IT-Sec Tutorstunde 3

Carl Koenig, Fabian Specht

Vorstellung Hausaufgaben

- (8) More Injection!
- (9) Textbook-RSA Issues
- (10) More RSA

(1a) Betriebsmodi

- Warum brauchen wir die ueberhaupt?

(1a) Betriebsmodi

- Warum brauchen wir die ueberhaupt?
  - lange Daten $\rightarrow$ mehrere Bloecke

(1a) Betriebsmodi

- Warum brauchen wir die ueberhaupt?
  - lange Daten $\rightarrow$ mehrere Bloecke
  - praktische Verknuepfung ist Aufgabe des Betriebsmodus

(1a) Betriebsmodi

- Warum brauchen wir die ueberhaupt?
  - lange Daten $\rightarrow$ mehrere Bloecke
  - praktische Verknuepfung ist Aufgabe des Betriebsmodus
- Beispiele

(1a) Betriebsmodi

- Warum brauchen wir die ueberhaupt?
  - lange Daten $\rightarrow$ mehrere Bloecke
  - praktische Verknuepfung ist Aufgabe des Betriebsmodus
- Beispiele
  - **E**lectronic **C**ode **B**ook

(1a) Betriebsmodi

- Warum brauchen wir die ueberhaupt?
  - lange Daten $\rightarrow$ mehrere Bloecke
  - praktische Verknuepfung ist Aufgabe des Betriebsmodus
- Beispiele
  - **E**lectronic **C**ode **B**ook
  - **C**ipher **B**lock **C**haining

(1a) Betriebsmodi

- Warum brauchen wir die ueberhaupt?
  - lange Daten $\rightarrow$ mehrere Bloecke
  - praktische Verknuepfung ist Aufgabe des Betriebsmodus
- Beispiele
  - **E**lectronic **C**ode **B**ook
  - **C**ipher **B**lock **C**haining
  - **C**oun**T**e**R**

(1b) drawing time

- Skizzen fuer ECB, CBC und CTR

(1b) drawing time

- Skizzen fuer ECB, CBC und CTR
- sehr wahrscheinlich Teil der Klausur!

(1) ECB

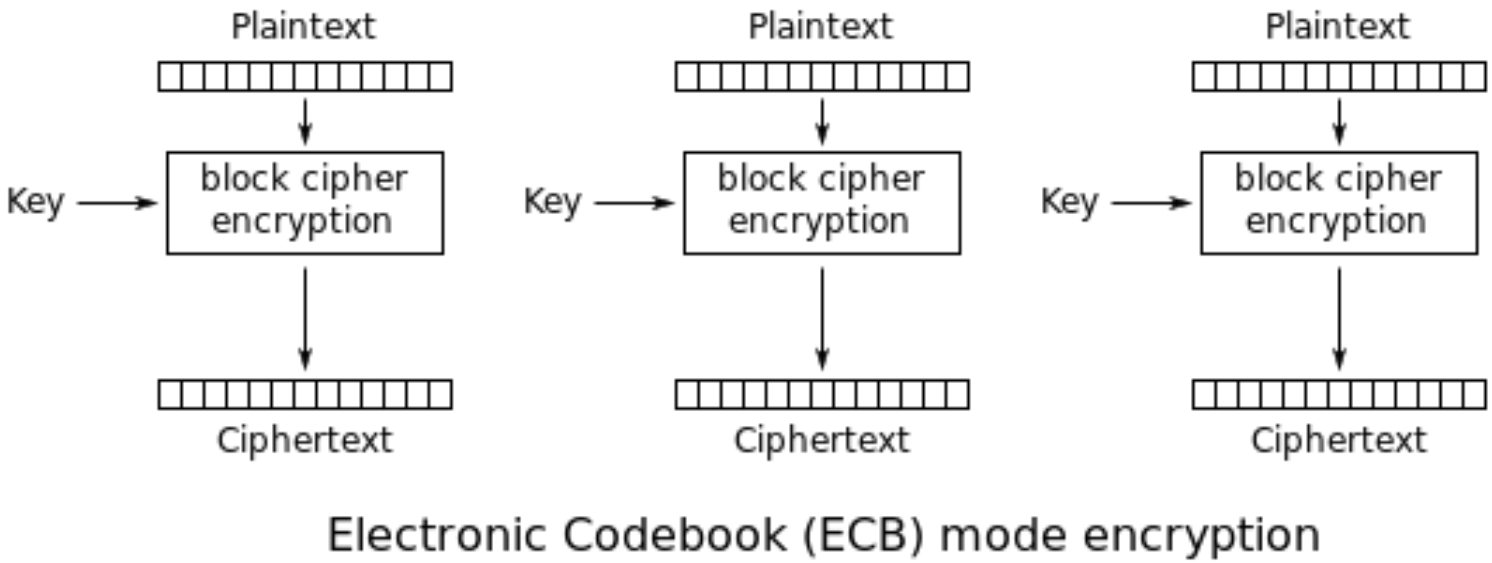


Figure 1: ECB Verschluesselung [1]

[1] https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

(1b) ECB

- Eigenschaften

(1b) ECB

- Eigenschaften
  - Muster erkennbar

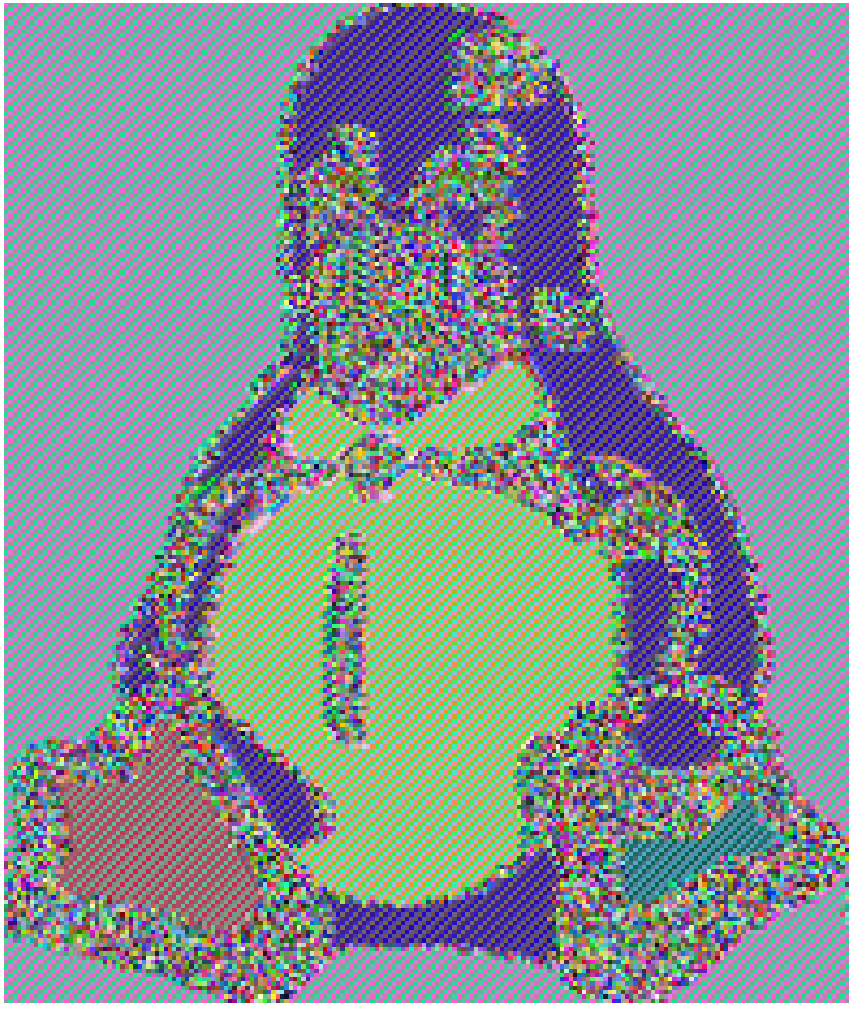
(1b) ECB

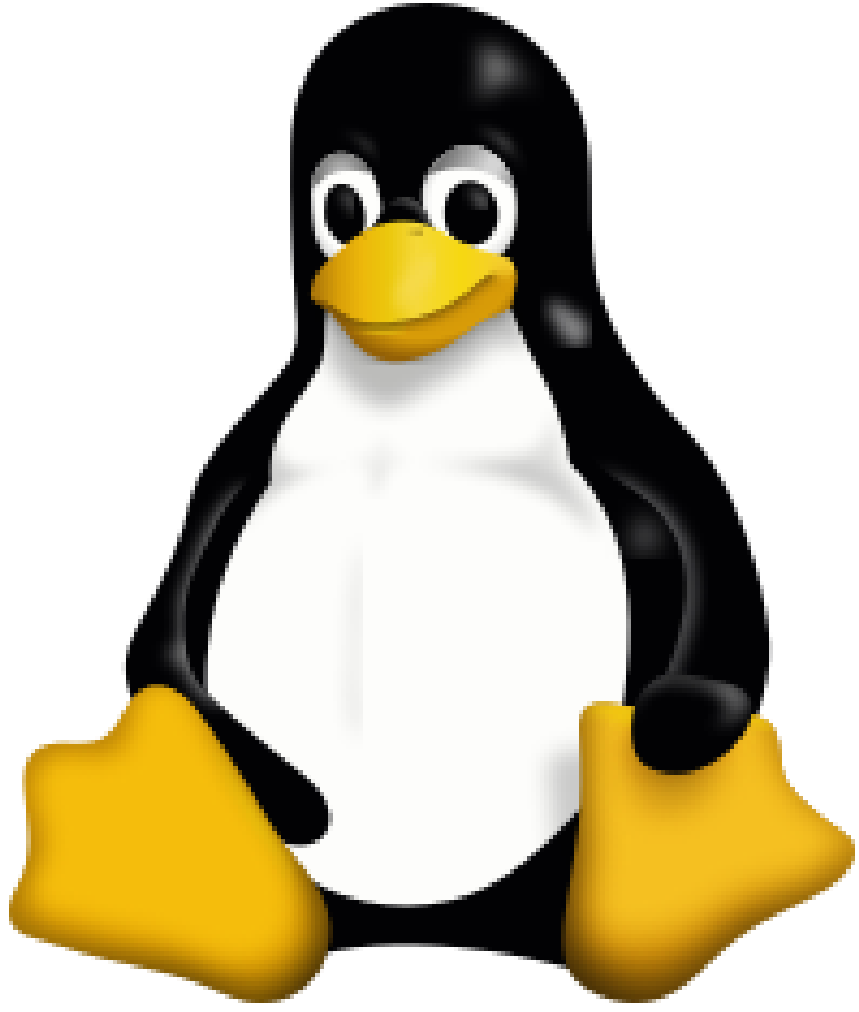
- Eigenschaften
  - Muster erkennbar
  - Bloecke sind leicht austauschbar

(1b) ECB

- Eigenschaften
  - Muster erkennbar
  - Bloecke sind leicht austauschbar
  - leicht parallelisierbar

(1b) ECB - Muster





(1b) CBC

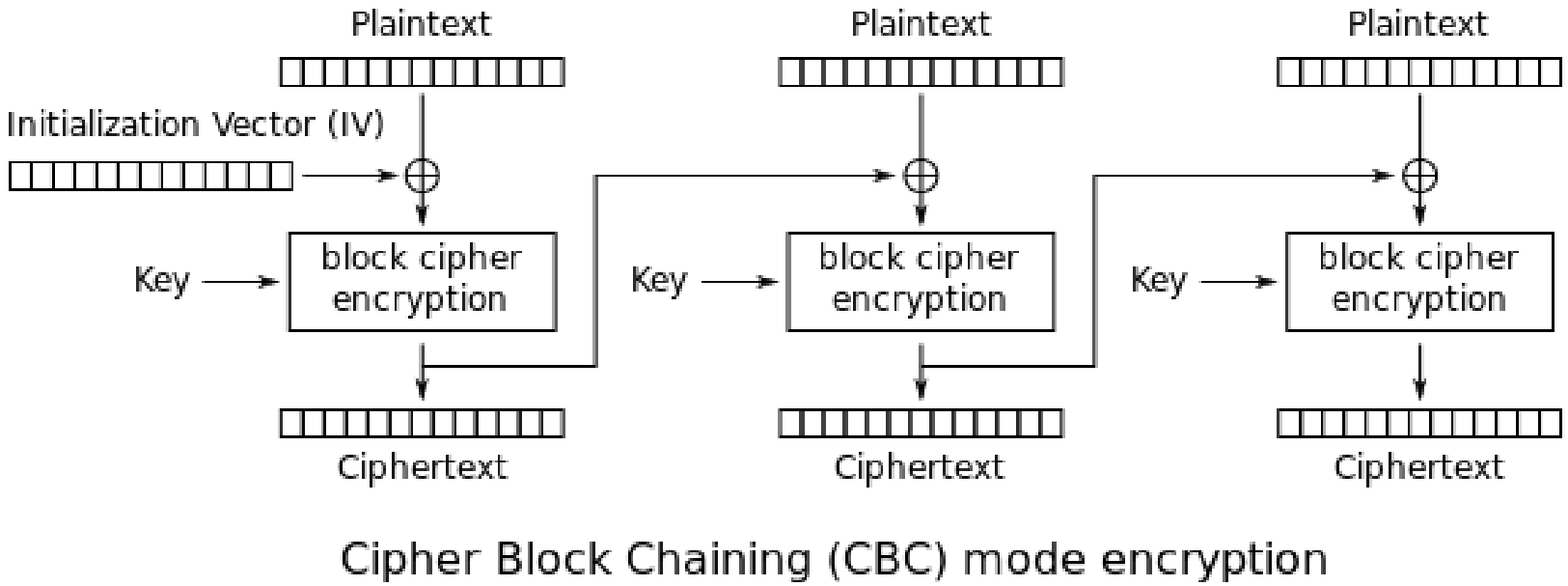


Figure 2: CBC Verschluesselung [2]

[2] https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

(1b) CBC

- Eigenschaften

(1b) CBC

- Eigenschaften
  - kein Muster mehr erkennbar, da jeder Block vom vorherigen Ciphertextblock abhaengt

(1b) CBC

- Eigenschaften
  - kein Muster mehr erkennbar, da jeder Block vom vorherigen Ciphertextblock abhaengt
  - nicht parallelisierbar

(1b) CTR

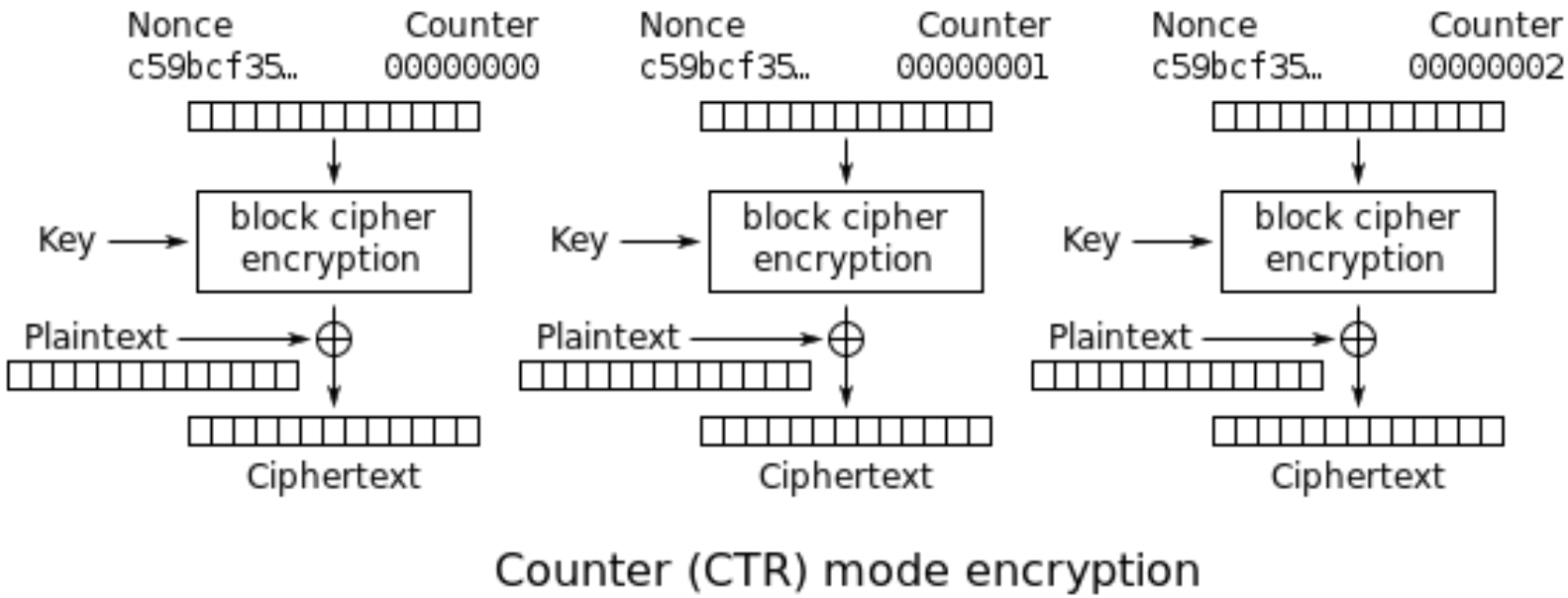


Figure 3: CTR Verschluesselung [3]

[3] https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

(1b) CTR

- Eigenschaften

(1b) CTR

- Eigenschaften
  - praktisch Stromchiffre

(1b) CTR

- Eigenschaften
  - praktisch Stromchiffre
  - nicht parallelisierbar

(2) WEP

- Algo in aelteren WLAN-Standards

(2) WEP

- Algo in aelteren WLAN-Standards
- verwendet Stromchiffre RC4

(2) WEP

- Algo in aelteren WLAN-Standards
- verwendet Stromchiffre RC4
- 24 Bit IV, symm. Schluessel

(2) WEP

- Algo in aelteren WLAN-Standards
- verwendet Stromchiffre RC4
- 24 Bit IV, symm. Schluessel
- IV wird oft wiederverwendet

(2a) WEP

- Welche Folgen hat es, wenn ein IV doppelt verwendet wird?

(2a) WEP

- Welche Folgen hat es, wenn ein IV doppelt verwendet wird?
  - K ist statisch (WLAN-Passwort)

(2a) WEP

- Welche Folgen hat es, wenn ein IV doppelt verwendet wird?
  - K ist statisch (WLAN-Passwort)
  - gleicher Schluesselstrom fuer mehrere Pakete

(2b) WEP

- Welchen Angriff ermoeglicht das, wenn wir M_2 kennen? (Reminder: an Whiteboard schreiben)

(3) PKCS#7

```
01 -- if l mod k = k-1
02 02 -- if l mod k = k-2
.
.
.
k k ... k k -- if l mod k = 0
```

Figure 4: PKCS#7

Beispiele

- AES ($k = 16$ Byte)

Beispiele

- AES (k = 16 Byte)
- “Foobar”

Beispiele

- AES (k = 16 Byte)
- “Foobar”
- “Das ist ein Test”

CBC Entschluesselung

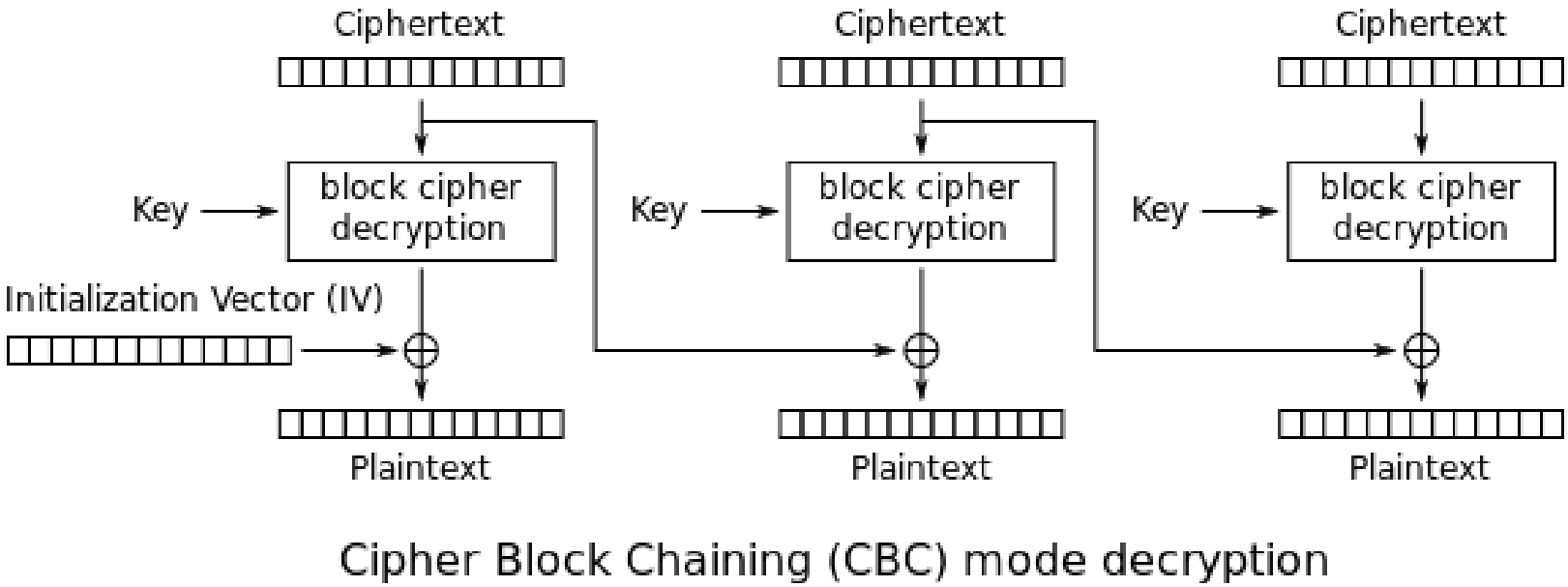


Figure 5: CBC Entschluesselung [4]

[4] https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Padding Oracle

Figure 6: Padding Oracle Scetch [5]

[5] Credit: Nguyet Ha Nguyenová