

# $\int$ Skripte **HSLU** Hochschule Luzern

## Modul I.BA KRYPT

### Musterprüfung/Kompetenznachweis 3

#### Datum, Zeit und Ort

Name: Musterlösung

#### Bedingungen (für die Prüfung):

**Zeit:** 90 Minuten  
**Hilfsmittel:** Beliebige schriftliche Unterlagen (Open book), ein beliebiger nicht kommunika-  
tionsfähiger TR, keine weiteren elektronische Geräte (Handy, Laptop, Tablet  
usw.).

Bitte beachten Sie:

- Mit Bleistift oder mit **roter** Farbe schreiben ist nicht gestattet.
- Lösungen auf den dafür vorgesehenen Platz eintragen und/oder die angehängten Zusatzblät-  
ter benutzen.
- Lesen Sie zuerst die Aufgaben, bevor Sie zu lösen anfangen!
- Saubere und deutliche Resultatformulierung (z.B. mit Resultatsatz, dort wo es angebracht  
ist).
- Unbelegte oder nicht nachvollziehbare Resultate werden nicht berücksichtigt.
- Ungültiges ist sauber durchzustreichen, Mehrfachlösungen werden nicht gewertet.
- Der Lösungsweg muss klar ersichtlich sein.
- Bei Multiple Choice Aufgaben wird falsches Ankreuzen mit Punktabzug bestraft, d.h. im  
Zweifelsfalle ist es besser die Felder offen zu lassen. Die Summe innerhalb einer solchen Auf-  
gabe kann aber nicht negativ werden.

#### Punktzahlen:

maximal: **60**  
für die Note 6: **50**  
für die Note 4: **30**

Ich wünsche Ihnen viel Glück und viel Erfolg

Josef Schuler

**Punkteübersicht:**

Aufgabe	Max. Punktzahl	Erreichte Punktzahl	
1)	9		
2)	6		
3)	7		
4)	6		
5)	6		
6)	5		
7)	8		
8)	8		
9)	5		
	-----		Note
<b>Total</b>	60		
	=====	=====	

**Notenskala:**

**Note** =  $\frac{1}{10} \cdot$  erreichte Punktzahl + 0,75 **Danach wird auf die halbe Note gerundet.**

**Als Tabelle:**

Note	Punkte	Anzahl
6 = A	≥ 50	
5,5 = B	≥ 45	
5 = C	≥ 40	
4,5 = D	≥ 35	
4 = E	≥ 30	
3,5 = FX	≥ 25	
3 = F	< 25	

## Aufgabe 1

9 Punkte

Das linke Klartext-Bild ist mit einer Blockchiffre verschlüsselt worden. Das rechte Bild ist die verschlüsselte Version.



a) [1 P.] Geben Sie einen geeigneten, aktuellen & standardisierten Algorithmus an. AES

b) [1 P.] Welche minimale Schlüsselgrösse muss verwendet werden? 128 Bit

c) [1 P.] In welchem Modus wurde das obige Bild verschlüsselt? ECB-Modus

d) [1 P.] Begründen Sie Ihre Angabe des Modus in Aufgabe c).

Gleiche Klartextblöcke werden in gleiche Chiffratblöcke verschlüsselt, daher ist in diesem Bild die Grundstruktur nach wie vor gut sichtbar.

e) [2 P.] Geben Sie je einen (weiteren) Vor- und Nachteil des obigen Modus an.

Vorteil: Parallelisierung resp. Teilverschlüsselung

Nachteil: Vertauschen von Blöcken wird ev. n. entdeckt.

f) [1 P.] Geben Sie einen Modus an, der das Bild besser verschlüsselt.

CBC- oder CTR-Modus (Angaben von weiteren Modi wie OFB, GCM o.a. werden auch akzeptiert.)

g) [1 P.] Das Klartext-Bild soll auf dem Übertragungsweg gegen Verändern geschützt werden. Wie machen Sie das, wenn der oben erwähnte Blockchiffrieralgorithmus benutzt werden soll?

CBC-MAC-Berechnung (oder kombinierte Modi wie GCM)

h) [1 P.] Gibt es für f) eine (symmetrische) Alternative ohne Verwendung eines Blockchiffrierers? Was braucht es dazu? Wie heisst die Konstruktion?

Ja, mit einer Stromchiffre, dazu braucht es einen Pseudorandom-generator.

**Aufgabe 2****6 Punkte**

Voraussetzungen:

- Alice besitzt den Schlüssel  $K_1$
- Bob besitzt den Schlüssel  $K_2$

Alice möchte Bob die Meldung  $M$  verschlüsselt zuschicken. Dabei verwenden Sie das untenstehende Protokoll, das ohne vorgängigen Schlüsselaustausch auskommt. Als Verschlüsselungsoperation wird die Stromchiffre benutzt.

Alice mit $K_1$	unsichere Leitung	Bob $K_2$
Alice <b>verschlüsselt</b> die Nachricht $M$ mit ihrem geheimen Schlüssel $K_1$ .		
	$C_1 = M \oplus K_1$ ----->	
		Bob <b>verschlüsselt</b> die Nachricht $C_1$ mit seinem geheimen Schlüssel $K_2$ .
	$C_2 = C_1 \oplus K_2$ <-----	
Alice <b>entschlüsselt</b> die Nachricht $C_2$ mit ihrem geheimen Schlüssel $K_1$ .		
	$C_3 = C_2 \oplus K_1$ ----->	
		Bob <b>entschlüsselt</b> die Nachricht $C_3$ mit seinem geheimen Schlüssel $K_2$ . ? $Y = C_3 \oplus K_2 \stackrel{?}{=} M$

- a) [3 P.] Beweisen Sie nun, dass der von Bob zu Letzt berechnete Wert  $Y = C_3 \oplus K_2$  tatsächlich gleich der Nachricht  $M$  ist.
- b) [3 P.] Es ist nun offensichtlich, dass man nun drei Meldungen statt nur eine Meldung über die Leitung schicken muss. Aufgrund dessen, dass dieses Protokoll nicht implementiert wurde, muss ja noch irgendwo ein anderer Hacken sein. Finden Sie diesen Hacken. **Tipp:** Versetzen Sie sich in Eve, die alle Meldungen abhören kann. Eve hat die Idee, dass sie einfach einmal alle drei über die Leitung geschickten Chiffre miteinander XOR'ed. Berechnen Sie nun, was dann rauskommt.

**Lösung:**

a)

- $C_3 = (C_1 \oplus K_2) \oplus K_1 = ((M \oplus K_1) \oplus K_2) \oplus K_1 = ((M \oplus K_1) \oplus K_1) \oplus K_2 = M \oplus K_2$
- Und daher ist  $Y = (M \oplus K_2) \oplus K_2 = M$

- b) Eve sieht ja alle 3 chiffrierten Meldungen; sie muss nur alle 3 Meldungen miteinander XOR'en.

$$C_1 \oplus C_2 \oplus C_3 = C_1 \oplus C_2 \oplus (C_2 \oplus K_1) = C_1 \oplus K_1 = (M \oplus K_1) \oplus K_1 = M$$

**Aufgabe 3****7 Punkte**

Sie setzen für eine PIN-Block-Verschlüsselung zwei Typen von Blockchiffren ein:

- Typ A = 256 Bit AES.
- Typ B = Doppel-AES mit je 128 Bit Schlüsselgrösse (Analog einem Doppel-DES).

Die zwei Typen unterziehen Sie nun einer kryptoanalytischen Betrachtung und kommen zu den folgenden Ergebnissen, die Sie nun entsprechend in der Tabelle auswählen und ausfüllen.

**Falsches Ankreuzen gibt Punktabzug, die Summe kann aber nicht negativ werden!**

Angriff	Typ von Attacke
<b>Table look up</b>	<input checked="" type="checkbox"/> Für Typ A und B muss ungefähr der gleiche Aufwand betrieben werden. <input type="checkbox"/> Für Typ A muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input type="checkbox"/> Für Typ B muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input type="checkbox"/> Man kann die Typen bei diesem Angriff gar nicht vergleichen.
<b>Exhaustive Key Search</b>	<input checked="" type="checkbox"/> Für Typ A und B muss ungefähr der gleiche Aufwand betrieben werden. <input type="checkbox"/> Für Typ A muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input type="checkbox"/> Für Typ B muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input type="checkbox"/> Man kann die Typen bei diesem Angriff gar nicht vergleichen.
<b>Time-memory-Trade off "meet-in-the-middle"</b>	<input type="checkbox"/> Für Typ A und B muss ungefähr der gleiche Aufwand betrieben werden. <input type="checkbox"/> Für Typ A muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input checked="" type="checkbox"/> Für Typ B muss der kleinere Aufwand betrieben werden nämlich Faktor <input type="text"/> anstatt <input type="text"/> _____. <input type="checkbox"/> Man kann die Typen bei diesem Angriff gar nicht vergleichen.

Lösung:

Angriff	Typ von Attacke
Table look up	<input checked="" type="checkbox"/> Für Typ A und B muss ungefähr der gleiche Aufwand betrieben werden. <input type="checkbox"/> Für Typ A muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input type="checkbox"/> Für Typ B muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input type="checkbox"/> Man kann die Typen bei diesem Angriff gar nicht vergleichen.
Exhaustive Key Search	<input checked="" type="checkbox"/> Für Typ A und B muss ungefähr der gleiche Aufwand betrieben werden. <input type="checkbox"/> Für Typ A muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input type="checkbox"/> Für Typ B muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input type="checkbox"/> Man kann die Typen bei diesem Angriff gar nicht vergleichen.
Time-memory-Trade off "meet-in-the-middle"	<input type="checkbox"/> Für Typ A und B muss ungefähr der gleiche Aufwand betrieben werden. <input type="checkbox"/> Für Typ A muss der kleinere Aufwand betrieben werden nämlich Faktor _____ anstatt _____. <input checked="" type="checkbox"/> Für Typ B muss der kleinere Aufwand betrieben werden nämlich Faktor $2 * 2^{128} = 2^{129}$ anstatt $2^{256}$ . <input type="checkbox"/> Man kann die Typen bei diesem Angriff gar nicht vergleichen.

Bewertungshinweis:

- Pro richtiges Ankreuzen, 1½ P.
- Angabe Faktor  $2^{256}$  gibt 1 P.
- Angabe Faktor  $2 * 2^{128} = 2^{129}$  gibt 1½ P.
- Pro falsches Ankreuzen ¾ P. Abzug, die Summe kann nicht negativ werden.


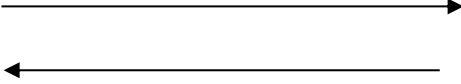

## Aufgabe 4


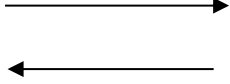

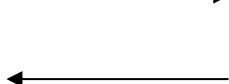

2 + 4 = 6 Punkte

## Aufgabe 4.1

2 Punkte

Im Folgenden sind die Abläufe eines nicht angegriffenen und eines angegriffenen Schlüsselaustausch Protokolls gegeben.

Alice		Bob
		
Super, Bob und ich haben nun den gleichen Schlüssel K ausgetauscht!		Super, Alice und ich haben nun den gleichen Schlüssel K ausgetauscht!

Alice		Eve		Bob
				
Super, Bob und ich haben nun <b>den gleichen Schlüssel K ausgetauscht!??</b>				Super, Alice und ich haben nun <b>den gleichen Schlüssel K ausgetauscht!??</b>

Beantworten Sie die folgenden Fragen (je ½ P.)

- Wie heisst der dargestellte Angriff? Man-in-the middle
- Bei welchem Schlüsselaustausch Protokoll ist der Angriff erfolgreich? Diffie-Hellman
- Warum ist der Angriff erfolgreich? Protokoll hat keine Benutzerauthentizität
- Korrigieren Sie im **angegriffenen Protokoll** die Aussage „...**den gleichen Schlüssel K ausgetauscht!??**“, d.h. ersetzen Sie **...**, so dass die beiden Aussagen stimmen.

Alice hat mit Eve einen K1 und Bob hat mit Eve einen K2 ausgetauscht.

**Lösung:**

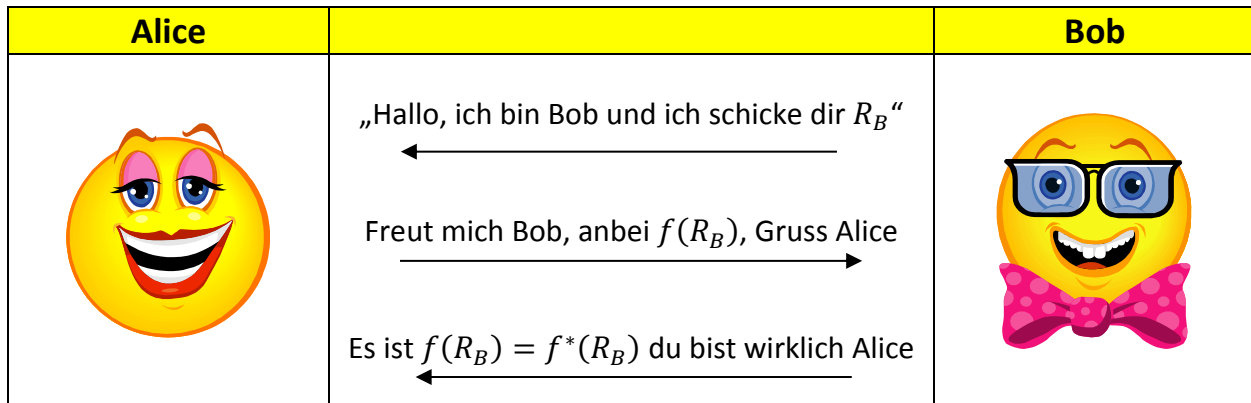
- Wie heisst der dargestellte Angriff? ***Man-in-the middle***
- Bei welchem Schlüsselaustausch Protokoll ist der Angriff erfolgreich? ***Diffie-Hellman***
- Warum ist der Angriff erfolgreich? ***Protokoll hat keine Benutzerauthentizität***
- Korrigieren Sie im angegriffenen Protokoll die Aussage „...den gleichen Schlüssel K ausgetauscht!??“ ***Alice hat mit Eve einen K1 und Bob hat mit Eve einen K2 ausgetauscht.***



**Aufgabe 4.2****4 Punkte**

Im Folgenden ist der Ablauf bei einer Authentisierung gegeben. Im Protokoll werden die folgenden Abkürzungen verwendet:

- $R_B$  = Zufallswert von Bob gewählt; «R» steht für Random.
- $f(R_B)$  der Hashwert von  $R_B$ , wobei  $f$  eine kryptographisch sichere Hashfunktion (z.B. SHA-2 oder SHA-3) ist. Das ist der Wert den Alice berechnet.
- $f^*(R_B)$  der Hashwert von  $R_B$ , wobei  $f^*$  die gleiche kryptographisch sichere Hashfunktion wie  $f$  ist, aber der Hashwert wird von Bob gerechnet.



Beantworten Sie die folgenden Fragen (je 1 P.)

- Ist das Protokoll „mutual“, wenn JA, dann begründen Sie warum, wenn NEIN, wer authentifiziert sich gegenüber wem?

**Nein, nur Alice authentifiziert sich gegenüber Bob.**

- Ist die gewählte Funktion (kryptographisch sichere Hashfunktion, z.B. SHA-2 oder SHA-3) ein geeigneter Mechanismus? Wenn JA, warum, wenn NEIN warum nicht, und geben Sie einen geeigneteren an.

**Nein, jedermann könnte diesen Hash rechnen; CBC-MAC oder HMAC.**

- Für eine erfolgreiche einseitige oder gegenseitige Authentisierung fehlt ein wichtiges Element, was für eines?

**Es fehlt ein gemeinsamer symmetrischer Schlüssel  $K$   
(Resp. zwei Public Key Schlüsselpaare)**

- Ein wesentliches Element für eine erfolgreiche einseitige oder gegenseitige Authentisierung ist vorhanden, was für eines?

**Die Anfrage mittels einem Randomwert.**

**Aufgabe 5****2 + 1 + 3 = 6 Punkte**

Gegeben ist ein RSA System mit den Primzahlen  $p = 23$  und  $q = 41$  sowie dem öffentlichen Exponenten  $e = 9$  und dem geheimen Exponenten  $d = 489$ .

- [2 P.] Zeigen Sie, dass es der öffentliche Exponent  $e = 9$  legitim ist.
- [1 P.] Zeigen Sie, dass der Exponent  $d$  zum Exponent  $e$  passt.
- [3 P.] Nun verschlüsselt Alice die Meldung  $m = ?$  mit dem gegebenen RSA-System und schickt die verschlüsselte Meldung  $c = 492$  über die Leitung. Die Angreiferin Eve will die verschlüsselte Meldung  $c$  so verändern, dass bei Bob nach dem Entschlüsseln die Meldung  $5 \cdot m$  erscheint. Berechnen Sie das neue Chiffre  $c'$ , welches Eve erzeugen und an Bob weiterschicken muss.

**Lösung:**

a)  $N = p \cdot q \Rightarrow \varphi(N) = \varphi(p) \cdot \varphi(q) = (p - 1) \cdot (q - 1) = 22 \cdot 40 = 880.$

Es muss gelten:  $\text{ggT}(e; \varphi(N)) = \text{ggT}(9; 880) = 1$

1 P.

Das kann man auf ohne TR z.B. auf die folgenden zwei Arten machen:

- Primfaktorzerlegung von  $880 = 2^4 \cdot 5 \cdot 11$ : Sie enthält den Teiler 3 nicht, und damit ist der geforderte  $\text{ggT}(9; 880) = \text{ggT}(3^2; 2^4 \cdot 5 \cdot 11) = 1$
- $e = 9 = 3^2$ . Nun muss ich nur noch zeigen, dass 880 den Teiler 3 nicht enthält. Das kann einfach gezeigt werden mit  $\frac{880}{3} = 293,33 \dots$

1 P.

- b) Es ist zu zeigen, dass  $e \cdot d \bmod \varphi(N) \equiv 1$  ist.

$$9 \cdot 489 \bmod 880 \equiv 4401 \bmod 880 \equiv 5 \cdot 880 + 1 \bmod 880 \equiv 1.$$

1 P.

- c) Eve muss  $c' \equiv 5^9 \cdot c \bmod N \equiv 5^9 \cdot 492 \bmod 943 \equiv 1'953'125 \cdot 492 \bmod 943$   
 $\equiv 172 \cdot 492 \bmod 943 \equiv 84'624 \bmod 943 \equiv 697$

**Resultat:** Eve muss den Wert 697 an Bob zuschicken.

3 P.

**Kontrolle (wird in der Prüfung nicht verlangt):**

$$697^{489} \bmod 943 \equiv 615 = 5 \cdot 123$$

**Aufgabe 6****5 Punkte**

Die 3-stellige Zahl  $x$  wird mit der Formel  $y \equiv (a \cdot x + b) \bmod N$  verschlüsselt. Die Entschlüsselungsfunktion lautet:  $x \equiv a^{-1} \cdot (y - b) \bmod N$ . Dabei ist  $N = 11 \cdot 23 \cdot 41$  ein Produkt von drei Primzahlen; der Wert  $N$  ist öffentlich bekannt. Die Werte  $a$  und  $b$  bilden in der Form  $(a; b)$  den geheimen Schlüssel. Die Werte  $a$  und  $b$  sind für die Verschlüsselung und Entschlüsselung geeignete Werte aus der Menge  $\{2; 3; \dots; N - 1\}$

- a) [1 P.] Begründen Sie, ob es sich hier um eine symmetrische oder asymmetrische Verschlüsselung handelt. **Achtung:** Die Angabe „symmetrisch“ oder „asymmetrisch“ ohne stichhaltige Begründung gibt keine Punkte!

**Lösung:**

Es handelt sich um eine symmetrische Verschlüsselung, da Sender und Empfänger den gleichen Schlüssel  $(a; b)$  haben müssen. (Dies ungeachtet dessen, dass der Sender noch auf  $a^{-1} \bmod N$  umrechnen muss).

- b) [4 P.] Aus wie vielen möglichen Schlüsseln der Form  $(a; b)$  können bei dieser Verschlüsselung ausgewählt werden? Es ist die exakte Zahl anzugeben.

**Lösung allgemein:**

- Für  $b$  sind alle möglichen Werte aus der Menge  $\{2; 3; \dots; N - 1\}$  möglich, daher gibt es für  $b$  total  $N - 2$  mögliche Werte.
- Für  $a$  sind aus der Menge  $\{2; 3; \dots; N - 1\}$  nur diejenigen möglich, die teilerfremd zu  $N$  sind. Da die Zahl 1 aber nicht drin sein darf lautet die Anzahl der möglichen Werte für  $a$  somit:  
 $\varphi(N) - 1 = \varphi(r \cdot s \cdot t) - 1 = \varphi(r) \cdot \varphi(s) \cdot \varphi(t) - 1 = (r - 1) \cdot (s - 1) \cdot (t - 1) - 1$ .
- Somit gibt es total  $(N - 2) \cdot [(r - 1) \cdot (s - 1) \cdot (t - 1) - 1]$  mögliche Schlüssel.

**Lösung mit den konkreten Zahlen:**

$$r = 11; s = 23; t = 41 \Rightarrow N = r \cdot s \cdot t = 11 \cdot 23 \cdot 41 = 10373$$

$$\Rightarrow N - 2 = 10371$$

$$\Rightarrow \varphi(N) - 1 = \varphi(r \cdot s \cdot t) - 1 = (11 - 1) \cdot (23 - 1) \cdot (41 - 1) - 1 = 10 \cdot 22 \cdot 40 - 1 = 8799$$

Somit gibt es total  $10371 \cdot 8799 = 91'254'429$  mögliche Schlüssel.

**Aufgabe 7****8 Punkte**

Gegeben ist die elliptische Kurve  $E: y^2 \equiv x^3 + x + 1$  über  $\mathbb{Z}_{23}$ .

- a) [2 P.] Überprüfen Sie, ob der Punkt (11; 19) auf der Kurve liegt.  
 b) [3 P.] Der Punkt  $P(3; 10)$  liegt auf der Kurve. Berechnen Sie die Koordinaten des Punktes  $R = 2P$ .  
 c) [3 P.] Die Punkte  $P(3; 10)$  und  $Q(9; 7)$  liegen auf der Kurve. Berechnen Sie die Koordinaten des Punktes  $T = P + Q$ .

Falls es Ihnen hilft, dürfen Sie zudem die Kehrwerttabelle mod 23 verwenden.

x	1	2	3	4	5	6	7	8	9	10	11
$x^{-1} \bmod 23$	1	12	8	6	14	4	10	3	18	7	21

x	12	13	14	15	16	17	18	19	20	21	22
$x^{-1} \bmod 23$	2	16	5	20	13	19	9	17	15	11	22

**Lösung:**

a)  $y^2 \equiv 19^2 \equiv 361 \equiv 16 \bmod 23$

$$x^3 + x + 1 \equiv 11^3 + 11 + 1 \equiv 1331 + 11 + 1 \equiv 1343 \equiv 9 \bmod 23$$

**Resultat:** Da die Werte nicht gleich sind, folgt dass der Punkt  $P(11; 19)$  nicht auf der Kurve liegt.

b) Berechnung von  $2 \cdot P = 2 \cdot (3; 10)$

$$s \equiv \frac{3 \cdot x_1^2 + a}{2 \cdot y_1} \bmod p \equiv \frac{3 \cdot 3^2 + 1}{2 \cdot 10} \equiv \frac{28}{20} \equiv 28 \cdot 20^{-1} \equiv 5 \cdot 20^{-1} \equiv 5 \cdot 15 \equiv 75 \equiv 6 \bmod 23$$

**Bemerkung:** In diesem Fall dürfte man kürzen, Grund: Die Kürzungsregel darf angewandt werden.

$$\frac{xa}{xb} \equiv xa \cdot (xb)^{-1} \equiv a \cdot (b)^{-1} \bmod m \Leftrightarrow \text{ggT}(x, m) = 1$$

$$\text{ggT}(4, 23) = 1 \Rightarrow \frac{28}{20} \equiv \frac{4 \cdot 7}{4 \cdot 5} \equiv 7 \cdot 5^{-1} \equiv 7 \cdot 14 \equiv 98 \equiv 6 \bmod 23$$

Oder einen Schritt weiter:

$$\text{ggT}(5, 23) = 1 \Rightarrow \frac{5}{20} \equiv \frac{5 \cdot 1}{5 \cdot 4} \equiv 1 \cdot 4^{-1} \equiv 1 \cdot 6 \equiv 6 \bmod 23$$

$$x_3 \equiv s^2 - x_1 - x_2 \bmod p \equiv 6^2 - 3 - 3 \bmod 23 \equiv 30 \bmod 23 \equiv 7$$

$$y_3 \equiv s(x_1 - x_3) - y_1 \bmod p \equiv 6(3 - 7) - 10 \bmod 23 \equiv -34 \equiv 12 \bmod 23$$

**Also:**  $2 \cdot (3; 10) = (7; 12)$

3 P.

c) Berechnung von  $P + Q = (3; 10) + (9; 7)$

Detailberechnungen:

$$s \equiv \frac{y_2 - y_1}{x_2 - x_1} \bmod p \equiv \frac{7 - 10}{9 - 3} \bmod 23 \equiv \frac{-3}{6} \equiv (-3) \cdot 6^{-1} \equiv 20 \cdot 4 \equiv 80 \equiv 11 \bmod 23$$

$$x_3 \equiv s^2 - x_1 - x_2 \bmod p \equiv 11^2 - 3 - 9 \equiv 209 \equiv 17 \bmod 23$$

$$y_3 \equiv s(x_1 - x_3) - y_1 \bmod p \equiv 11(3 - 17) - 10 \equiv -164 \equiv 20 \bmod 23$$

**Resultat:**  $(3; 10) + (9; 7) = (17; 20)$

3 P.

**Aufgabe 8****8 Punkte**

Alice schickt eine Meldung  $M \in \mathbb{Z}_{19}$  verschlüsselt an Bob. Es wird die Verschlüsselungsmethode von Volker-Müller mit Elliptischen Kurven eingesetzt. Aus gewissen Gründen wird die eigentliche Verschlüsselungsoperation ersetzt. Anstatt der XOR-Operation  $\oplus$  wird die Addition mod 19 verwendet. Bob hat die folgenden Elemente gewählt...

- ... die elliptische Kurve  $E: y^2 \equiv x^3 + 3x + 9$  über  $\mathbb{Z}_{19}$ .
- ... den Basispunkt  $P(2; 17)$ .
- ... den Secret Key  $d = 21$ .

Alice verschlüsselt die Nachricht  $M = 12$ . Sollte Alice einen zufälligen Wert generieren müssen, dann können Sie annehmen, dass der Wert 15 gewählt wird.

Alice beginnt den Datenaustausch mit der Meldung (\*) = „Hallo Bob, ich möchte dir eine verschlüsselte Meldung schicken.“

Füllen Sie nun die folgende Tabelle aus. Sollten es in der Tabelle zu wenig Platz für allfällige Berechnungen haben, so führen Sie diese bitte auf der nächsten Seite durch.

Sämtliche Operationen mit den Punkten können in der separat ausgeteilten Tabelle nachgeschaut werden.

Alice	unsichere Leitung	Bob
	(*) ----->	
	$K_{\text{pub}} = (p, a, b, q, P, Q)$ <-----	Bob schickt $K_{\text{pub}} = (p, a, b, q, P, Q)$
$K_{\text{pub}}$ in der vorgegebenen Reihenfolge angeben. $= (p, a, b, q, P, Q)$		
Verschlüsselt Meldung $M = 12$		
	Meldung notieren ----->	
		Entschlüsselung

Lösung:

Alice	unsichere Leitung	Bob
	(*) ----->	
	$K_{\text{pub}} = (p, a, b, q, P, Q)$ <-----	Bob schickt $K_{\text{pub}} = (p, a, b, q, P, Q)$
$K_{\text{pub}}$ in der vorgegebenen Reihenfolge angeben.  $= (p, a, b, q, P, Q)$  $(19, 3, 9, 23, (2; 17), (16; 12))$		
Verschlüsselt Meldung $M = 12$ $i = 15$ $K_E = i \cdot P = 15 \cdot (2; 17) = (12; 5)$ $K_M = i \cdot Q = 15 \cdot (16; 12) = (11; 9)$ $Y = M + x\text{Koord von } K_M \text{ mod } 19$ $= 12 + 11 \equiv 23 \equiv 4 \text{ mod } 19$		
	Alle nötigen Werte $(Y, K_E) = (4, (12; 5))$ ----->	
		$K_M = d \cdot K_E$  $= 21 \cdot (12; 5) = (11; 9)$  $M = Y - x\text{Koord } K_M \text{ mod } 19$ $= 4 - 11 \equiv -7 \equiv 12 \text{ mod } 19$

Bewertungshinweise:

- Q berechnen, 1 P.
- Angabe des korr.  $K_{\text{pub}}$  1 P.
- Verschlüsselung  $3 \cdot 1 = 3$  P.
- Korr. Meldung an Bob, 1 P.
- Entschlüsselung  $2 \cdot 1 = 2$  P.

**Aufgabe 9****5 Punkte**

Sie nutzen eine Sicherheitsapplikation, die Zertifikate für die Authentifizierung des Kommunikationspartners verwendet. Beim Versuch, sich mit einem neuen Partner zu verbinden, erhalten Sie eine Fehlermeldung, wonach das Root-CA-Zertifikat, das dem Zertifikat des Verbindungspartners zugrunde liegt, nicht vertrauenswürdig sei. Sie haben die Möglichkeit, den Verbindungsaufbau abubrechen oder das Root-CA-Zertifikat zu installieren. Die Sicherheitsapplikation zeigt Ihnen den Inhalt und weitere Eigenschaften des Root-CA-Zertifikats an. Sie entscheiden sich, das Root-CA-Zertifikat installieren.

- a) Was müssen Sie tun, bevor Sie das Zertifikat installieren. Beschreiben Sie den Vorgang stichwortartig (3 Punkte).
- b) Die oben beschriebene Fehlermeldung tritt glücklicherweise nur selten auf, weil die Prüfung des Zertifikats des Verbindungspartners in der Regel ohne Fehler durchgeführt werden kann. Beschreiben Sie in wenigen Worten, wie die Sicherheitsapplikation (oder das Betriebssystem) die Echtheit des Zertifikats des Verbindungspartners überprüft (1 Punkt). Welche Rolle spielt dabei der so genannte Trust Anchor (1 Punkt).

**Lösung:**

- a) Das Root-CA-Zertifikat muss auf Echtheit geprüft werden (1 Punkt). Die Echtheitsprüfung wird mithilfe des Fingerprints durchgeführt (1 Punkt). Bei der Überprüfung des Fingerprints wird der lokal angezeigte Fingerprint mit dem Fingerprint aus einer vertrauenswürdigen Referenzquelle verglichen (1 Punkt).
- b) Die Sicherheitsapplikation (oder das Betriebssystem) überprüft die Signatur auf dem Zertifikat des Verbindungspartners mithilfe des Zertifikats der herausgebenden Zertifizierungsstelle (Root-CA-Zertifikat) (1 Punkt). Die herausgebende Zertifizierungsstelle muss im System als vertrauenswürdige Root-CA hinterlegt sein; sie wird so zum Trust Anchor (1 Punkt).

**Anhang zur Aufgabe 8 (wird separat verteilt und muss resp. darf nicht abgegeben werden)**

<b>P(0; 3)</b>		<b>P(0; 16)</b>		<b>P(2; 2)</b>		<b>P(2; 17)</b>
1·P = (0; 3)		1·P = (0; 16)		1·P = (2; 2)		1·P = (2; 17)
2·P = (5; 4)		2·P = (5; 15)		2·P = (16; 12)		2·P = (16; 7)
3·P = (11; 10)		3·P = (11; 9)		3·P = (5; 4)		3·P = (5; 15)
4·P = (15; 3)		4·P = (15; 16)		4·P = (4; 3)		4·P = (4; 16)
5·P = (4; 16)		5·P = (4; 3)		5·P = (18; 9)		5·P = (18; 10)
6·P = (3; 11)		6·P = (3; 8)		6·P = (15; 3)		6·P = (15; 16)
7·P = (2; 17)		7·P = (2; 2)		7·P = (11; 9)		7·P = (11; 10)
8·P = (9; 10)		8·P = (9; 9)		8·P = (12; 5)		8·P = (12; 14)
9·P = (16; 12)		9·P = (16; 7)		9·P = (3; 11)		9·P = (3; 8)
10·P = (12; 14)		10·P = (12; 5)		10·P = (0; 16)		10·P = (0; 3)
11·P = (18; 9)		11·P = (18; 10)		11·P = (9; 9)		11·P = (9; 10)
12·P = (18; 10)		12·P = (18; 9)		12·P = (9; 10)		12·P = (9; 9)
13·P = (12; 5)		13·P = (12; 14)		13·P = (0; 3)		13·P = (0; 16)
14·P = (16; 7)		14·P = (16; 12)		14·P = (3; 8)		14·P = (3; 11)
15·P = (9; 9)		15·P = (9; 10)		15·P = (12; 14)		15·P = (12; 5)
16·P = (2; 2)		16·P = (2; 17)		16·P = (11; 10)		16·P = (11; 9)
17·P = (3; 8)		17·P = (3; 11)		17·P = (15; 16)		17·P = (15; 3)
18·P = (4; 3)		18·P = (4; 16)		18·P = (18; 10)		18·P = (18; 9)
19·P = (15; 16)		19·P = (15; 3)		19·P = (4; 16)		19·P = (4; 3)
20·P = (11; 9)		20·P = (11; 10)		20·P = (5; 15)		20·P = (5; 4)
21·P = (5; 15)		21·P = (5; 4)		21·P = (16; 7)		21·P = (16; 12)
22·P = (0; 16)		22·P = (0; 3)		22·P = (2; 17)		22·P = (2; 2)
23·P = $\emptyset$		23·P = $\emptyset$		23·P = $\emptyset$		23·P = $\emptyset$

<b>P(3; 8)</b>		<b>P(3; 11)</b>		<b>P(4; 3)</b>		<b>P(4; 16)</b>
1·P = (3; 8)		1·P = (3; 11)		1·P = (4; 3)		1·P = (4; 16)
2·P = (18; 9)		2·P = (18; 10)		2·P = (12; 5)		2·P = (12; 14)
3·P = (4; 16)		3·P = (4; 3)		3·P = (9; 10)		3·P = (9; 9)
4·P = (0; 16)		4·P = (0; 3)		4·P = (11; 10)		4·P = (11; 9)
5·P = (2; 2)		5·P = (2; 17)		5·P = (5; 15)		5·P = (5; 4)
6·P = (12; 14)		6·P = (12; 5)		6·P = (2; 2)		6·P = (2; 17)
7·P = (15; 3)		7·P = (15; 16)		7·P = (18; 9)		7·P = (18; 10)
8·P = (5; 15)		8·P = (5; 4)		8·P = (3; 11)		8·P = (3; 8)
9·P = (9; 9)		9·P = (9; 10)		9·P = (0; 3)		9·P = (0; 16)
10·P = (16; 12)		10·P = (16; 7)		10·P = (15; 16)		10·P = (15; 3)
11·P = (11; 10)		11·P = (11; 9)		11·P = (16; 7)		11·P = (16; 12)
12·P = (11; 9)		12·P = (11; 10)		12·P = (16; 12)		12·P = (16; 7)
13·P = (16; 7)		13·P = (16; 12)		13·P = (15; 3)		13·P = (15; 16)
14·P = (9; 10)		14·P = (9; 9)		14·P = (0; 16)		14·P = (0; 3)
15·P = (5; 4)		15·P = (5; 15)		15·P = (3; 8)		15·P = (3; 11)
16·P = (15; 16)		16·P = (15; 3)		16·P = (18; 10)		16·P = (18; 9)
17·P = (12; 5)		17·P = (12; 14)		17·P = (2; 17)		17·P = (2; 2)
18·P = (2; 17)		18·P = (2; 2)		18·P = (5; 4)		18·P = (5; 15)
19·P = (0; 3)		19·P = (0; 16)		19·P = (11; 9)		19·P = (11; 10)
20·P = (4; 3)		20·P = (4; 16)		20·P = (9; 9)		20·P = (9; 10)
21·P = (18; 10)		21·P = (18; 9)		21·P = (12; 14)		21·P = (12; 5)
22·P = (3; 11)		22·P = (3; 8)		22·P = (4; 16)		22·P = (4; 3)
23·P = $\emptyset$		23·P = $\emptyset$		23·P = $\emptyset$		23·P = $\emptyset$



P(5; 4)		P(5; 15)		P(9; 9)		P(9; 10)
1·P = (5; 4)		1·P = (5; 15)		1·P = (9; 9)		1·P = (9; 10)
2·P = (15; 3)		2·P = (15; 16)		2·P = (2; 17)		2·P = (2; 2)
3·P = (3; 11)		3·P = (3; 8)		3·P = (0; 16)		3·P = (0; 3)
4·P = (9; 10)		4·P = (9; 9)		4·P = (16; 7)		4·P = (16; 12)
5·P = (12; 14)		5·P = (12; 5)		5·P = (3; 11)		5·P = (3; 8)
6·P = (18; 10)		6·P = (18; 9)		6·P = (5; 15)		6·P = (5; 4)
7·P = (16; 7)		7·P = (16; 12)		7·P = (12; 5)		7·P = (12; 14)
8·P = (2; 2)		8·P = (2; 17)		8·P = (4; 16)		8·P = (4; 3)
9·P = (4; 3)		9·P = (4; 16)		9·P = (11; 9)		9·P = (11; 10)
10·P = (11; 9)		10·P = (11; 10)		10·P = (18; 10)		10·P = (18; 9)
11·P = (0; 16)		11·P = (0; 3)		11·P = (15; 3)		11·P = (15; 16)
12·P = (0; 3)		12·P = (0; 16)		12·P = (15; 16)		12·P = (15; 3)
13·P = (11; 10)		13·P = (11; 9)		13·P = (18; 9)		13·P = (18; 10)
14·P = (4; 16)		14·P = (4; 3)		14·P = (11; 10)		14·P = (11; 9)
15·P = (2; 17)		15·P = (2; 2)		15·P = (4; 3)		15·P = (4; 16)
16·P = (16; 12)		16·P = (16; 7)		16·P = (12; 14)		16·P = (12; 5)
17·P = (18; 9)		17·P = (18; 10)		17·P = (5; 4)		17·P = (5; 15)
18·P = (12; 5)		18·P = (12; 14)		18·P = (3; 8)		18·P = (3; 11)
19·P = (9; 9)		19·P = (9; 10)		19·P = (16; 12)		19·P = (16; 7)
20·P = (3; 8)		20·P = (3; 11)		20·P = (0; 3)		20·P = (0; 16)
21·P = (15; 16)		21·P = (15; 3)		21·P = (2; 2)		21·P = (2; 17)
22·P = (5; 15)		22·P = (5; 4)		22·P = (9; 10)		22·P = (9; 9)
23·P = $\emptyset$		23·P = $\emptyset$		23·P = $\emptyset$		23·P = $\emptyset$

P(11; 9)		P(11; 10)		P(12; 5)		P(12; 14)
1·P = (11; 9)		1·P = (11; 10)		1·P = (12; 5)		1·P = (12; 14)
2·P = (3; 8)		2·P = (3; 11)		2·P = (11; 10)		2·P = (11; 9)
3·P = (16; 7)		3·P = (16; 12)		3·P = (2; 2)		3·P = (2; 17)
4·P = (18; 9)		4·P = (18; 10)		4·P = (3; 11)		4·P = (3; 8)
5·P = (9; 10)		5·P = (9; 9)		5·P = (15; 16)		5·P = (15; 3)
6·P = (4; 16)		6·P = (4; 3)		6·P = (16; 12)		6·P = (16; 7)
7·P = (5; 4)		7·P = (5; 15)		7·P = (0; 16)		7·P = (0; 3)
8·P = (0; 16)		8·P = (0; 3)		8·P = (18; 10)		8·P = (18; 9)
9·P = (15; 16)		9·P = (15; 3)		9·P = (5; 4)		9·P = (5; 15)
10·P = (2; 2)		10·P = (2; 17)		10·P = (9; 9)		10·P = (9; 10)
11·P = (12; 5)		11·P = (12; 14)		11·P = (4; 16)		11·P = (4; 3)
12·P = (12; 14)		12·P = (12; 5)		12·P = (4; 3)		12·P = (4; 16)
13·P = (2; 17)		13·P = (2; 2)		13·P = (9; 10)		13·P = (9; 9)
14·P = (15; 3)		14·P = (15; 16)		14·P = (5; 15)		14·P = (5; 4)
15·P = (0; 3)		15·P = (0; 16)		15·P = (18; 9)		15·P = (18; 10)
16·P = (5; 15)		16·P = (5; 4)		16·P = (0; 3)		16·P = (0; 16)
17·P = (4; 3)		17·P = (4; 16)		17·P = (16; 7)		17·P = (16; 12)
18·P = (9; 9)		18·P = (9; 10)		18·P = (15; 3)		18·P = (15; 16)
19·P = (18; 10)		19·P = (18; 9)		19·P = (3; 8)		19·P = (3; 11)
20·P = (16; 12)		20·P = (16; 7)		20·P = (2; 17)		20·P = (2; 2)
21·P = (3; 11)		21·P = (3; 8)		21·P = (11; 9)		21·P = (11; 10)
22·P = (11; 10)		22·P = (11; 9)		22·P = (12; 14)		22·P = (12; 5)
23·P = $\emptyset$		23·P = $\emptyset$		23·P = $\emptyset$		23·P = $\emptyset$

P(15; 3)		P(15; 16)		P(16; 7)		P(16; 12)
1·P = (15; 3)		1·P = (15; 16)		1·P = (16; 7)		1·P = (16; 12)
2·P = (9; 10)		2·P = (9; 9)		2·P = (4; 16)		2·P = (4; 3)
3·P = (18; 10)		3·P = (18; 9)		3·P = (15; 16)		3·P = (15; 3)
4·P = (2; 2)		4·P = (2; 17)		4·P = (12; 14)		4·P = (12; 5)
5·P = (11; 9)		5·P = (11; 10)		5·P = (0; 3)		5·P = (0; 16)
6·P = (0; 3)		6·P = (0; 16)		6·P = (9; 9)		6·P = (9; 10)
7·P = (4; 16)		7·P = (4; 3)		7·P = (3; 11)		7·P = (3; 8)
8·P = (16; 12)		8·P = (16; 7)		8·P = (11; 9)		8·P = (11; 10)
9·P = (12; 5)		9·P = (12; 14)		9·P = (18; 9)		9·P = (18; 10)
10·P = (3; 8)		10·P = (3; 11)		10·P = (5; 4)		10·P = (5; 15)
11·P = (5; 15)		11·P = (5; 4)		11·P = (2; 2)		11·P = (2; 17)
12·P = (5; 4)		12·P = (5; 15)		12·P = (2; 17)		12·P = (2; 2)
13·P = (3; 11)		13·P = (3; 8)		13·P = (5; 15)		13·P = (5; 4)
14·P = (12; 14)		14·P = (12; 5)		14·P = (18; 10)		14·P = (18; 9)
15·P = (16; 7)		15·P = (16; 12)		15·P = (11; 10)		15·P = (11; 9)
16·P = (4; 3)		16·P = (4; 16)		16·P = (3; 8)		16·P = (3; 11)
17·P = (0; 16)		17·P = (0; 3)		17·P = (9; 10)		17·P = (9; 9)
18·P = (11; 10)		18·P = (11; 9)		18·P = (0; 16)		18·P = (0; 3)
19·P = (2; 17)		19·P = (2; 2)		19·P = (12; 5)		19·P = (12; 14)
20·P = (18; 9)		20·P = (18; 10)		20·P = (15; 3)		20·P = (15; 16)
21·P = (9; 9)		21·P = (9; 10)		21·P = (4; 3)		21·P = (4; 16)
22·P = (15; 16)		22·P = (15; 3)		22·P = (16; 12)		22·P = (16; 7)
23·P = $\emptyset$		23·P = $\emptyset$		23·P = $\emptyset$		23·P = $\emptyset$

P(18; 9)		P(18; 10)				
1·P = (18; 9)		1·P = (18; 10)				
2·P = (0; 16)		2·P = (0; 3)				
3·P = (12; 14)		3·P = (12; 5)				
4·P = (5; 15)		4·P = (5; 4)				
5·P = (16; 12)		5·P = (16; 7)				
6·P = (11; 9)		6·P = (11; 10)				
7·P = (9; 10)		7·P = (9; 9)				
8·P = (15; 16)		8·P = (15; 3)				
9·P = (2; 17)		9·P = (2; 2)				
10·P = (4; 3)		10·P = (4; 16)				
11·P = (3; 11)		11·P = (3; 8)				
12·P = (3; 8)		12·P = (3; 11)				
13·P = (4; 16)		13·P = (4; 3)				
14·P = (2; 2)		14·P = (2; 17)				
15·P = (15; 3)		15·P = (15; 16)				
16·P = (9; 9)		16·P = (9; 10)				
17·P = (11; 10)		17·P = (11; 9)				
18·P = (16; 7)		18·P = (16; 12)				
19·P = (5; 4)		19·P = (5; 15)				
20·P = (12; 5)		20·P = (12; 14)				
21·P = (0; 3)		21·P = (0; 16)				
22·P = (18; 10)		22·P = (18; 9)				
23·P = $\emptyset$		23·P = $\emptyset$				