XTEA

Gruppe 109 – Aufgabe A502

Liming Kuang Yaxuan Chen Feng Hu

25.08.2022

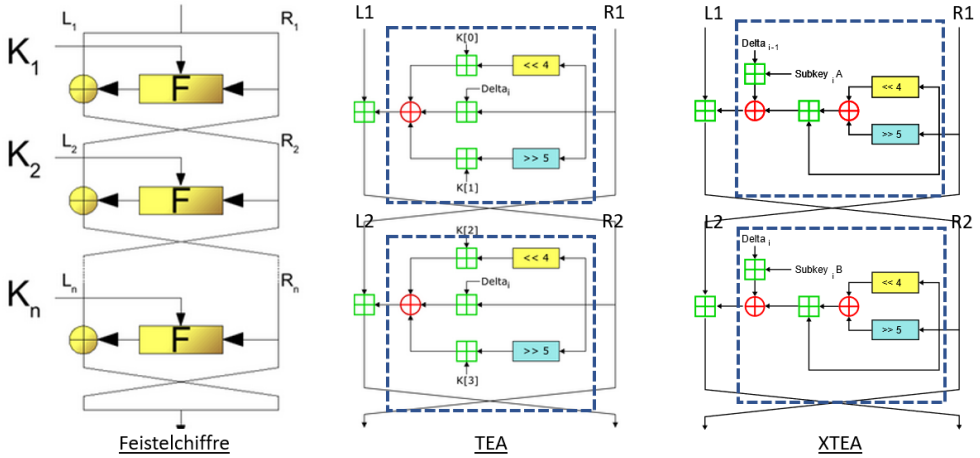
Agenda

Aufbau einer Feistelchiffre

- Blockverschlüsselung mit einer bestimmten Blocklänge, z. B. 64-Bit
- Ein Block wird in zwei (meist gleich große) Teile geteilt und in n aufeinanderfolgenden Runden verarbeitet
- Rundenfunktion
- umkehrbare Verknüpfung, oft verwendet *XOR*

Strukturvergleich

Feistelchiffre vs. *TEA* vs. *XTEA*



Padding auf Blocklänge

Padding Verfahren: z. B. *PKCS#7*

- Padding muss **immer** gemacht werden, d. h. mindestens ein Padding-Byte
- Wert des Padding-Byte = Anzahl der aufzufüllenden Bytes
- Wenn die Länge des Klartextes bereits ein Vielfaches der Blocklänge ist, müssen auch 8 Padding-Bytes hinzugefügt werden

Verarbeitung mehrerer Blöcke

- ECB (**E**lectronic **C**ode **B**ook Mode): Jeder Block wird unabhängig verschlüsselt.
- CBC (**C**ipher **B**lock **C**haining Mode): Jeder Geheimtextblock fließt in den nächsten ein und für den ersten Block wird ein Initialisierungsvektor (IV) benötigt.

Test Methodologie

- **Test Pyramid**
  - End-to-End Test
  - Service Test
  - Unit Test
- In unseren Tests wurde eine vereinfachte Version ohne Service Test verwendet

End-to-End Test

- Bash Skript – einfache Batch-Verarbeitung von umfangreichen Benutzereingaben
- 5 Tests insgesamt:
  - 4 Tests für normale Eingaben
  - Ein umfangreicher Test der Fehlerhandlung, der 11 verschiedene Fehleingaben enthält
- Beispiele der Fehleingaben:
  - Fehlende Eingabedatei.
  - Falsches Format von Schlüssel/IV-Eingabe. (z. B.: -k a,12,345,b; -k 1,2,3)
  - Falsche Rheinfolge der Optionen und ungültige Option.(z. B.: -o steht vor -V/-B; –not-an-option; -x;)

Unit Test

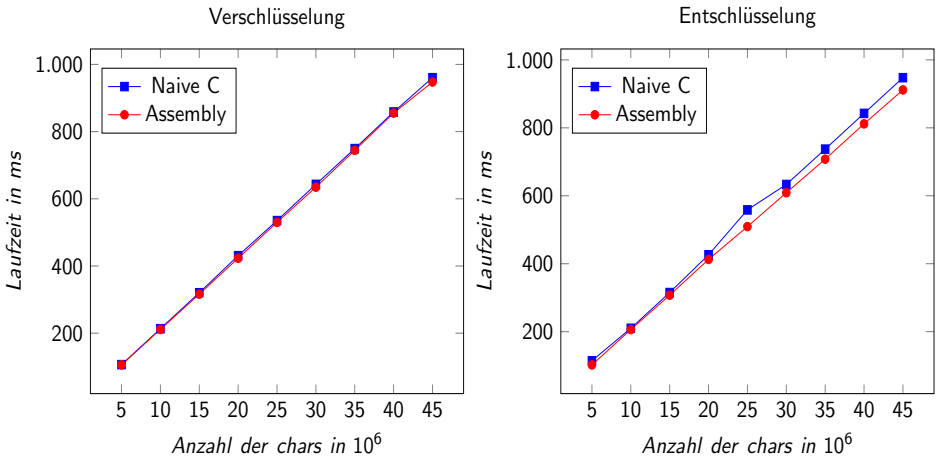
- C-Programm, mit *assert ()* realisiert
- Relativ isolierte Tests, mit denen die Korrektheit jeder einzelnen Funktionsimplementierung verifiziert wurde
- 9 wichtigsten c-Funktionen wurden getestet
- Die grundlegende funktionale Korrektheit jeder Funktion wird getestet.
- Zusätzlich noch 14 Rand-/Sonderfälle, z. B.:
  - wie *xtea_encrypt ()* Funktion paddet, wenn die Länge der Eingabe kleiner als die Blocklänge ist.
  - maximale/minimale Eingabedaten für *xtea_encrypt_block ()* Funktion

Laufzeitanalyse

- GNU Profiler
  - **-pg**
  - **-gropf**
- Verschlüsselung *xtea_encrypt_block ()* und Hex-codierung *binary_to_hex ()*.
  - CBC Zeitaufwand
- Zeitmessung
  - *clock_gettime (CLOCK_MONOTONIC, struct timespec * res)*

Vergleich

Naive C Implementierung vs. Assemblerimplementierung



Vergleich

Naive C Implementierung vs. C Implementierung mit Lookup-Tabelle