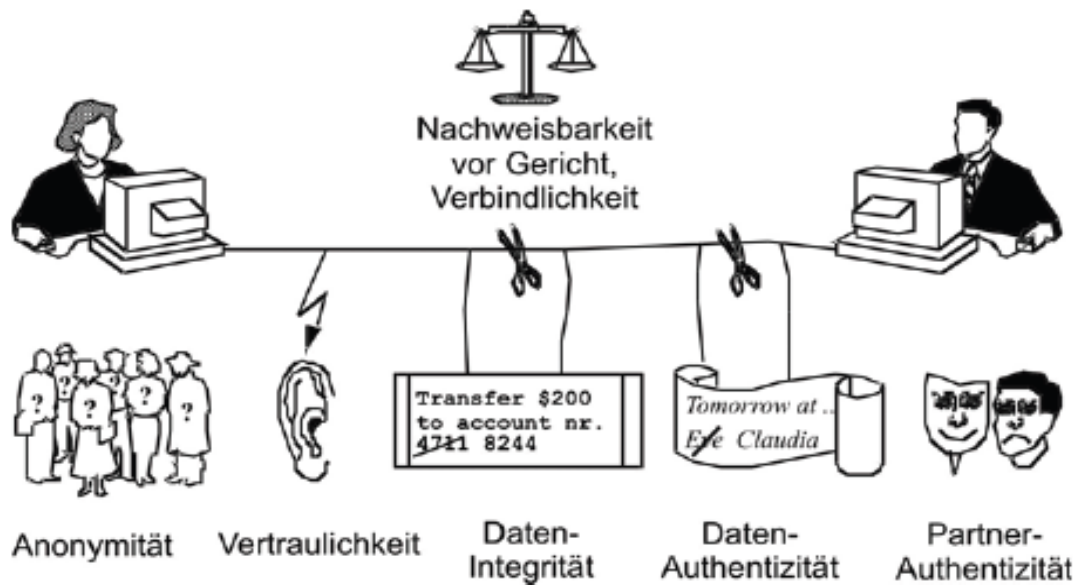


Aufgabe 1:**8 Punkte**

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

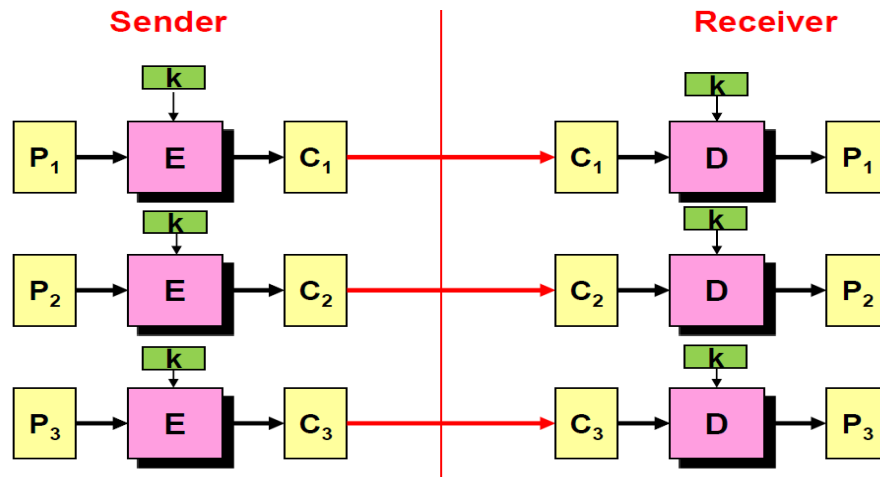


[8 P.] Kreuzen Sie alle korrekten Aussagen der Form „der gegebene Kryptographische Sicherheitsmechanismus kann Basis für den angekreuzten Sicherheitsdienst sein.“ **Falsches Ankreuzen wird mit Punktabzug versehen, die Summe kann nicht negativ werden.**

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

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 checked="" 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 checked="" 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 checked="" type="checkbox"/> 3-DES <input type="checkbox"/> RSA <input type="checkbox"/> Hashfunktionen wie SHA-1 <input type="checkbox"/> Elliptische Kurven <input checked="" 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 checked="" 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?

Lösung:

a) 3072 Bit bedeutet, dass $N = pq$ eine Zahl mit 3072 Bit ist, d.h. sie hat die Grösse 2^{3072}

$$2^{3072} = 2^{10 \cdot 307,2} = (2^{10})^{307,2} \approx (10^3)^{307,2} = 10^{3 \cdot 307,2} = 10^{921,6} \approx (10^{460})^2$$

1 P.

$$= 10^{460} \cdot 10^{460}$$

Somit muss p wie q je ungefähr 460-stellig sein.

2 P.

b) Ungefähr wie viele 400-stellige Primzahlen gibt es?

Die Eulersch'e Pi-Funktion $\pi(n) = \frac{n}{\ln(n)}$ gibt eine Abschätzung wie viele Primzahlen es von 1, bis n hat.

Somit gibt es ungefähr

$$\pi(n = 400) - \pi(n = 399) = \frac{10^{400}}{\ln(10^{400})} - \frac{10^{399}}{\ln(10^{399})} = \frac{10 \cdot 10^{399}}{400 \cdot \ln(10)} - \frac{10^{399}}{399 \cdot \ln(10)}$$

$$= 10^{399} \cdot \underbrace{\frac{1}{\ln(10)} \cdot \left(\frac{10}{400} - \frac{1}{399} \right)}_{\approx 1 \cdot 10^{-2}} \approx 10^{399} \cdot 10^{-2} = 10^{397}$$

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.

Lösung:

$$116_{10} = 1110100_2$$





1 P.

Im Detail:

























Zahl											
1	Nichts										
1		2	3								
1				6	7						
0						14					
1							28	29			
0									58		
0										116	

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

Bewertungshinweis: Pro falsche Position, 1½ Pte Abzug.

Aufgabe 5.2**4 Punkte**

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

Lösung:

- a) Ein 2048 Bit RSA hat in etwa die klassische Sicherheit eines 224 Bit ECC, resp. umgekehrt eine 384 Bit ECC hat in etwa die klassische Sicherheit eines 7680 Bit RSA.

b) Anzahl Qubit für das Faktorisieren: $K \approx 2k = 2 \cdot 2048 = 4096$ ½ P.

Anzahl Qubit für das ECC-Problem: 2 P.

$$K \approx 5k + 8\sqrt{k} + 5 \cdot \log_2 k = 5 \cdot 384 + 8 \cdot \sqrt{384} + 5 \cdot \log_2 384 \approx 2120$$

In Bezug auf die Quantencomputer ist ein 2048 Bit RSA sicherer als eine 384 Bit ECC. ½ P.

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:

Lösung:

Kunde kennt den Public Key (3, 33)	Meldung	Bank kennt Secret Key (3, 11, 7)
1. Wahl der Nachricht m: $m = 2$		
2. Nachricht m „blinden“: $r = 5$ $m' \equiv 5^3 \cdot 2 \bmod 33 \equiv 19$		
3. geblindete Nachricht m' schicken:	$m' = 19$ ----->	
4. Nachricht m' signieren:		$s' \equiv (19)^7 \bmod 33 \equiv 13$
5. Signatur s' zurückschicken:	$s' = 13$ <-----	
6. Signatur s aus s' extrahieren: $s \equiv \frac{13}{5} \equiv 13 \cdot 5^{-1} \equiv 13 \cdot 20 \equiv 29 \bmod 33$		

7. Kontrolle mit Signatur s direkt rechnen:

$$\underbrace{m^7 \equiv 2^7 \equiv 29 \bmod 33 = s}_{OK}$$

Bemerkung:

Der Kunde kann nun mit $(m, s) = (2, 29)$ im Shop einkaufen. Der Shopbesitzer will natürlich kontrollieren, ob das Geld echt ist und überprüft die Signatur

$$\underbrace{s^3 \equiv 29^3 \equiv 2 \bmod 33 = m}_{OK}$$

Bei der Einlieferung des Geldes bei der Bank, macht die Bank natürlich die gleiche Überprüfung der Signatur wie der Shopbesitzer.

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.

Lösung:

a) Kann keine Gleichung für eine elliptische Kurve sein, da der Modulus keine Primzahl ist.

[1 P.]

b) Die Nichtsingularitätsbedingung $4 \cdot 3^3 + 27 \cdot 10^2 \equiv 2808 \equiv 0 \text{ mod } 13$ ergibt Null, daher kann es keine Gleichung für eine elliptische Kurve sein.

[1½ P.]

c) Die Nichtsingularitätsbedingung $4 \cdot 4^3 + 27 \cdot 2^2 \equiv 364 \equiv 16 \text{ mod } 29 \not\equiv 0 \text{ mod } 29$, also kann sie Gleichung für eine elliptische Kurve sein.

[1½ P.]

Aufgabe 7.2**10 Punkte**

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

- a) [2 P.] Liegt der Punkt $B(15; 8)$ auf der Kurve?
 b) [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 $S = 14 \cdot P$.
 c) [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

Lösungen

- a) $P(15; 8)$ in die Gleichung einsetzen.

Der Punkt $P(15; 8)$ in $y^2 \equiv x^3 + 3x + 9 \bmod 19$ eingesetzt: $8^2 \equiv 15^3 + 3 \cdot 15 + 9 \bmod 19$

$$8^2 \equiv 64 \equiv 7 \bmod 19 \quad \text{und} \quad 15^3 + 3 \cdot 15 + 9 \equiv 3429 \equiv 9 \bmod 19 \quad 1\frac{1}{2} \text{ P.}$$

Resultat: Der Punkt $P(15; 8)$ liegt demnach **nicht** auf der Kurve. ½ P.

- b) Koordinaten von Punkt $S = 14 \cdot P = 8 \cdot P + 6 \cdot P = 2R + Q$. 1 P.

Für $2 \cdot R(4; 16)$ gilt:

$$s \equiv \frac{3 \cdot x_1^2 + a}{2 \cdot y_1} \bmod p \equiv \frac{3 \cdot 4^2 + 3}{2 \cdot 16} \bmod 19 \equiv \frac{51}{32} \bmod 19 \equiv \frac{13}{13} \bmod 19 \equiv 1$$

$$x_3 \equiv s^2 - x_1 - x_2 \bmod p \equiv 1^2 - 4 - 4 \bmod 19 \equiv -7 \bmod 19 \equiv 12$$

$$y_3 \equiv s(x_1 - x_3) - y_1 \bmod p \equiv 1(4 - 12) - 16 \bmod 19 \equiv 14$$

Also: $2 \cdot (4; 16) = (12; 14)$ 3 P.

Für $2 \cdot R(4; 16) + Q(15; 16) = (12; 14) + (15; 16)$ gilt

Detailberechnungen:

$$s \equiv \frac{y_2 - y_1}{x_2 - x_1} \bmod p \equiv \frac{16 - 14}{15 - 12} \bmod 19 \equiv \frac{2}{3} \bmod 19 \equiv (2 \cdot 3^{-1}) \bmod 19$$

$$\equiv (2 \bmod 19 \cdot 3^{-1} \bmod 19) \bmod 19 \equiv (2 \cdot 13) \bmod 19 \equiv 7 \quad (\text{siehe Tabelle})$$

$$x_3 \equiv s^2 - x_1 - x_2 \bmod p \equiv 7^2 - 15 - 12 \bmod 19 \equiv 22 \bmod 19 \equiv 3$$

$$y_3 \equiv s(x_1 - x_3) - y_1 \bmod p \equiv 7(12 - 3) - 14 \bmod 19 \equiv 49 \bmod 19 \equiv 11$$

Resultat: $(12; 14) + (15; 16) = 14 * P = (3; 11)$

3 P.

c) 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 $p = 23$ ist das somit: $19 + 1 - 2\sqrt{19} \leq |E| \leq 19 + 1 + 2\sqrt{19}$, also: $11 \leq |E| \leq 28$

Resultat:

Eine Kurve mit mod 23 kann zwischen 11 und 28 Punkte haben, somit kann diese Anzahl **nicht** stimmen.

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		

- [2 P.] Berechnen Sie den ausgetauschten Schlüssel = Masterkey = T₁ \oplus T₂ \oplus T₃
- [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?

Lösung:

a) Masterkey = T₁ \oplus T₂ \oplus T₃ = 6C \oplus 15 \oplus A9 = D0

- b) Es passiert nichts. Selbst wenn er zwei Couverts hätte öffnen können, hätte er keine Information über den Schlüssel. Dies selbst wenn er unendlich viele Computerressourcen zur Verfügung hätte. Er (oder die Mafia) hätte nicht Informationen, als sie durch raten erhalten würden, resp. nicht mehr als sie zum vorneherein schon wissen, nämlich der Masterkey **00** bis **FF** lauten muss.

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)

Lösung:

Das Schlüsselpaar sollte *nicht* für Verschlüsselungsoperationen verwendet werden. (1 Punkt)
Begründung: Wenn das Schlüsselpaar nur auf der Smart-Card existiert, dann gibt es kein Backup des privaten Schlüssels. Bei einem Schlüsselverlust sind deshalb die verschlüsselten Daten verloren. (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)

Lösung:

Das grundsätzliche Problem besteht darin, dass Zertifikate vor deren Verwendung von den Applikationen nicht mehr auf Gültigkeit hin geprüft werden können. (1 Punkt)

Wenn Zertifikate vor der Verschlüsselung von Daten nicht mehr auf Gültigkeit hin geprüft werden können, werden Daten möglicherweise für einen Angreifer verschlüsselt. (1 Punkt)

Wenn Zertifikate vor der Verifikation von Signaturen nicht mehr auf Gültigkeit hin geprüft werden können, können Signaturen, die von einem Angreifer erstellt worden sind, nicht mehr als gefälscht erkannt werden. (1 Punkt)