

\int Skripte **HSLU** Hochschule Luzern

Modul I.BA KRYPT

Musterprüfung/Kompetenznachweis 2

Datum, Zeit und Ort

Name: _____

Bedingungen (für die Prüfung):

Zeit: 90 Minuten
Hilfsmittel: Beliebige schriftliche Unterlagen (Open book), ein beliebiger **nicht kommunikat**
ionsfähiger 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:

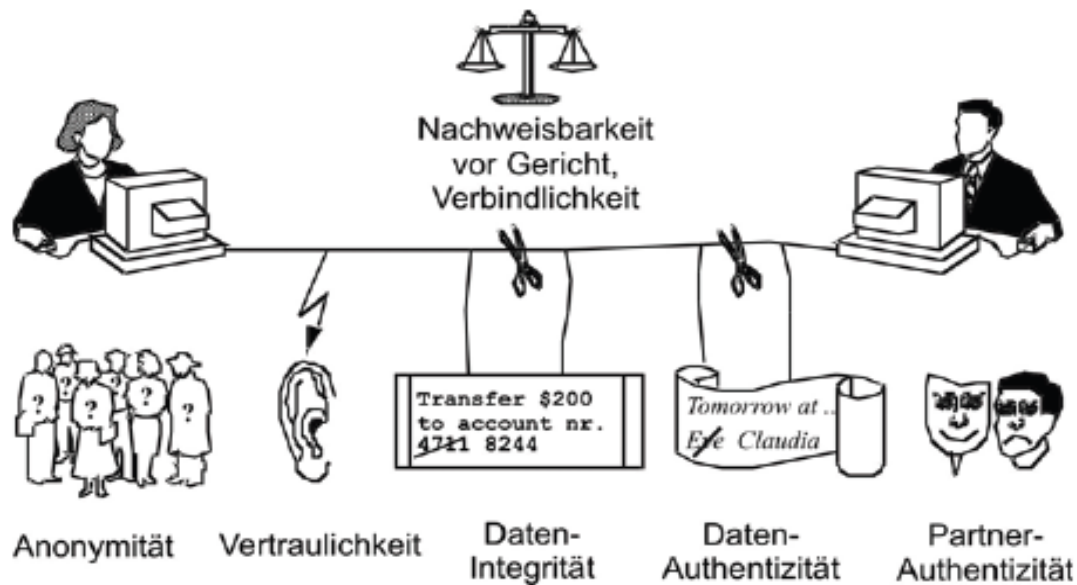
Aufgabe	Max. Punktzahl	Erreichte Punktzahl	
1)	8		
2)	5		
3)	6		
4)	4		
5)	4 + 4 = 8		
6)	6		
7)	4 + 10 = 14		
8)	4		
9)	5		
	-----		Note
Total	60		
	=====	=====	

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:**8 Punkte**

In einem Buch werden die folgenden Sicherheitsdienste in einer Zeichnung dargestellt. Leider wurden die Kryptographischen Mechanismen nicht mit eingezeichnet.

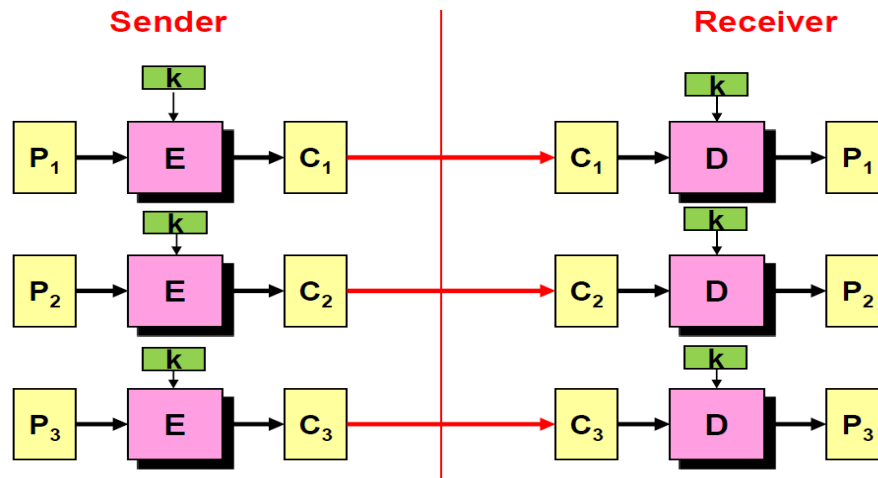


[8 P.] Kreuzen Sie alle korrekten Aussagen der Form „der gegebene Kryptographische Sicherheitsmechanismus kann Basis für den angekreuzten Sicherheitsdienst sein.“ **Falsches Ankreuzen wird mit Punktabzug versehen, die Summe kann nicht negativ werden.**

Sicherheitsdienst \ Krypt. Mechanismus	Vertraulichkeit	Datenintegrität	Partnerauthentizität	Keiner dieser Dienste
Sym. Verschlüsselung				
Asym. Verschlüsselung				
Diffie-Hellman Schlüsselaustausch Protokoll				
Hybride Verschlüsselung				
MAC- Berechnung				
Digitale Signatur				
C-R Protokoll mit MAC				
C-R Protokoll mit digitaler Signatur				

Aufgabe 2**5 Punkte**

Im Folgenden ist auf der Senderseite die Verschlüsselung der Klartextblöcke P_1 , P_2 und P_3 mit dem Schlüssel k in die Chiffretextblöcke C_1 , C_2 und C_3 und beim Receiver die Entschlüsselung abgebildet.



Kreuzen Sie nun alle richtigen Antworten an. **Falsches Ankreuzen wird mit Punktabzug versehen.** Die Summe kann aber nicht negativ werden.

5 P.

NR	Aufgabe	Auswahl
a)	Bei diesem Verfahren handelt es sich um ein...	<input type="checkbox"/> ... symmetrisches Verfahren <input type="checkbox"/> ... asymmetrisches Verfahren <input type="checkbox"/> ... hybrides Verfahren <input type="checkbox"/> Keine der Angaben ist zutreffend.
b)	Es handelt sich dabei um eine ...	<input type="checkbox"/> ... Hashfunktion <input type="checkbox"/> ... Blockchiffre <input type="checkbox"/> ... Stromchiffre <input type="checkbox"/> ... Public Key Verfahren <input type="checkbox"/> Keine der Angaben ist zutreffend.
c)	Als Algorithmen kommen z.B. folgende infrage.	<input type="checkbox"/> Diffie-Hellman <input type="checkbox"/> ECC <input type="checkbox"/> 3-DES <input type="checkbox"/> RSA <input type="checkbox"/> Hashfunktionen wie SHA-1 <input type="checkbox"/> Elliptische Kurven <input type="checkbox"/> AES <input type="checkbox"/> Keine der Angaben ist zutreffend.
d)	Das abgebildete Verfahren zeigt den folgenden Modus.	<input type="checkbox"/> CBC <input type="checkbox"/> OFB <input type="checkbox"/> CTR <input type="checkbox"/> ECB <input type="checkbox"/> Keine der Angaben ist zutreffend.

Aufgabe 3**6 Punkte**

Sie wollen einen 3072 Bit RSA einsetzen.





- a) [3 P.] Wie viele Dezimalstellen müssen die zu wählenden Primzahlen haben?
- b) [3 P.] Angenommen Sie bräuchten 400-stellige Primzahlen, wie viele davon gibt es?

Aufgabe 4**4 Punkte**

























Sie berechnen d^{116} mittels Square and Multiply (SaM). Schreiben Sie detailliert die einzelnen Schritte auf. Es ist nur die korrekte Reihenfolge der resultierenden Exponenten aufzuschreiben.

Aufgabe 5**4 + 4 = 8 Punkte****Aufgabe 5.1****4 Punkte**

[4 P.] Welchen Schlüssel können Alice und Bob nach dem untenstehenden Austausch verwenden? Alice und Bob machen folgende Codierung miteinander ab:

			
1	0	1	0

Alice schickt folgende Sequenz und wählt dabei die untenstehenden Filter:

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

Aufgabe 5.2**4 Punkte**

- [1 P.] Vergleichen Sie die klassische Sicherheit von einem 2048 Bit RSA und einer 384 Bit ECC.
- [3 P.] Vergleichen Sie die Sicherheit von einem 2048 Bit RSA und einer 384 Bit ECC, wenn es Quantencomputer mit genügend vielen Qubits gäbe.

Aufgabe 6**6 Punkte**

Im Folgenden ist das Protokoll einer blinden Signatur mit dem RSA gegeben.
 Füllen Sie die offenen Stellen aus.

Werte: (i) $p = 3, q = 11 \Rightarrow N = pq = 33$ und $\varphi(N) = (p - 1)(q - 1) = 20$
 (ii) $e = 3$, und damit ist $d = e^{-1} \bmod \varphi(N) = 3^{-1} \bmod 20 = 7$.

Kunde kennt den Public Key (_____)	Meldung	Bank kennt Secret Key (_____)
<u>1. Wahl der Nachricht m:</u> $m = 2$		
<u>2. Nachricht m „blinden“:</u> $r = 5$ $m' \equiv$ _____		
<u>3. geblindete Nachricht m' schicken:</u>	$m' =$ _____ ----->	
<u>4. Nachricht m' signieren:</u>		$s' \equiv$ _____
<u>5. Signatur s' zurückschicken:</u>	$s' =$ _____ <-----	
<u>6. Signatur s aus s' extrahieren:</u> $s \equiv$ _____		

7. Kontrolle mit Signatur s direkt rechnen:

Platz für Nebenrechnungen:

Aufgabe 7**14 Punkte****Aufgabe 7.1****4 Punkte**

Gegeben sind drei Gleichungen:

a) $E: y^2 \equiv x^3 + 3x + 6 \text{ über } \mathbb{Z}_{21}$

b) $E: y^2 \equiv x^3 + 3x + 10 \text{ über } \mathbb{Z}_{13}$

c) $E: y^2 \equiv x^3 + 4x + 2 \text{ über } \mathbb{Z}_{29}$

Begründen Sie welche dieser Gleichungen als Gleichung für eine elliptische Kurve dienen kann und welche nicht.

Aufgabe 7.2**10 Punkte**

Gegeben ist die elliptische Kurve $E: y^2 \equiv x^3 + 3x + 9$ über \mathbb{Z}_{19}

- [2 P.] Liegt der Punkt $B(15; 8)$ auf der Kurve?
- [7 P.] Von einem Punkt P , der auf der Kurve liegt kennt man die Koordinaten von $6 \cdot P = Q(15; 16)$ und $4 \cdot P = R(4; 16)$. Bestimmen Sie die Koordinaten des Punktes $S = 14 \cdot P$.
- [1 P.] Sie bestimmen alle Punkte der Kurve und kommen auf die Anzahl 32. Kann diese Zahl stimmen?

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

Aufgabe 8**4 Punkte**

Im folgenden Protokoll wird ein symmetrischer Schlüssel mittels einem Kurier auf zwei Rechenzentren verteilt (RZ₁ und RZ₂). Die Operation \oplus bedeutet die XOR-Operation.

RZ ₁	Kurier	RZ ₂
Erzeugt Schlüsselteil $T_1 = 6C$	T_1 in verschlossenem Couvert ----->	Unterschreibt, das Couvert in unbeschädigtem Zustand erhalten zu haben. Erzeugt Schlüsselteil $T_2 = 15$
	Bringt die Bestätigung zurück und T_2 in verschl. Couvert <-----	
Erzeugt Schlüsselteil $T_3 = A9$	T_3 in verschlossenem Couvert ----->	Unterschreibt, das Couvert in unbeschädigtem Zustand erhalten zu haben. Berechnet: Masterkey = $T_1 \oplus T_2 \oplus T_3$
	Bringt die Bestätigung zurück <-----	
Berechnet: Masterkey = $T_1 \oplus T_2 \oplus T_3$		

- a) [2 P.] Berechnen Sie den ausgetauschten Schlüssel = Masterkey = $T_1 \oplus T_2 \oplus T_3$
- b) [2 P.] Es gelang dem Kurier ein Couvert zu öffnen, den Teilschlüssel zu betrachten und das Couvert wieder so zu verschliessen, dass es wie unversehrt aussah. Den Teilschlüssel verkaufte er für viel Geld an die Mafia. Kann die Mafia mit diesem Teilschlüssel etwas über den Masterkey erfahren? Wenn ja, was und wie schlimm ist dieser Angriff?

Aufgabe 9**5 Punkte****Aufgabe 9.1:****2 Punkte**

Asymmetrische Schlüsselpaare können auf Smart-Cards berechnet werden. Technisch ist es dabei möglich sicherzustellen, dass der private Schlüssel nicht aus der Karte ausgelesen werden kann. Der private Schlüssel existiert in diesem Fall also ausschliesslich auf der Karte selber. Beantworten Sie zu diesem Szenario die folgende Frage:

Für welche kryptografische Operation (Verschlüsseln oder Signieren) sollten Sie das dem beschriebenen Szenario zugrundeliegende Schlüsselpaar *nicht* verwenden? (1 Punkt) Begründen Sie Ihre Antwort. (1 Punkt)

Aufgabe 9.2:**3 Punkte**

Welches grundsätzliche Problem ergibt sich bei der Anwendung von PKI-Verfahren, wenn aufgrund eines Software-Problems keine CRLs mehr ausgestellt werden können? (1 Punkt) Welche Sicherheitsprobleme entstehen dabei bei der Verschlüsselung von Daten? (1 Punkt) Und welche bei der Verifikation von Signaturen? (1 Punkt)