

\int Skripte **HSLU** Hochschule Luzern

Modul I.BA_KRYPT

Musterprüfung/Kompetenznachweis 1

Datum, Zeit und Ort

Name: Musterlösung

Bedingungen (für die Prüfung):

Zeit: 90 Minuten
Hilfsmittel: Beliebige schriftliche Unterlagen (Open book), ein beliebiger nicht kommunikatonsfähiger 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 Zusatzblätter benutzen.
- Lesen Sie zuerst die Aufgaben, bevor Sie zu lösen anfangen!
- Saubere und deutliche Resultatformulierung.
- Unbelegte oder nicht nachvollziehbare Resultate werden nicht berücksichtigt.
- Ungültiges ist sauber durchzustreichen, Mehrfachlösungen werden nicht gewertet.
- Der Lösungsweg muss klar ersichtlich sein.
- Rechenaufgaben werden mit dem Unterstreichen des Resultates beendet.
- Zu Textaufgaben gehört am Schluss ein Resultatsatz in Prosa.
- Dort wo offene Stellen auszufüllen sind, sind nur diese offenen Stellen auszufüllen.
- 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 Aufgabe 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)	7		
2)	7		
3)	5		
4)	7		
5)	5		
6)	7		
7)	14		
8)	4		
9)	3		
	-----		Note
Total	60		
	=====	=====	

Notenskala:

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**7 Punkte****Aufgabe 1.1**

Sie setzen einen 128-Bit Blockchiffre-Algorithmus ein. Nun wird eine neue Version veröffentlicht; diese Version hat ebenfalls eine Schlüsselgrösse von 128 Bit, aber anstatt 128 Bit Input- und Outputgrösse hat sie neu 192 Bit Input- und Outputgrösse.

- a) [1 P.] Welche der zwei Brute-Force Attacks wird/werden nun aufwändiger?
- b) [3 P.] Um welchen Faktor wird/werden die Attacke(n) nun schwieriger?

Lösung:

- a) Es wird nur der Table Look up Angriff erschwert.
- b) Speicherbedarf allgemein: Sei n = Anzahl Schlüsselbits und m = die Anzahl der Input- resp. Outputbits

$$\text{Speicherplatz} = m \cdot 2^n$$

Somit ist der Erschwernisfaktor $= \frac{192 \cdot 2^{128}}{128 \cdot 2^{128}} = 1,5$; oder ein zusätzlicher Speicheraufwand von 50%.

Aufgabe 1.2

[3 P.] Ein CH-Sicherheitsexperte hat in einem Zeitungsinterview den folgenden Ratschlag zur Verschlüsselung von Bankdaten formuliert:

„.... die Bankdaten sollten in einzelne Gruppen zusammengefasst sein, die jede mit einem anderen Verfahren und einem unterschiedlichen digitalen Schlüssel verschlüsselt werden. Diese verschlüsselten Gruppen sollten dann komprimiert und nochmals verschlüsselt werden, wiederum mit einem anderen Verschlüsselungsverfahren und einem weiteren digitalen Schlüssel.....“.

Kommentieren Sie diesen Ratschlag.

Lösung:





- 1) Es gibt keinen Grund Gruppen zu bilden und mit verschiedenen Schlüsseln zu arbeiten.
- 2) Es ist ziemlich nutzlos, verschlüsselte Daten zu komprimieren, es gibt weder eine grössere Sicherheit, noch spart man Platz. (Bemerkung: Einzig vor dem Verschlüsseln würde eine Komprimierung eine Platzersparnis bringen).
- 3) Kaskaden von Verschlüsselungen sind mit AES nicht mehr nötig.
- 4) Key Management wird komplizierter.

Bewertungshinweis:

























Es genügen 3 von diesen 4 Argumenten.

Aufgabe 2**7 Punkte**

- a) [4 P.] Welche Bits sind nach dem untenstehenden Austausch bei Alice und Bob identisch?
Alice und Bob machen folgende Codierung miteinander ab:

			
0	1	1	0

Alice schickt folgende Sequenz und wählt dabei die untenstehenden Filter:

Zufälliges Photon								
Polarisierung von Alice								
Zwischenlinie für eigene Notizen.	1	1	0	1	1	0	1	0
Bobs Wahl der Filter								
Zwischenlinie für eigene Notizen.								
Gemeinsamer Schlüssel von Alice und Bob	-	1	-	1	1	0	-	0

Bewertungshinweis:

➤ Pro falsche Position, 1½ Pte Abzug.

- b) [3 P.] Sie müssen für einen SHA-384 einen 384 Bit Schlüssel mit dem obigen Verfahren austauschen. Erklären Sie wie viele Schlüsselbit Sie austauschen müssen, und wie, warum und wie viele Sie „verlieren“.

Lösung:

[1 P.] Ca. Faktor 4 Mal mehr, also ca. 1536 Bit.

[1 P.] Ca. die Hälfte verliert man, weil der falsche Filter verwendet wurde. Somit bleiben noch 768 übrig.

[1 P.] Davon braucht man die Hälfte, die man aufdeckt, um zu bemerken, ob man abgehört wurde.

Aufgabe 3**5 Punkte**

Folgendes Protokoll wird publiziert.

Abkürzungen:

ID_A = Identifikationsnummer von A (z.B. IP-Adresse).

ID_B = Identifikationsnummer von B (z.B. IP-Adresse).

N_A = 256 Bit Zufallszahl von A generiert.

N_B = 256 Zufallszahl von B generiert.

$Hash_{AB}$ = Hashwert mit SHA-256 über die Inhalte in der Klammer von A (für B).

$Hash_{BA}$ = Hashwert mit SHA-256 über die Inhalte in der Klammer von B (für A).

NR	Teilnehmer A	Meldung	Teilnehmer B
1)	Generiert zufällig N_A		
2)		ID_A, N_A ----->	
3)			Generiert zufällig N_B und schickt $Hash_{BA}(..)$
4)		$N_B, Hash_{BA}(N_A, N_B, ID_B)$ -----<	
5)	Verifiziert $Hash_{BA}(..)$ und gene- riert und schickt $Hash_{AB}(..)$.		
6)		$Hash_{AB}(N_A, N_B)$ ----->	
7)			Verifiziert $Hash_{AB}(..)$

a) [2 P.] Für was **sollte** dieses Verfahren am ehesten dienen? Kreuzen Sie entsprechend an. Falsches Ankreuzen gibt **Punktabzug**, die Summe kann aber nicht negativ werden.

- ☐ Einseitige Authentisierung gewähren
- ☐ Vertraulichkeit/Geheimhaltung gewähren
- ☐ Non repudiation of receipt erreichen
- ☐ Integrität gewähren
- ☐ Nicht-Abstreitbarkeit des Ursprungs erreichen
- ☒ Gegenseitige Authentisierung erwirken

b) [3 P.] Kommentieren Sie die Wirksamkeit gegen den/die geplanten Angriffe.

Lösung:

Im Hash ist kein Geheimnis drin, somit kann alles auch von Eve berechnet werden und ist somit absolut sinnlos.

Aufgabe 4**8 Punkte**

Eine Codebook Analyse hat nicht das Auffinden des unbekannten Schlüssels zum Ziel, sondern die direkte Rekonstruktion des Klartextes.

Der Ablauf geht wie folgt:

- Man berechnet eine (unter Umständen grosse) Anzahl von Chiffretextblöcken aus „sinnvollen“ Klartextblöcken, unter Anwendung des unbekannten Schlüssels.
- Speicherung der Klartext/Chiffretext-Paare (Aufbau des Codebuchs).
- Vergleich des abgehörten Chiffretextes mit den gespeicherten Paaren.

a) [2 P.] Um was für einen Typ von Attacke handelt es sich hier? Kreuzen Sie entsprechend an. Falsches Ankreuzen gibt **Punktabzug**, die Summe kann aber nicht negativ werden.

- ☐ Ciphertext-only Attacke
☐ Known-plaintext Attacke
☒ Chosen-plaintext Attacke
☐ Chosen-ciphertext Attacke

b) [6 P.] Gegeben ist ein 64-Bit PIN-Block der folgenden Form.

	PIN-Länge	PIN	Padding
1	6	PPPPPP	32 Zufallsbit

- Im ersten Halbbyte steht fix eine „1“
- Im zweiten Halbbyte steht fix eine „6“
- Im dritten bis achten Halbbyte stehen je eine Ziffer von 0, ..., 9
- In den letzten 8 Halbbytes stehen insgesamt 32 Zufallsbits.

Geben Sie die Grösse des Codebooks in Anzahl Harddisks von 10 TerraByte an.

Lösung:

Die Entropie der ersten zwei Halbbytes ist je Null: 1 P.

Die Entropie der 6 Ziffern ist $6 \cdot 3,3 \text{ Bits} = \text{ca. } 20 \text{ Bits}$. 1 P.

Die Entropie der 32 Zufallsbits beträgt 32 Bit. 1 P.

Somit müssen $2^{32+20} = 2^{52}$ Blöcke à 64 Bit gespeichert werden. 1 P.

$$\text{Anzahl Terabyte} = \frac{64 \cdot 2^{52}}{8 \cdot 2^{40}} = 8 \cdot 2^{12} = 2^{15} = 32'768 \quad 1 \text{ P.}$$

Resultat: Somit braucht es ca. 3'300 HD à 10 TByte. 1 P.

Aufgabe 5**5 Punkte**

Gegeben sind einige Algorithmen (Alg). Kreuzen Sie die richtige(n) Antwort(en) an. In der Spalte „Verfahren“ ist nur eine Antwort anzukreuzen. In der Spalte „Geeignet...“ sind mehrere Antworten möglich. Falsch angekreuzte Aussagen ergeben einen Punkteabzug, die Summe kann aber nicht negativ werden.

Alg.	Verfahren	Geeignet
RSA	<input type="checkbox"/> Symmetrisches <input checked="" type="checkbox"/> Asymmetrisches <input type="checkbox"/> Weder noch	<input type="checkbox"/> <u>nur</u> um Schlüssel auszutauschen <input type="checkbox"/> zum Berechnen eines CBC-MAC <input type="checkbox"/> <u>nur</u> zur gegenseitigen Authentisierung <input checked="" type="checkbox"/> zum Berechnen einer digitalen Signatur <input checked="" type="checkbox"/> zum Verschlüsseln <input type="checkbox"/> passt nicht in dieses Schema
AES	<input checked="" type="checkbox"/> Symmetrisches <input type="checkbox"/> Asymmetrisches <input type="checkbox"/> Weder noch	<input type="checkbox"/> <u>nur</u> um Schlüssel auszutauschen <input checked="" type="checkbox"/> zum Berechnen eines CBC-MAC <input type="checkbox"/> <u>nur</u> zur gegenseitigen Authentisierung <input type="checkbox"/> zum Berechnen einer digitalen Signatur <input checked="" type="checkbox"/> zum Verschlüsseln <input type="checkbox"/> passt nicht in dieses Schema
Diffie-Hellman	<input type="checkbox"/> Symmetrisches <input checked="" type="checkbox"/> Asymmetrisches <input type="checkbox"/> Weder noch	<input checked="" type="checkbox"/> <u>nur</u> um Schlüssel auszutauschen <input type="checkbox"/> zum Berechnen eines CBC-MAC <input type="checkbox"/> <u>nur</u> zur gegenseitigen Authentisierung <input type="checkbox"/> zum Berechnen einer digitalen Signatur <input type="checkbox"/> zum Verschlüsseln <input type="checkbox"/> passt nicht in dieses Schema
SHA-1	<input type="checkbox"/> Symmetrisches <input type="checkbox"/> Asymmetrisch <input checked="" type="checkbox"/> Weder noch	<input type="checkbox"/> <u>nur</u> um Schlüssel auszutauschen <input type="checkbox"/> zum Berechnen eines CBC-MAC <input type="checkbox"/> <u>nur</u> zur gegenseitigen Authentisierung <input type="checkbox"/> zum Berechnen einer digitalen Signatur <input type="checkbox"/> zum Verschlüsseln <input checked="" type="checkbox"/> passt nicht in dieses Schema

Bewertungshinweis:

- Pro richtiges Kreuz ½ Punkte, pro falsches ¼ Punkte Abzug.

Aufgabe 6**7 Punkte**

Um eine Doppelunterschrift zu implementieren wird der geheime Exponent $d = 59$ und der dazugehörige öffentliche Schlüssel ($e = 11$, $N = 91$) erzeugt.

Der aufzuteilende Exponent wird in die zwei Teile $T_1 = 126$ und $T_2 = x$ additiv aufgeteilt.

Die zu signierende Nachricht $m = 12345678$, die Hashfunktion sei die Quersumme der Nachricht mod 10.

Wie lautet die Signatur mit dem Exponenten T_2 , und wie lautet die vollständige Signatur der Nachricht m resp. $h(m)$, wenn die Signatur mit dem Exponenten T_1 den Wert 64 hat?

Lösung:

Berechnung von $\varphi(N) = \varphi(91) = \varphi(7 \cdot 13) = (7-1)(13-1) = 6 \cdot 12 = 72$

1 P.

Berechnung von $T_2 = x$: $d = T_1 + T_2 \bmod \varphi(N)$, also $59 = 126 + x \bmod 72$, also $x = 59 - 126 \bmod 72 = -67 \bmod 72 = 5$.

3 P.

Berechnung von $h(m)$: Quersumme von $m = 36$, somit $h(m) = 36 \bmod 10 = 6$.

1 P.

Berechnung der zweiten Hälfte der Signatur: $(h(m))^{T_2} \bmod N = 6^5 \bmod 91 = 41$

1 P.

Berechnung der Signatur von $h(m) = 64 \cdot 41 \bmod 91 = 76$

1 P.

Resultat: Die Signatur lautet $s = 76$

Bemerkung:

- Die Verifikation der Signatur: $s^e \bmod 91 = 76^{11} \bmod 91 = 6$
- Die direkte Berechnung der Signatur lautet: $6^{59} \bmod 91 = 76$

Bewertungshinweis:

Die direkte Berechnung der Signatur mit einem Rechner gibt 1 Punkt.

Aufgabe 7**14 Punkte**

Gegeben ist die elliptische Kurve $E: y^2 \equiv x^3 + x + 1$ über \mathbb{Z}_{19}

- [2 P.] Überprüfen Sie, ob die Kurve eine elliptische Kurve ist.
- [2 P.] Liegt der Punkt $P(15; 16)$ auf der Kurve?
- [7 P.] Der Punkt $Q(5; 13)$ liegt auf der Kurve. Berechnen Sie nun die Koordinaten des Punktes $S = 3 \cdot Q$
- [1 P.] Der Punkt $T(7; 3)$ liegt auf der Kurve. Bestimmen Sie die Koordinaten des Punktes $U = -T$.
- [2 P.] Die gegebene elliptische Kurve hat 21 Punkte. Überprüfen Sie, ob das stimmen kann.

Falls es Ihnen hilft, dürfen Sie die Kehrwerttabelle mod 19 im Folgenden verwenden.

x	1	2	3	4	5	6	7	8	9	10
$x^{-1} \bmod 19$	1	10	13	5	4	16	11	12	17	2

x	11	12	13	14	15	16	17	18
$x^{-1} \bmod 19$	7	8	3	15	14	6	9	18

Lösungen

- Die Nichtsingularitätsbedingung für $y^2 \equiv x^3 + a \cdot x + b \bmod p$ lautet:
 $4a^3 + 27b^2 \not\equiv 0 \bmod p$ ½ P.
 Für $a = 1$ und $b = 1$ bedeutet das: $4 \cdot 1^3 + 27 \cdot 1^2 = 31 \equiv 12 \bmod 19 \not\equiv 0 \bmod 19$ 1½ P.

- $P(15; 16)$ in die Gleichung einsetzen.

Der Punkt $P(15; 16)$ in $y^2 \equiv x^3 + x + 1 \bmod 19$ eingesetzt: $16^2 \equiv 15^3 + 1 \cdot 15 + 1 \bmod 19$

$$16^2 \equiv 256 \bmod 19 \equiv 9 \bmod 19 \text{ und } 15^3 + 1 \cdot 15 + 1 \equiv 3391 \bmod 19 \equiv 9 \bmod 19$$

1 P.

Resultat: Der Punkt $P(15; 16)$ liegt demnach auf der Kurve. 1 P.

- Koordinaten von Punkt $S = 3 \cdot Q = 2 \cdot Q + Q$. 1 P.

Für $2 \cdot Q(5; 13)$ gilt:

$$s \equiv \frac{3 \cdot x_1^2 + a}{2 \cdot y_1} \bmod p \equiv \frac{3 \cdot 5^2 + 1}{2 \cdot 13} \bmod 19 \equiv \frac{76}{26} \bmod 19 \equiv 76 \cdot 26^{-1} \bmod 19$$

$$\equiv (75 \bmod 19 \cdot 26^{-1} \bmod 19) \bmod 19 \equiv (0 \cdot (26^{-1} \bmod 19)) \bmod 19 \equiv 0$$

$$x_3 \equiv s^2 - x_1 - x_2 \bmod p \equiv 0^2 - 5 - 5 \bmod 19 \equiv -10 \bmod 19 = 9$$

$$y_3 \equiv s(x_1 - x_3) - y_1 \bmod p \equiv 0(5 - 9) - 13 \bmod 19 \equiv -13 \bmod 19 = 6$$

Also: $2 \cdot (5; 13) = (9; 6)$ 3 P.

Für $2 \cdot Q(5; 13) + Q(5; 13) = (9; 6) + (5; 13)$ gilt:

Detailberechnungen:

$$s \equiv \frac{y_2 - y_1}{x_2 - x_1} \mod p \equiv \frac{13 - 6}{5 - 9} \mod 19 \equiv \frac{7}{-4} \mod 19 \equiv \frac{7}{15} \mod 19 \equiv$$

$$\equiv (7 \cdot 15^{-1}) \mod 19 \equiv (7 \cdot 14) \mod 19 \equiv 98 \mod 19 = 3$$

$$x_3 \equiv s^2 - x_1 - x_2 \mod p \equiv 3^2 - 9 - 5 \mod 19 \equiv -5 \mod 19 \equiv 14$$

$$y_3 \equiv s(x_1 - x_3) - y_1 \mod p \equiv 3(9 - 14) - 6 \mod 19 \equiv -21 \mod 19 = 17$$

Resultat: $3Q(5; 13) = (14; 17)$

3 P.

d) $(7; 3) \rightarrow U = -T(7; -3)$

$$U(7; -3) = U(7; -3 \mod 19) = U(7; 16)$$

e) Mit dem Theorem von Hasse, kann die Anzahl der Kurvenpunkte abgeschätzt werden:

$$p + 1 - 2\sqrt{p} \leq |E| \leq p + 1 + 2\sqrt{p}$$

Für $p = 19$ ist das somit: $19 + 1 - 2\sqrt{19} \leq |E| \leq 19 + 1 + 2\sqrt{19}$, also: $12 \leq |E| \leq 28$

Resultat:

Eine Kurve mit mod 19 kann zwischen 12 und 28 Punkte haben, somit kann diese Anzahl (21 Kurvenpunkte) stimmen.

Bewertungshinweise:

- Rechenfehler werden mit 1 Punkt Abzug bewertet.
- Fehlende Interpretation, ½ P. Abzug.

Aufgabe 8:**4 Punkte**

Die Erstellung von digitalen Signaturen mithilfe von RSA erfolgt in zwei Schritten (=mathematische Operationen). Nennen Sie diese beiden Schritte (je 1 Punkt) und benennen Sie das Sicherheitsziel, das durch die Anwendung des jeweiligen Schrittes erreicht wird (je 1 Punkt).

	Mathematische Operation	Sicherheitsziel
1. Schritt		
2. Schritt		

Lösung:

	Mathematische Operation	Sicherheitsziel
1. Schritt	Berechnung des Hashwerts der Daten	Integrität
2. Schritt	Signatur des Hashwerts mit dem privaten Schlüssel des Signierers	Authentizität

Aufgabe 9:**3 Punkte**

Alice und Bob möchten untereinander verschlüsselte und signierte E-Mails austauschen. Beide haben sich deshalb Zertifikate einer öffentlichen Zertifizierungsstelle (z.B. SwissSign AG, QuoVadis Trustlink Schweiz AG etc.) beschafft, die sie nun einmalig gegenseitig als E-Mail-Anhang austauschen wollen. Es bieten sich ihnen hierzu 4 E-Mail-Versandoptionen entsprechend den möglichen Sicherheitszielen an. Wählen Sie die *minimal notwendige* Versandoption (1 Punkt) und begründen Sie, warum diese E-Mail-Versandoption ausreicht. (2 Punkte).

Versandoption	
«gewöhnliche» E-Mail	
Verschlüsselt	
Signiert	
Signiert und verschlüsselt	

Lösung:

Versandoption	
«gewöhnliche» E-Mail	x
Verschlüsselt	
Signiert	
Signiert und verschlüsselt	

Begründung: Zertifikate müssen nicht verschlüsselt verteilt werden, da sie öffentliche Schlüssel beinhalten und somit selber auch öffentlich sind (1 Punkt). Zertifikate müssen zudem auch nicht signiert verteilt werden, da sie von der Zertifizierungsstelle signiert sind, wodurch deren Authentizität sichergestellt ist (1 Punkt).