

# IT-Security Tutorübung 03

---

Dorian Zedler

6. November 2023

Technische Universität München

Quizizz / Aufgabe 1

Hausaufgaben Präsentationen

Aufgaben

## Quizizz / Aufgabe 1

---

<https://quizizz.com/admin/quiz/654614409bd71e643ca04ee6>

# Hausaufgaben Präsentationen

---

# Aufgaben

---

## Aufgabe 2a - Kryptoanalyse vs. Kryptografie

a) Was ist der Unterschied zwischen *Kryptografie* und *Kryptoanalyse*?

## Aufgabe 2a - Kryptoanalyse vs. Kryptografie

- a) Was ist der Unterschied zwischen *Kryptografie* und *Kryptoanalyse*?
- **Kryptografie** ist die Wissenschaft der *Entwicklung* sicherer Ver- und Entschlüsselungsverfahren



## Aufgabe 2a - Kryptoanalyse vs. Kryptografie

- a) Was ist der Unterschied zwischen *Kryptografie* und *Kryptoanalyse*?
- **Kryptografie** ist die Wissenschaft der *Entwicklung* sicherer Ver- und Entschlüsselungsverfahren
  - **Kryptoanalyse** ist die Wissenschaft der *Analyse* und des *Brechens* von Ver- und Entschlüsselungsverfahren

## Aufgabe 2b - symmetrisch vs. asymmetrisch

- b) Was ist der zentrale Unterschied zwischen *asymmetrischen* und *symmetrischen* Verschlüsselungsverfahren?

## Aufgabe 2b - symmetrisch vs. asymmetrisch

- b) Was ist der zentrale Unterschied zwischen *asymmetrischen* und *symmetrischen* Verschlüsselungsverfahren?
- **Symmetrische** Verschlüsselung verwendet *den gleichen Schlüssel* zum Ver- und Entschlüsseln
    - dieser wird *geheim* gehalten
    - jeder im Besitz des Schlüssels kann verschlüsseln und entschlüsseln

b) Was ist der zentrale Unterschied zwischen *asymmetrischen* und *symmetrischen* Verschlüsselungsverfahren?

- **Symmetrische** Verschlüsselung verwendet *den gleichen Schlüssel* zum Ver- und Entschlüsseln
  - dieser wird *geheim* gehalten
  - jeder im Besitz des Schlüssels kann verschlüsseln und entschlüsseln
- **Asymmetrische** Verschlüsselung verwendet *unterschiedliche Schlüssel* zum Ver- und Entschlüsseln
  - einer davon wird *geheim* gehalten, der andere *veröffentlicht*
  - jeder kann verschlüsseln, nur der Empfänger kann entschlüsseln

## Aufgabe 2c - Kerckhoffs Prinzip

c) Was ist Kerckhoffs Prinzip und warum ist es sinnvoll es zu befolgen?

- c) Was ist Kerckhoffs Prinzip und warum ist es sinnvoll es zu befolgen?
- Die Sicherheit eines Verschlüsselungsverfahrens darf nur von der Geheimhaltung des Schlüssels abhängen
  - Wenn die Sicherheit von der Geheimhaltung des Verfahrens abhängt, wird das Verfahren in der Praxis früher oder später bekannt und damit nutzlos
  - Das Verfahren muss öffentlich bekannt und trotzdem sicher sein  
→ **Kein Security by Obscurity!**

## Aufgabe 2d - Brute-Force bei DES

- d) Der Schlüsselraum bei DES beträgt  $2^{56}$ . Wie lange würde ein Angreifer für einen Brute-Force-Angriff mit einer handelsüblichen CPU brauchen? Verwenden Sie als Berechnungsgrundlage eine CPU mit 3GHz (3 GHz bedeutet  $3 * 10^9$  wiederholende Vorgänge pro Sekunde), die pro Instruktion eine komplette DES Verschlüsselung durchführen kann.

## Aufgabe 2d - Brute-Force bei DES

- d) Der Schlüsselraum bei DES beträgt  $2^{56}$ . Wie lange würde ein Angreifer für einen Brute-Force-Angriff mit einer handelsüblichen CPU brauchen? Verwenden Sie als Berechnungsgrundlage eine CPU mit 3GHz (3 GHz bedeutet  $3 \cdot 10^9$  wiederholende Vorgänge pro Sekunde), die pro Instruktion eine komplette DES Verschlüsselung durchführen kann.

$$\underbrace{\frac{2^{56}}{3 \cdot 10^9}}_{\substack{\text{Sekunden} \\ \text{für alle} \\ \text{Schlüssel}}} \cdot \underbrace{\frac{1}{60 \cdot 60 \cdot 24}}_{\substack{\text{Umrechnen} \\ \text{in Tage}}} \cdot \underbrace{\frac{1}{2}}_{\substack{\text{Im Durchschnitt findet} \\ \text{man den richtigen} \\ \text{Schlüssel nach der} \\ \text{Hälfte aller} \\ \text{Möglichkeiten}}} \approx 138.9 \text{ Tage}$$



## Aufgabe 2d - Brute-Force bei DES

- d) Kann DES bei einer Brute-Force-Dauer von 138.9 Tagen als sicher angesehen werden?

- d) Kann DES bei einer Brute-Force-Dauer von 138.9 Tagen als sicher angesehen werden?
- Geheime Daten sind nach 138.9 Tagen oft immer noch geheim  
→alles, was in unter 10 Jahren geknackt werden kann, ist unbrauchbar
  - Außerdem gibt es noch andere Angriffe auf DES, die deutlich schneller sind, z.B. *COPA-COBANA*
  - Bei AES liegt die Brute-Force-Dauer im Bereich der Zeit, die das Universum existiert
  - **DES ist nicht mehr sicher!**

## Aufgabe 2e - Schlüssellänge

- e) Warum müssen Schlüssel für das RSA-Verschlüsselungsverfahren deutlich länger sein als Schlüssel für symmetrische Verfahren?

- e) Warum müssen Schlüssel für das RSA-Verschlüsselungsverfahren deutlich länger sein als Schlüssel für symmetrische Verfahren?
- Die Sicherheit von RSA basiert auf der Schwierigkeit der Faktorisierung des Schlüssels
    - Bei größeren Zahlen ist die Faktorisierung schwieriger
  - Durch analytische Verfahren ist die Faktorisierung bei kleineren Zahlen zu einfach zu lösen
  - Bei symmetrischen Verfahren gibt es weniger analytische Möglichkeiten
    - Die Schlüssel können kürzer sein

## Aufgabe 3 - Blockchiffren

- Gegeben sind Klartext-Ciphertext-Paare
- Auf einer symmetrischen Blockchiffre basierend
- Ohne Padding
- $E$  ist die Verschlüsselungsfunktion,  $k$  der Schlüssel

$$(1) E_k(00000000_{16})=92298ec0_{16}$$

$$(2) E_k(000000010000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$$

## Aufgabe 3a - Auffälligkeiten im Ciphertext

(1)  $E_k(00000000_{16})=92298ec0_{16}$

(2)  $E_k(000000010000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$

- a) Gibt es Auffälligkeiten zwischen Klartext- und Ciphertextblöcken.  
Erkennen Sie Sicherheitsprobleme?

## Aufgabe 3a - Auffälligkeiten im Ciphertext

$$(1) E_k(00000000_{16})=92298ec0_{16}$$

$$(2) E_k(0000000100000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$$

a) Gibt es Auffälligkeiten zwischen Klartext- und Ciphertextblöcken.

Erkennen Sie Sicherheitsprobleme?

- Der Klartext  $00000001_{16}$  wird zweimal zu  $b736e2bc_{16}$  verschlüsselt
- Der Klartext  $00000000_{16}$  wird zweimal zu  $92298ec0_{16}$  verschlüsselt
- Blockchiffre im **ECB-Modus** verwendet
- Probleme:

## Aufgabe 3a - Auffälligkeiten im Ciphertext

$$(1) E_k(00000000_{16})=92298ec0_{16}$$

$$(2) E_k(0000000100000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$$

a) Gibt es Auffälligkeiten zwischen Klartext- und Ciphertextblöcken.  
Erkennen Sie Sicherheitsprobleme?

- Der Klartext  $00000001_{16}$  wird zweimal zu  $b736e2bc_{16}$  verschlüsselt
- Der Klartext  $00000000_{16}$  wird zweimal zu  $92298ec0_{16}$  verschlüsselt
- Blockchiffre im **ECB-Modus** verwendet
- Probleme:
  - Rückschlüsse auf Inhalt des Klartextes möglich
  - Vertauschen der Blöcke möglich
  - Beibehaltung von Mustern im Klartext:





## Aufgabe 3b - Blockgröße

$$(1) E_k(00000000_{16})=92298ec0_{16}$$

$$(2) E_k(000000010000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$$

b) Was ist die verwendete Blockgröße?

## Aufgabe 3b - Blockgröße

$$(1) E_k(00000000_{16})=92298ec0_{16}$$

$$(2) E_k(000000010000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$$

b) Was ist die verwendete Blockgröße?

- Da in (1) ein 32-Bit Klartextblock zu einem 32-Bit Ciphertextblock verschlüsselt wird, muss die Blockgröße kleiner gleich 32-Bit sein.

## Aufgabe 3b - Blockgröße

$$(1) E_k(00000000_{16})=92298ec0_{16}$$

$$(2) E_k(000000010000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$$

b) Was ist die verwendete Blockgröße?

- Da in (1) ein 32-Bit Klartextblock zu einem 32-Bit Ciphertextblock verschlüsselt wird, muss die Blockgröße kleiner gleich 32-Bit sein.
- Es können nur ganze Blöcke verschlüsselt werden  
→Blockgröße muss ein Teiler von 32-Bit sein, sonst könnte der Block aus (1) nicht verschlüsselt werden.  
→Möglich wären 1, 2, 4, 8, 16 oder 32-Bit

## Aufgabe 3b - Blockgröße

$$(1) E_k(00000000_{16})=92298ec0_{16}$$

$$(2) E_k(000000010000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$$

b) Was ist die verwendete Blockgröße?

- Da in (1) ein 32-Bit Klartextblock zu einem 32-Bit Ciphertextblock verschlüsselt wird, muss die Blockgröße kleiner gleich 32-Bit sein.
- Es können nur ganze Blöcke verschlüsselt werden  
→Blockgröße muss ein Teiler von 32-Bit sein, sonst könnte der Block aus (1) nicht verschlüsselt werden.  
→Möglich wären 1, 2, 4, 8, 16 oder 32-Bit
- Es müssen **32-Bit** sein, da wir sonst in (1) eine wiederholende Sequenz im Ciphertext hätten, da  $0000_{16}$  mehrmals verschlüsselt wird.

## Aufgabe 3c - Konfusion und Diffusion

(1)  $E_k(00000000_{16})=92298ec0_{16}$

(2)  $E_k(000000010000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$

- c) Was ist Konfusion und Diffusion? Sind diese Eigenschaften im Beispiel erfüllt?

## Aufgabe 3c - Konfusion und Diffusion

(1)  $E_k(00000000_{16})=92298ec0_{16}$

(2)  $E_k(0000000100000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$

c) Was ist Konfusion und Diffusion? Sind diese Eigenschaften im Beispiel erfüllt?

(1)  $E_k(00000000_{16})=92298ec0_{16}$

(2)  $E_k(0000000100000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$

- **Konfusion:** Der Schlüssel soll sich nicht aus Klartext-Ciphertext-Paaren ableiten lassen

## Aufgabe 3c - Konfusion und Diffusion

(1)  $E_k(00000000_{16})=92298ec0_{16}$

(2)  $E_k(0000000100000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$

c) Was ist Konfusion und Diffusion? Sind diese Eigenschaften im Beispiel erfüllt?

(1)  $E_k(00000000_{16})=92298ec0_{16}$

(2)  $E_k(0000000100000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$

- **Konfusion:** Der Schlüssel soll sich nicht aus Klartext-Ciphertext-Paaren ableiten lassen  
→ **Unklar**, da Schlüssel nicht bekannt
- **Diffusion:** Kleine Änderungen im Klartext sollen große Änderungen im Ciphertext bewirken

## Aufgabe 3c - Konfusion und Diffusion

$$(1) E_k(00000000_{16})=92298ec0_{16}$$

$$(2) E_k(0000000100000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$$

c) Was ist Konfusion und Diffusion? Sind diese Eigenschaften im Beispiel erfüllt?

$$(1) E_k(00000000_{16})=92298ec0_{16}$$

$$(2) E_k(0000000100000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$$

- **Konfusion:** Der Schlüssel soll sich nicht aus Klartext-Ciphertext-Paaren ableiten lassen  
→ **Unklar**, da Schlüssel nicht bekannt
- **Diffusion:** Kleine Änderungen im Klartext sollen große Änderungen im Ciphertext bewirken  
→ **Erfüllt**, da sich der Ciphertext bei Änderung von einem Bit im Klartext komplett ändert (siehe (1) und (2))



## Aufgabe 3d - Entschlüsselung

$$(1) E_k(00000000_{16})=92298ec0_{16}$$

$$(2) E_k(0000000100000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$$

d) Sie testen die Entschlüsselungsfunktion  $D$  des Entwicklers zu  $E$  und erhalten:

$$D_k(d35c273e_{16}) = 00000001_{16}$$

Ist das möglich?

## Aufgabe 3d - Entschlüsselung

$$(1) E_k(00000000_{16})=92298ec0_{16}$$

$$(2) E_k(0000000100000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$$

d) Sie testen die Entschlüsselungsfunktion  $D$  des Entwicklers zu  $E$  und erhalten:

$$D_k(d35c273e_{16}) = 00000001_{16}$$

Ist das möglich?

- **Nein**, das ist nicht möglich!

## Aufgabe 3d - Entschlüsselung

$$(1) E_k(00000000_{16})=92298ec0_{16}$$

$$(2) E_k(0000000100000000000000001_{16})=b736e2bc92298ec0b736e2bc_{16}$$

d) Sie testen die Entschlüsselungsfunktion  $D$  des Entwicklers zu  $E$  und erhalten:

$$D_k(d35c273e_{16}) = 00000001_{16}$$

Ist das möglich?

- **Nein**, das ist nicht möglich!
- Blockchiffren sind **Bijektiv**  
→ Jeder Klartextblock wird auf genau einen Ciphertextblock abgebildet und umgekehrt

## Aufgabe 4a - RSA Basics

- a) Seien die beiden Primzahlen  $p = 41$  und  $q = 17$  gegeben. Welcher der beiden Parameter  $e_1 = 32$ ,  $e_2 = 49$  ist ein gültiger RSA-Exponent?

- a) Seien die beiden Primzahlen  $p = 41$  und  $q = 17$  gegeben. Welcher der beiden Parameter  $e_1 = 32$ ,  $e_2 = 49$  ist ein gültiger RSA-Exponent?
- Bei RSA gilt:
    - $n = p \cdot q$ ,
    - $n$  ist öffentlich,  $p$  und  $q$  sind geheim
    - $\text{ggT}(\varphi(n), e) = 1$  (wobei  $\varphi(n) = (p - 1) \cdot (q - 1)$ , da  $p$  und  $q$  Primzahlen sind)

## Aufgabe 4a - RSA Basics

- a) Seien die beiden Primzahlen  $p = 41$  und  $q = 17$  gegeben. Welcher der beiden Parameter  $e_1 = 32$ ,  $e_2 = 49$  ist ein gültiger RSA-Exponent?
- Bei RSA gilt:
    - $n = p \cdot q$ ,
    - $n$  ist öffentlich,  $p$  und  $q$  sind geheim
    - $\text{ggT}(\varphi(n), e) = 1$  (wobei  $\varphi(n) = (p - 1) \cdot (q - 1)$ , da  $p$  und  $q$  Primzahlen sind)
  - $\varphi(n) = 40 \cdot 16 = 640$

## Aufgabe 4a - RSA Basics

a) Seien die beiden Primzahlen  $p = 41$  und  $q = 17$  gegeben. Welcher der beiden Parameter  $e_1 = 32$ ,  $e_2 = 49$  ist ein gültiger RSA-Exponent?

- Bei RSA gilt:
  - $n = p \cdot q$ ,
  - $n$  ist öffentlich,  $p$  und  $q$  sind geheim
  - $ggT(\varphi(n), e) = 1$  (wobei  $\varphi(n) = (p - 1) \cdot (q - 1)$ , da  $p$  und  $q$  Primzahlen sind)
- $\varphi(n) = 40 \cdot 16 = 640$
- $ggT(640, e_1) = ggT(640, 32) = 32 \rightarrow$  **Ungültig**

## Aufgabe 4a - RSA Basics

a) Seien die beiden Primzahlen  $p = 41$  und  $q = 17$  gegeben. Welcher der beiden Parameter  $e_1 = 32$ ,  $e_2 = 49$  ist ein gültiger RSA-Exponent?

- Bei RSA gilt:
  - $n = p \cdot q$ ,
  - $n$  ist öffentlich,  $p$  und  $q$  sind geheim
  - $ggT(\varphi(n), e) = 1$  (wobei  $\varphi(n) = (p - 1) \cdot (q - 1)$ , da  $p$  und  $q$  Primzahlen sind)
- $\varphi(n) = 40 \cdot 16 = 640$
- $ggT(640, e_1) = ggT(640, 32) = 32 \rightarrow$  **Ungültig**
- $ggT(640, e_2) = ggT(640, 49) = 1 \rightarrow$  **Gültig**



## Aufgabe 4a - RSA Basics

- a) Seien die beiden Primzahlen  $p = 41$  und  $q = 17$  und der Exponent  $e = 49$  gegeben. Berechnen Sie den zugehörigen privaten Schlüssel  $K_{pr} = (p, q, d)$ . Sie können hierbei den erweiterten Euklidischen Algorithmus verwenden.

## Aufgabe 4a - RSA Basics

a) Seien die beiden Primzahlen  $p = 41$  und  $q = 17$  und der Exponent  $e = 49$  gegeben. Berechnen Sie den zugehörigen privaten Schlüssel  $K_{pr} = (p, q, d)$ . Sie können hierbei den erweiterten Euklidischen Algorithmus verwenden.

- Bei RSA gilt:
  - $n = p \cdot q$ ,
  - $n$  ist öffentlich,  $p$  und  $q$  sind geheim
  - $\text{ggT}(\varphi(n), e) = 1$  (wobei  $\varphi(n) = (p - 1) \cdot (q - 1)$ , da  $p$  und  $q$  Primzahlen sind)
  - $K_{pub} = (n, e)$
  - $d \equiv e^{-1} \pmod{\varphi(n)}$
  - $K_{pr} = (p, q, d)$

## Aufgabe 4a - RSA Basics

- $d \equiv e^{-1} \pmod{\varphi(n)} = 49^{-1} \pmod{640}$
- Gesucht ist die Inverse von 49 modulo 640  
→ EEA auf 49 und 640 anwenden

## Aufgabe 4a - RSA Basics

- $d \equiv e^{-1} \pmod{\varphi(n)} = 49^{-1} \pmod{640}$
- Gesucht ist die Inverse von 49 modulo 640  
→ EEA auf 49 und 640 anwenden

a	b	$\lfloor \frac{b}{a} \rfloor$	$\alpha$	$\beta$
49	640	$\lfloor \frac{640}{49} \rfloor = 13$	$1 - (13 \cdot -16) = 209$	-16
$640 \bmod 49 = 3$	49	$\lfloor \frac{49}{3} \rfloor = 16$	$0 - (16 \cdot 1) = -16$	1
$49 \bmod 3 = 1$	3		1	0

- 49 stand in der ersten Zeile bei a  
→  $49^{-1} \pmod{640}$  steht in der ersten Zeile bei  $\alpha$   
→  $49^{-1} \pmod{640} \equiv 209$
- $K_{pr} = (p, q, d) = (41, 17, 209)$

## Aufgabe 4b - RSA anwenden

- b) Ver- und Entschlüsseln Sie die Nachricht  $m = 5$  mithilfe des RSA-Algorithmus mit den Parametern  $p = 3$ ,  $q = 11$ ,  $d = 7$ ,  $e = 3$ .

b) Ver- und Entschlüsseln Sie die Nachricht  $m = 5$  mithilfe des RSA-Algorithmus mit den Parametern  $p = 3$ ,  $q = 11$ ,  $d = 7$ ,  $e = 3$ .

- Bei RSA gilt:
  - $n = p \cdot q$ ,
  - $K_{pub} = (n, e)$
  - $K_{pr} = (p, q, d)$
  - $c \equiv m^e \pmod{n}$  (Verschlüsselung)
  - $m \equiv c^d \pmod{n}$  (Entschlüsselung)

## Aufgabe 4b - RSA anwenden

b) Ver- und Entschlüsseln Sie die Nachricht  $m = 5$  mithilfe des RSA-Algorithmus mit den Parametern  $p = 3$ ,  $q = 11$ ,  $d = 7$ ,  $e = 3$ .

- Bei RSA gilt:
  - $n = p \cdot q$ ,
  - $K_{pub} = (n, e)$
  - $K_{pr} = (p, q, d)$
  - $c \equiv m^e \pmod{n}$  (Verschlüsselung)
  - $m \equiv c^d \pmod{n}$  (Entschlüsselung)
- $n = 3 \cdot 11 = 33$
- $c = 5^3 \pmod{33} = 26$
- $m = 26^7 \pmod{33} = 5$

## Aufgabe 4b - RSA anwenden

- b) Ver- und Entschlüsseln Sie die Nachricht  $m = 9$  mithilfe des RSA-Algorithmus mit den Parametern  $p = 5$ ,  $q = 11$ ,  $d = 3$ ,  $e = 27$ .



b) Ver- und Entschlüsseln Sie die Nachricht  $m = 9$  mithilfe des RSA-Algorithmus mit den Parametern  $p = 5$ ,  $q = 11$ ,  $d = 3$ ,  $e = 27$ .

- Bei RSA gilt:
  - $n = p \cdot q$ ,
  - $K_{pub} = (n, e)$
  - $K_{pr} = (p, q, d)$
  - $c \equiv m^e \pmod{n}$  (Verschlüsselung)
  - $m \equiv c^d \pmod{n}$  (Entschlüsselung)

## Aufgabe 4b - RSA anwenden

b) Ver- und Entschlüsseln Sie die Nachricht  $m = 9$  mithilfe des RSA-Algorithmus mit den Parametern  $p = 5$ ,  $q = 11$ ,  $d = 3$ ,  $e = 27$ .

- Bei RSA gilt:
  - $n = p \cdot q$ ,
  - $K_{pub} = (n, e)$
  - $K_{pr} = (p, q, d)$
  - $c \equiv m^e \pmod{n}$  (Verschlüsselung)
  - $m \equiv c^d \pmod{n}$  (Entschlüsselung)
- $n = 5 \cdot 11 = 55$
- $c = 9^{27} \pmod{55} = 4$
- $m = 4^3 \pmod{55} = 9$

c) Warum ist es problematisch Textbook-RSA direkt zu verwenden?

- c) Warum ist es problematisch Textbook-RSA direkt zu verwenden?
- Probleme mit Textbook-RSA:
    - Wenn  $c = m^e < n$ , dann greift das Modulo nicht  
→ Berechnung von  $m$  ist trivial:  $m = \sqrt[e]{c}$

## Aufgabe 4c - Textbook-RSA

- c) Warum ist es problematisch Textbook-RSA direkt zu verwenden?
- Probleme mit Textbook-RSA:
    - Wenn  $c = m^e < n$ , dann greift das Modulo nicht  
→ Berechnung von  $m$  ist trivial:  $m = \sqrt[e]{c}$
    - Derselbe Klartext wird immer in denselben Ciphertext verschlüsselt

- c) Warum ist es problematisch Textbook-RSA direkt zu verwenden?
- Probleme mit Textbook-RSA:
    - Wenn  $c = m^e < n$ , dann greift das Modulo nicht  
→ Berechnung von  $m$  ist trivial:  $m = \sqrt[e]{c}$
    - Derselbe Klartext wird immer in denselben Ciphertext verschlüsselt
    - Homomorphie bzgl. Multiplikation:  
Gegeben: Verschlüsselte Nachricht  $c = Enc(m)$   
Ziel: Empfänger soll nicht  $m$ , sondern  $m \cdot 2$  erhalten

c) Warum ist es problematisch Textbook-RSA direkt zu verwenden?

- Probleme mit Textbook-RSA:

- Wenn  $c = m^e < n$ , dann greift das Modulo nicht  
→ Berechnung von  $m$  ist trivial:  $m = \sqrt[e]{c}$
- Derselbe Klartext wird immer in denselben Ciphertext verschlüsselt
- Homomorphie bzgl. Multiplikation:

Gegeben: Verschlüsselte Nachricht  $c = Enc(m)$

Ziel: Empfänger soll nicht  $m$ , sondern  $m \cdot 2$  erhalten

$$c' = 2^e \cdot c \pmod n$$

$$Dec(c') \equiv (s \cdot c)^d \equiv (2^e \cdot m^e)^d \equiv 2^{ed} \cdot m^{ed} = 2 \cdot m \pmod n$$

c) Warum ist es problematisch Textbook-RSA direkt zu verwenden?

- Probleme mit Textbook-RSA:

- Wenn  $c = m^e < n$ , dann greift das Modulo nicht

- Berechnung von  $m$  ist trivial:  $m = \sqrt[e]{c}$

- Derselbe Klartext wird immer in denselben Ciphertext verschlüsselt

- Homomorphie bzgl. Multiplikation:

- Gegeben: Verschlüsselte Nachricht  $c = Enc(m)$

- Ziel: Empfänger soll nicht  $m$ , sondern  $m \cdot 2$  erhalten

- $$c' = 2^e \cdot c \pmod n$$

- $$Dec(c') \equiv (s \cdot c)^d \equiv (2^e \cdot m^e)^d \equiv 2^{ed} \cdot m^{ed} = 2 \cdot m \pmod n$$

- Alle diese Probleme lassen sich durch die Verwendung eines geeigneten Padding-Schemas lösen!



## Aufgabe 4d - Exponenten

In der Praxis werden häufig die kurzen Exponenten  $e = 3, 17$  und  $2^{16} + 1$  als öffentliche Exponenten verwendet um die Verschlüsselung zu beschleunigen.

- d) Warum sollten diese drei kurzen Exponenten nicht als Wert für den privaten Exponenten  $d$  in Applikationen verwendet werden, in welchen die Entschlüsselung beschleunigt werden soll?

## Aufgabe 4d - Exponenten

In der Praxis werden häufig die kurzen Exponenten  $e = 3$ ,  $17$  und  $2^{16} + 1$  als öffentliche Exponenten verwendet um die Verschlüsselung zu beschleunigen.

- d) Warum sollten diese drei kurzen Exponenten nicht als Wert für den privaten Exponenten  $d$  in Applikationen verwendet werden, in welchen die Entschlüsselung beschleunigt werden soll?
- Würde einen Brute-Force-Angriff auf den privaten Exponenten sehr leicht machen
  - Beim öffentlichen Exponenten ist es egal, weil er ohnehin öffentlich ist

## Aufgabe 4d - Exponenten

In der Praxis werden häufig die kurzen Exponenten  $e = 3, 17$  und  $2^{16} + 1$  als öffentliche Exponenten verwendet um die Verschlüsselung zu beschleunigen.

- d) Schlagen sie eine minimale Länge (in Bits) für den Exponenten  $d$  vor und begründen Sie ihre Antwort.

## Aufgabe 4d - Exponenten

In der Praxis werden häufig die kurzen Exponenten  $e = 3, 17$  und  $2^{16} + 1$  als öffentliche Exponenten verwendet um die Verschlüsselung zu beschleunigen.

d) Schlagen sie eine minimale Länge (in Bits) für den Exponenten  $d$  vor und begründen Sie ihre Antwort.

- Direkter Brute-Force wäre schon ab 128 Bit nicht mehr möglich
- Es gibt aber analytische Angriffe, die mit deutlich weniger Rechenaufwand auskommen
- Bitlänge von  $d$  sollte mindestens **ein Drittel der Bitlänge von  $n$**  entsprechen
- RSA-2048  $d$  also mindestens 615 Bit lang sein (siehe <https://www.keylength.com>)

**Fragen? Feedback?**

---

**Bis zum nächsten Mal!**

---