AES beeinflusst, wenn man die Reihenfolge dieser beiden Operationen in jeder Runde vertauscht?

Aufgabe 2 Improved Encryption Standard (IES)
Prof. Dr. Schar Latan hat eine neue Blockchiffre *Improved Encryption Standard* (IES) veröffentlicht. Dabei handelt es sich um eine modifizierte Variante des AES, bei dem die Operation ShiftRows durch MixColumns ersetzt wurde. D.h. eine Runde IES ist die Ausführung der folgenden vier Operationen hintereinander:

1) **SubBytes**, 2) **MixColumns**, 3) **MixColumns** und 4) **AddRoundKey**.

Ist der IES sicher? Begründen sie ihre Antwort.

Aufgabe 3 Reduzierter AES
Eine AES-Runde besteht aus einer Sequenz von vier Basisoperationen:

1) **SubBytes**, 2) **ShiftRows**, 3) **MixColumns** und 4) **AddRoundKey**.

Jede dieser Operationen ist essentiell für die Sicherheit des AES. Die folgende Aufgabe demonstriert die Unsicherheit des AES, sobald eine dieser Operationen fehlt. Seien zwei Klartexte $P, P' \in \{0,1\}^{128}$ gegeben:

$$P = \texttt{000102030405060708090a0b0c0d0e0f},$$
$$P' = \texttt{010102030405060708090a0b0c0d0e0f}.$$

Beide wurden mit je drei verschiedenen Versionen des AES verschlüsselt:

1. Einmal mit einer AES-Version, bei der MixColumns fehlte;
2. Einmal mit einer AES-Version, bei der ShiftRows fehlte, und
3. Einmal mit einer vollständigen AES-Version.

Es gilt stets: C ist die Verschlüsselung von P und C' die Verschlüsselung von P'. Ordnen Sie zu, welches der Chiffretext-Paare C, C' mit welcher AES-Version erstellt wurde. Begründen Sie Ihre Antworten.

Paar 1:

$$C = \texttt{2b45b04bce63e0c1e750ca0c876248a9},$$
$$C' = \texttt{b6012b6ece63e0c1e750ca0c876248a9}$$

Paar 2:

$$C = \texttt{231446982181c5ca6476f957632cbd2a},$$
$$C' = \texttt{bbac089c1cc8ff7e83f147177b488316}$$

Paar 3:

$$C = \texttt{ceee58e9437269400fc7e2466b25564c},$$
$$C' = \texttt{b7ee58e9437269400fc7e2466b25564c}.$$

Aufgabe 4 Betriebsmodi: Verschlüsselung
Sei E eine Blockchiffre mit der Blocklänge 3 Bit. Der Schlüssel K sei bekannt und es gilt:

$$\begin{array}{ll} E_K(0) = 2, & E_K(4) = 1 \\ E_K(1) = 0, & E_K(5) = 4 \\ E_K(2) = 5, & E_K(6) = 3 \\ E_K(3) = 7, & E_K(7) = 6 \end{array}$$

Verschlüsseln Sie den Klartext $(2, 4, 3, 2)$

a) im Electronic Codebook Mode (ECB),

b) im Cipher Block Chaining Mode (CBC) mit Initialwert 4,

c) im Counter Mode (Ctr) mit dem Startwert $R = 6$

Aufgabe 5 Betriebsmodi: Entschlüsselung
Sei E eine Blockchiffre mit der Blocklänge 4 Bit mit $E_K(M) = (M+K) \bmod 16$. Entschlüsseln Sie den Chiffretext $(2, 4, 3, 2)$ unter dem Schlüssel 13

a) im Electronic Codebook Mode (ECB),

b) im Cipher Block Chaining Mode (CBC)

c) im Counter Mode (Ctr)

Aufgabe 6 CTR und CBC
Alice kodiert die Nachricht $M =$ "`Zahle Bob EUR100`" in 8-Bit-ASCII
(siehe `http://en.wikipedia.org/wiki/ASCII`)
und verschlüsselt sie mit zufälligem Startwert R mit AES im Counter-Mode. Die Hexadezimalrepräsentation von M und dem zugehörigen Chiffretext (R, C_1) sind:

$$M = \texttt{5A61686C6520426F6220455552313030},$$
$$R = \texttt{31323334353637383132333435363738},$$
$$C_1 = \texttt{05F7B0E285CB10CAFC541B4515FB5C50}.$$

a) Was ist der Chiffretext zur Nachricht M' = "`Zahle Eve EUR500`"? Begründen Sie kurz Ihre Antwort.

b) Mit AES-CBC und dem Initialwert C_0 ist der zu M gehörende Chiffretext (C_0, C_1) nun:

$$C_0 = \texttt{31323334353637383132333435363738},$$
$$C_1 = \texttt{9D8CB470BA3F6AA12B693B271E3F59B4}.$$

Was ist der Chiffretext zur Nachricht M' = "`Zahle Eve EUR500`"? Begründen Sie kurz Ihre Antwort.

Dies zeigt, dass Counter-Mode und CBC nicht die Integrität von Nachrichten garantieren können.

Aufgabe 7 Sichere MACs
Sei $E_K(.)$ eine sichere n-bit Blockchiffre und $M = M_1, \ldots M_\ell$ mit $|M_i| = n$ Sind die folgenden MACs sicher? Begründen Sie ihre Antwort.

a) $MAC_K(M) = E_K\left(\bigoplus_{i=1}^{\ell} M_i\right)$

b) $MAC_K(M) = \bigoplus_{i=1}^{\ell} E_K(M_i)$

c) $MAC_K(M) = \bigoplus_{i=1}^{\ell} (E_K(i \oplus M_i))$

Aufgabe 8 Sicherheit von Hashfunktionen
Sei $F : \{0,1\}^* \to \{0,1\}^n$ eine sichere Hashfunktion und $G : \{0,1\}^* \to \{0,1\}^n$ eine Hashfunktion welche nicht kollisionsresistent ist. Ist die Hashfunktion $H : \{0,1\}^* \to \{0,1\}^n$ mit $H(x) := F(G(x))$ sicher? Begründen Sie Ihre Antwort.

Aufgabe 9 Verschlüsselte Dateiübertragung v2 (16 Punkte)

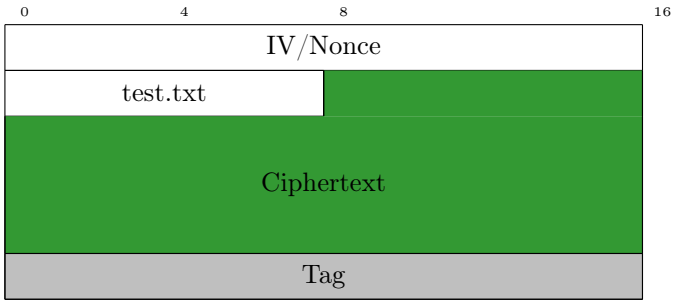
Modifizieren Sie den Client und Server aus dem vorherigen Übungsaufgabenblatt so, dass mit dem AE-Scheme POET verschlüsselte Dateien übertragen werden. Der Server soll die Dateien entschlüsseln und den Tag (kryptographische Prüfsumme) verifizieren. Die Associated Data (AD, Header) soll aus einem zufälligen 128-Bit Initial Vector (IV) und dem Dateinamen bestehen. Verwenden Sie bei ihrer Implementation den folgenden Schlüssel

```
1 byte_t key[KEYLEN] =
    {0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15};
```

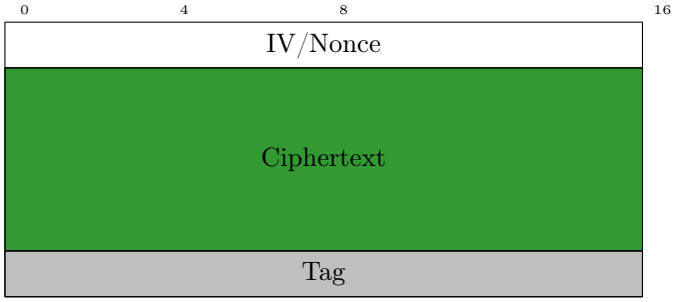
Gehen Sie wie folgt vor.

- Laden Sie die Dateien `aes.h, aes.c poet.h` und `poet.c` aus dem Moodelkurs herunter.
- Passen Sie ihr Makefile an.
- Client

- Initialisierung von POET mit dem vorgegebenen Schlüssel.
- Verarbeitung des Headers der aus einem zufälligen IV (128-Bit) und dem Dateinamen der zu übertragenen Datei besteht. *(Hinweis: Zufallsbytes können mit dem Systemcall* `getrandom()` *generiert werden).*
- Senden Sie den Header an den Server.
- Verschlüsseln sie die einzelnen Klartextblöcke der Datei und übertragen Sie die zugehörigen Chiffretextblöcke an den Server.
- Generieren Sie den Tag und den finalen Chiffretextblock und übertragen Sie beides an den Server.
- Visualisierung der zu übertragenen Daten für die Datei `test.txt`. Die Einheit ist Bytes.



- Server
  - Empfangen Sie den Header.
  - Zerlegen Sie Header in IV und Dateiname.
  - Legen Sie eine Datei mit dem Dateinamen under der zusätzlichen Endung `.enc` an.
  - Schreiben Sie den IV in diese Datei.
  - Schreiben Sie die empfangenen Chiffretextblöcke und Tag in die Datei.
  - Visualisierung des Inhaltes der verschlüsselten Datei `test.txt.enc` in Bytes.



  - Entschlüsseln Sie die Datei mit POET.
  - Löschen Sie die Chiffretextdatei mit der Endung `.enc`.

  - Löschen Sie die Klartext Datei falls deren Entschlüsslung nicht erfolgreich war, d. h. wenn die Verifikation des Tags nicht erfolgreich war.

- Testen Sie ihre Implementation ausgiebig. Wenn Sie alles richtig gemacht haben, dann sollte eine unbedarfte Benutzer:in keinen Unterschied zu der Client-Server-Version ohne Verschlüsselung feststellen können.

(*Hinweis: Sie können mit dem Netzwerk-Sniffer Wireshark (*`https://www.wireshark.org`*) sicherstellen, dass die Daten verschlüsselt übertragen werden.*)
Diese Lösung ist natürlich noch nicht praxistauglich, da ein hardkodierter Schlüssel verwendet wird. Aber immerhin wird bei der Übertragung die Vertraulichkeit und Integrität der Daten geschützt. Dies Lösung ist schon sehr viel besser als eine Lösung ohne Transportverschlüsselung.