



15. Juli 2003

**Semestralklausur (Diplomklausur für FB18) zu
Public Key Infrastrukturen im SS03
Version A**

Name, Vorname:

Matrikelnummer: Fachbereich:

Aufbaustudium: Wiederholer(in): Fachsemester:

Unterschrift:

Hinweise:

1. Prüfen Sie, ob die Klausur alle 6 Aufgaben enthält.
2. Füllen Sie das Deckblatt vollständig aus.
3. Halten Sie ihren Studenausweis und einen Lichtbildausweis bereit.
4. Kennzeichnen Sie alle verwendeten Blätter zuerst mit Name und Matrikelnr.
5. Es sind die verwendeten Formeln und die Zwischenergebnisse anzugeben.
6. Markieren Sie auf dem Deckblatt die bearbeiteten Aufgaben.
7. Zum Bestehen der Prüfung ist es hinreichend 50 Punkte zu erreichen.
8. Ihnen stehen 90 min zum Bearbeiten der Aufgaben zur Verfügung.
9. Es sind keinerlei Hilfsmittel zugelassen.

Aufgabe	1	2	3	4	5	6
Punkte maximal	50	10	10	10	10	10
bearbeitet						
Punkte erreicht						

Aufgabe 1: Multiple Choice Aufgaben (50 Punkte)

Bei den folgenden Multiple-Choice-Aufgaben ist die Anzahl der möglichen korrekten Antworten nicht eingeschränkt. Das heißt: in jeder Aufgabe können null bis alle zur Auswahl stehenden Antworten korrekt sein. Geben sie ihre Antworten in den Kästchen links neben der entsprechenden Zeile. Korrekte Aussagen werden auf dem angekreuzt, inkorrekte Aussagen auf dem . Ein fehlendes Kreuz wird als falsch gesetztes Kreuz gewertet. Richtig gesetzte Kreuze geben Punkte, falsch gesetzte geben Punktabzug. Erhaltene Punkte und Punktabzüge werden innerhalb jeder Teilaufgabe verrechnet. Es ist nicht möglich negative Punkte aus einer Teilaufgabe "mitzunehmen".

a) Welche der folgenden Aussagen über das in der Vorlesung vorgestellte vereinfachte Schichtenmodell sind korrekt?

- Das vereinfachte Schichtenmodell hat 5 Schichten.
- Die Sicherungsschicht dient der kryptographischen Absicherung des Datenverkehrs.
- Jeder Knoten, über den ein IPsec-Paket läuft muss IPsec-spezifische Protokolldaten auswerten können.
- Kryptographische Absicherung auf der Anwendungsschicht ist möglich.
- Die kryptographische Absicherung einer Schicht sichert alle darüber liegenden Schichten vollständig ab.

b) Welche der im folgenden genannten Vertrauensmodelle unterstützt PGP?

- Direct Trust
- Hierarchical Trust
- Independent Trust
- User Trust
- Web of Trust

c) Grundsätzlich gilt in PGP:

- Teilnehmer können das Vertrauen in andere Teilnehmer frei wählen.
- Teilnehmer können Vertrauen anderer Teilnehmer übernehmen.
- Den Grad der Authentizität fremder Schlüssel stellt jeder Benutzer explizit selber ein.
- Teilnehmer können öffentliche Schlüssel signieren.
- Jeder Teilnehmer kann nur ein Schlüsselpaar besitzen.

d) Mit PGP können folgende Schutzziele direkt erreicht werden:

- Integrität
- Authentizität
- Verbindlichkeit
- Datiertheit
- Anonymität

e) Ihnen liegt ein selbst-signiertes Zertifikat vor. Weitere Informationen haben Sie nicht. Welche der folgenden Aussagen sind in dieser Situation *mit Sicherheit gültig*?

- Der Inhaber ist eine offizielle CA, der Sie vertrauen können.
- Der Aussteller ist eine offizielle CA, da Privatpersonen überhaupt keine selbst-signierte Zertifikate ausstellen können.
- Es kann sich nur um ein PGP-Zertifikat handeln. Bei X.509-Zertifikaten wird dieser Mechanismus nicht verwendet.
- Die Integrität des Zertifikats seit dem Signaturzeitpunkt ist garantiert.
- Die Authentizität des Zertifikats ist garantiert.

f) Für die Revokation eines Zertifikats gilt:

- Im Kettenmodell wirkt sie sich auf die Gültigkeit aller Signaturen aus, die von dem zugehörigen privaten Schlüssel *vorher* geleistet wurden.
- Sie kann aus verschiedenen Gründen erfolgen.
- Die dadurch entstehende Revokationsinformation (z.B. CRL) wird immer von dem Aussteller des revozierten Zertifikats unterschrieben.
- Wurde ein Schlüssel kompromittiert, verhindert die Revokation im *erweiterten Schalenmodell*, dass gefälschte Signaturen erstellt werden können, die auch nach der Revokation noch als gültig gelten.
- Sie gilt ab dem Zeitpunkt, an dem der Vorfall, der zur Revokation geführt hat, stattgefunden hat.

g) Welche der folgenden Aussagen sind richtig für eine PKI, deren Zertifikate dem X.509 Standard genügen?

- Jedes aktive Trust-Center ist auch eine Wurzelinstanz.
- Jedes aktive Trust-Center muss wenigstens ein eigenes gültiges Schlüssel-paar haben, das von einer Wurzelinstanz zertifiziert ist.
- Jedes aktive Trust-Center muss wenigsten ein eigenes Schlüsselpaar besitzen, dessen Gültigkeit über eine Zertifikatskette auf eine Wurzelinstanz zurückgeführt werden kann.
- Jedes aktive Trust-Center muss eine gültige Revokationsliste bereitstellen.
- Jedes aktive Trust-Center muss Key-Backup für die Verschlüsselungs-Schlüssel seiner Teilnehmer betreiben.

h) Welche der folgenden Attribute müssen in einem X.509 Zertifikat vorhanden sein?

- Zertifikatsseriennummer
- IssuerDN (Name des Ausstellers)
- Key Usage
- CRL Distributions Point
- Production Time

- i) Welches sind die Vorteile von symmetrischen Verschlüsselungsverfahren gegenüber asymmetrischen?
- Der Schlüsselaustausch ist einfacher.
 - Alle Nachrichten für einen Empfänger werden mit dem gleichen Schlüssel verschlüsselt, unabhängig davon wer sie schickt.
 - Die Verschlüsselung ist schneller.
 - Sie sind sicherer.
 - Sie können auch zur Signatur von Dokumenten eingesetzt werden.
- j) Sie wollen mittels PKI-Techniken eine verschlüsselte und signierte E-Mail verschicken. Welche Schlüssel benötigen Sie dafür?
- Den Private-Key des Senders.
 - Den Public-Key des Senders.
 - Den Private-Key des Empfängers.
 - Den Public-Key des Empfängers.
 - Den Public-Key des Trust-Centers.

Lösungsvorschlag

- a) Welche der folgenden Aussagen über das in der Vorlesung vorgestellte vereinfachte Schichtenmodell sind korrekt?
- Das vereinfachte Schichtenmodell hat 5 Schichten.
 - Die Sicherungsschicht dient der kryptographischen Absicherung des Datenverkehrs.
 - Jeder Knoten, über den ein IPsec-Paket läuft muss IPsec-spezifische Protokolldaten auswerten können.
 - Kryptographische Absicherung auf der Anwendungsschicht ist möglich.
 - Die kryptographische Absicherung einer Schicht sichert alle darüber liegenden Schichten vollständig ab.
- b) Welche der im folgenden genannten Vertrauensmodelle unterstützt PGP?
- Direct Trust
 - Hierarchical Trust
 - Independent Trust
 - User Trust
 - Web of Trust

c) Grundsätzlich gilt in PGP:

- Teilnehmer können das Vertrauen in andere Teilnehmer frei wählen.
- Teilnehmer können Vertrauen anderer Teilnehmer übernehmen.
- Den Grad der Authentizität fremder Schlüssel stellt jeder Benutzer explizit selber ein.
- Teilnehmer können öffentliche Schlüssel signieren.
- Jeder Teilnehmer kann nur ein Schlüsselpaar besitzen.

d) Mit PGP können folgende Schutzziele direkt erreicht werden:

- Integrität
- Authentizität
- Verbindlichkeit
- Datiertheit
- Anonymität

e) Ihnen liegt ein selbst-signiertes Zertifikat vor. Weitere Informationen haben Sie nicht. Welche der folgenden Aussagen sind in dieser Situation *mit Sicherheit gültig*?

- Der Inhaber ist eine offizielle CA, der Sie vertrauen können.
- Der Aussteller ist eine offizielle CA, da Privatpersonen überhaupt keine selbst-signierte Zertifikate ausstellen können.
- Es kann sich nur um ein PGP-Zertifikat handeln. Bei X.509-Zertifikaten wird dieser Mechanismus nicht verwendet.
- Die Integrität des Zertifikats seit dem Signaturzeitpunkt ist garantiert.
- Die Authentizität des Zertifikats ist garantiert.

f) Für die Revokation eines Zertifikats gilt:

- N Im Kettenmodell wirkt sie sich auf die Gültigkeit aller Signaturen aus, die von dem zugehörigen privaten Schlüssel *vorher* geleistet wurden.
- J Sie kann aus verschiedenen Gründen erfolgen.
- N Die dadurch entstehende Revokationsinformation (z.B. CRL) wird immer von dem Aussteller des revozierten Zertifikats unterschrieben.
- N Wurde ein Schlüssel kompromittiert, verhindert die Revokation im *erweiterten Schalenmodell*, dass gefälschte Signaturen erstellt werden können, die auch nach der Revokation noch als gültig gelten.
- N Sie gilt ab dem Zeitpunkt, an dem der Vorfall, der zur Revokation geführt hat, stattgefunden hat.

g) Welche der folgenden Aussagen sind richtig für eine PKI, deren Zertifikate dem X.509 Standard genügen?

- N Jedes aktive Trust-Center ist auch eine Wurzelinstanz.
- N Jedes aktive Trust-Center muss wenigstens ein eigenes gültiges Schlüssel-paar haben, das von einer Wurzelinstanz zertifiziert ist.
- J Jedes aktive Trust-Center muss wenigsten ein eigenes Schlüsselpaar besitzen, dessen Gültigkeit über eine Zertifikatskette auf eine Wurzelinstanz zurückgeführt werden kann.
- J Jedes aktive Trust-Center muss eine gültige Revokationsliste bereitstellen.
- N Jedes aktive Trust-Center muss Key-Backup für die Verschlüsselungs-Schlüssel seiner Teilnehmer betreiben.

h) Welche der folgenden Attribute müssen in einem X.509 Zertifikat vorhanden sein?

- J Zertifikatsseriennummer
- J IssuerDN (Name des Ausstellers)
- N Key Usage
- N CRL Distributions Point
- N Production Time

i) Welches sind die Vorteile von symmetrischen Verschlüsselungsverfahren gegenüber asymmetrischen?

- N Der Schlüsselaustausch ist einfacher.
- N Alle Nachrichten für einen Empfänger werden mit dem gleichen Schlüssel verschlüsselt, unabhängig davon wer sie schickt.
- J Die Verschlüsselung ist schneller.
- N Sie sind sicherer.
- N Sie können auch zur Signatur von Dokumenten eingesetzt werden.

j) Sie wollen mittels PKI-Techniken eine verschlüsselte und signierte E-Mail verschicken. Welche Schlüssel benötigen Sie dafür?

- J Den Private-Key des Senders.
- N Den Public-Key des Senders.
- N Den Private-Key des Empfängers.
- J Den Public-Key des Empfängers.
- N Den Public-Key des Trust-Centers.

Aufgabe 2: X.509 Zertifikate und Gültigkeitsmodelle (10 Punkte)

In dieser Aufgabe geht es ausschließlich um das *erweiterte Schalenmodell* (Hybridmodell). Der Vertrauensanker sei stets "DFN Root". Die für die Bearbeitung der Aufgabe wesentlichen Daten der verwendeten Zertifikate sind nachfolgend tabelliert. Dabei beziehen sich alle Datumsangaben auf das Jahr 2003:

Zertifikat A	
Subject	DFN Root
Issuer	DFN Root
NotBefore	1.6.
NotAfter	30.11.
Public Key	$PubKey_A$

Zertifikat B	
Subject	TU Darmstadt
Issuer	DFN Root
NotBefore	1.6.
NotAfter	30.9.
Public Key	$PubKey_B$

Zertifikat C	
Subject	Uni Gießen
Issuer	DFN Root
NotBefore	1.7.
NotAfter	31.12.
Public Key	$PubKey_C$

Zertifikat D	
Subject	FB Informatik
Issuer	TU Darmstadt
NotBefore	1.6.
NotAfter	31.10.
Public Key	$PubKey_D$

Zertifikat E	
Subject	Alice
Issuer	FB Informatik
NotBefore	1.7.
NotAfter	31.12.
Public Key	$PubKey_E$

Alice hat drei Dokumente mit ihrem privaten Schlüssel ($PrivKey_E$) signiert, wobei Dok_1 am 15.8., Dok_2 am 15.9. und Dok_3 am 15.10. unterschrieben wurden.

- a) Bestimmen Sie für alle drei Dokumente, welches Ergebnis die Gültigkeits-Prüfung der jeweiligen Signatur am am 20.10. hätte. Falls eine Prüfung ungültig ausfällt, geben Sie den Grund dafür an!
- b) Nehmen Sie an, dass Zertifikat D (ausgestellt auf "FB Informatik") am 5.9. revoziert wird. Bestimmen Sie den Zeitraum, in dem Alice Dokumente signieren konnte, die am 20.10. als gültig geprüft werden können!
- c) Nehmen Sie an, dass sich "FB Informatik" eine Cross-Zertifizierung mit "Uni Gießen" durchgeführt hat. Die dadurch entstandenen Zertifikate sind nicht vor dem 1.10. und nicht nach dem 30.11. gültig. Gehen Sie außerdem davon aus, dass die in Aufgabenteil b) beschriebene Revokation stattgefunden hat!
 - (i) Geben Sie die Cross-Zertifikate nach obigem Muster an.
 - (ii) Bestimmen Sie nun für alle drei Dokumente, welches Ergebnis die Gültigkeits-Prüfung der jeweiligen Signatur am am 20.10. hätte! Falls eine Prüfung ungültig ausfällt, geben Sie den Grund dafür an!

Lösungsvorschlag

Im folgenden geht es um das erweiterte Schalenmodell (Hybridmodell).

Die Signatur eines Dokumentes ist gültig zu einem Zeitpunkt t , wenn ein Zertifikat C mit folgenden Eigenschaften existiert:

- Die Signatur des Dokuments lässt sich mit dem öffentlichen Schlüssel des Zertifikats rechnerisch prüfen.
- Der Zeitpunkt der *Erstellung* des Dokuments t' liegt im Gültigkeitsintervall von C ¹
- Nach C durfte der entsprechende private Schlüssel für Dokumentensignaturen verwendet werden²
- C ist zum Zeitpunkt t' gültig.

Ein Zertifikat C ist zum Zeitpunkt t gültig, entweder wenn es

- ein selbst-signiertes Zertifikat ist,
- die Signatur des Zertifikats mit dem im Zertifikat enthaltenen öffentlichen Schlüssel geprüft werden kann *und*
- das Zertifikat zum Zeitpunkt t als Vertrauensanker anerkannt ist.

oder, wenn ein Zertifikat D mit folgenden Eigenschaften existiert:

- Die Signatur von C lässt sich mit dem öffentlichen Schlüssel von D rechnerisch prüfen.
- t liegt im Gültigkeitsintervall von D
- Nach D durfte der entsprechende private Schlüssel für das Erstellen von Zertifikaten verwendet werden³
- D ist zum Zeitpunkt t gültig.

¹notBefore bzw. notAfter

²ist hier nicht relevant

³ist hier nicht relevant

- a) Wir haben genau eine Zertifikatskette, die von Alice zum Vertrauensanker "DFN Root" führt: $E \rightarrow D \rightarrow B \rightarrow A$. Wir prüfen die Kette zum Zeitpunkt der Erstellung der Dokumentsignatur.

Dok_1 Prüfung zum 15.8.:

Zertifikat E ist *gültig* zum 15.8..
Zertifikat D ist *gültig* zum 15.8..
Zertifikat B ist *gültig* zum 15.8..
Zertifikat A ist *gültig* zum 15.8..

Dok_1 Prüfung zum 15.9.:

Zertifikat E ist *gültig* zum 15.9..
Zertifikat D ist *gültig* zum 15.9..
Zertifikat B ist *gültig* zum 15.9..
Zertifikat A ist *gültig* zum 15.9..

Dok_1 Prüfung zum 15.10.:

Zertifikat E ist *gültig* zum 15.10..
Zertifikat D ist *gültig* zum 15.10..
Zertifikat B ist *nicht gültig* zum 15.10.. Zertifikat abgelaufen
(15.10. > *notAfter*)

- b) Maßgeblich ist im Hybridmodell der Zeitpunkt der Signatur des Dokuments. D.h. wenn das Dokument zu einem Zeitpunkt signiert wurde, zu dem die Zertifikatskette gültig war, ist es auch am 20.10. noch gültig. Wir betrachten wieder die Zertifikatskette $E \rightarrow D \rightarrow B \rightarrow A$. Sie ist nicht gültig vor dem 1.6. (wegen A, B und D) und sie ist nicht gültig ab dem 5.9. (wegen der Revokation von D). Alice kann folglich Dokumente nicht vor dem 1.7. aber vor dem 5.9. signieren. Diese sind dann am 20.10. noch gültig.

- c) (i) Bei der gegenseitigen Cross-Zertifizierung entstehen zwei Zertifikate:

Zertifikat F		Zertifikat G	
Subject	Uni Gießen	Subject	FB Informatik
Issuer	FB Informatik	Issuer	Uni Gießen
NotBefore	1.10.	NotBefore	1.10.
NotAfter	30.11.	NotAfter	30.11.
Public Key	$PubKey_C$	Public Key	$PubKey_D$

- (ii) Die Prüfung erfolgt wie bei a), nur das wir ggf. noch eine zweite Zertifikatskette betrachten können: $E \rightarrow G \rightarrow C \rightarrow A$.

Dok_1 erstellt am 15.8.:

Zertifikat E ist *gültig* zum 15.8..
 Zertifikat D ist *gültig* zum 15.8..
 Zertifikat B ist *gültig* zum 15.8..
 Zertifikat A ist *gültig* zum 15.8..

Dok_2 erstellt am 15.9.:

Zertifikat E ist *gültig* zum 15.9..
 Zertifikat D ist *nicht gültig* zum 15.9.. D ist revoziert!
 und
 Zertifikat E ist *gültig* zum 15.9..
 Zertifikat G ist *nicht gültig* zum 15.9.. G noch nicht gültig

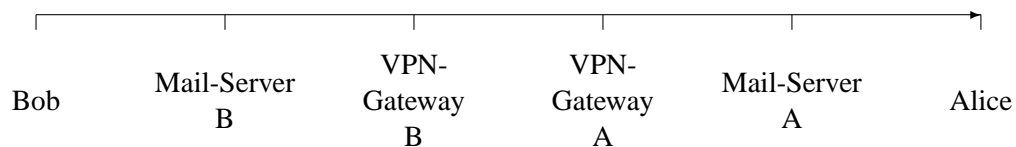
Dok_3 erstellt am 15.10.:

Zertifikat E ist *gültig* zum 15.10..
 Zertifikat D ist *nicht gültig* zum 15.10.. D ist revoziert
 aber
 Zertifikat E ist *gültig* zum 15.10..
 Zertifikat G ist *gültig* zum 15.10..
 Zertifikat C ist *gültig* zum 15.10..
 Zertifikat A ist *gültig* zum 15.10..

Aufgabe 3: vereinfachtes Schichtenmodell (10 Punkte)

Alice und Bob arbeiten in zwei verschiedenen Ländern in Filialen der selben Firma F. Alice Arbeitet in Filiale A, Bob in Filiale B. Alle LANs von F sind über VPN-Gateways (Schutzmechanismus: IPsec im ESP-Tunnel-Modus) miteinander verbunden. Außerdem besitzt die Firma eine über alle Ihre Filialen ausgedehnte PKI. Alice besitzt keine eigenen Schlüsselpaare. Bob besitzt gültige Schlüsselpaare. Alice und Bob kommunizieren mittels Email (via filial-eigener Mailserver) miteinander. Der Schutz der Emails erfolgt in der Firma F mittels S/MIME.

- a) Kann Alice den IPsec-Tunnel nutzen? Begründen Sie Ihre Antwort!
- b) Wie kann Alice die PKI zur Absicherung von Emails nutzen? Begründen Sie Ihre Antwort!
- c) Bob sendet eine signierte aber nicht verschlüsselte Email an Alice. Die von der Mail zurückgelegte Strecke ist nachfolgend skizziert. Welche der Schutzziele *Authentizität*, *Verbindlichkeit*, *Vertraulichkeit* bzw. *Anonymität* erreichen die von der Firma F eingesetzten Sicherheitsmechanismen. Tragen Sie dazu in der Skizze die jeweils maximale Strecke ein, auf der diese Schutzziele erreicht werden und beschriften Sie diese mit dem Namen des Schutzziels, dem Namen des Sicherheitsmechanismus' und der entsprechenden Protokollebene nach vereinfachtem Schichtenmodell.



Lösungsvorschlag

- a) Ja.
Der Tunnel ist völlig unabhängig von den Schlüsseln der einzelnen User. (1 Punkt)

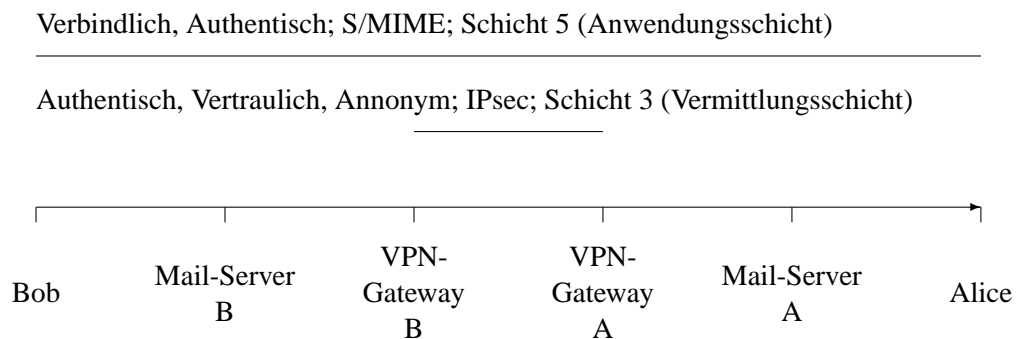
Der Tunnel ist für Alice (bzw. ihre Applikationen) transparent. Sie muss ihn sogar nutzen ob, sie will oder nicht. (1 Punkt)

b) Eingeschränkt.

Sie kann selber keine verschlüsselten Daten erhalten oder eigene Daten signieren. (1 Punkt).

Sie kann aber anderen PKI Teilnehmern verschlüsselte Daten schicken und deren Signaturen verifizieren. (1 Punkt)

c) Die Situation stellt sich wie folgt dar.



Aufgabe 4: Smartcards (10 Punkte)

Smartcards sind Geräte mit beschränkten Ressourcen. Sie können in einer PKI als Hardware-PSE (Personal Security Environment) eingesetzt werden.

- a) Warum sind Smartcards sicherer als Software-PSE? Begründen Sie Ihre Antwort!
- b) Ein Benutzer will die Verschlüsselungsfähigkeiten seines Email-Clients nutzen. Aus Sicherheitsgründen verwendet er eine Smartcard, auf der der private Schlüssel untergebracht ist. Zu diesem Zweck hat er einen Chipkartenleser ohne Tastatur an seinem PC angeschlossen.

Skizzieren Sie, welche Informationen beim Ver- bzw. Entschlüsseln zwischen welchen Geräten ausgetauscht werden! Beschreiben Sie, auf welchem Gerät welche Berechnungen durchgeführt werden!

Welche Probleme entstehen aufgrund der Ressourcenbeschränktheit der Smartcard?

Lösungsvorschlag

- a) Smartcards bieten:
 - aktive Sicherheitsmaßnahmen (Anzahl der Versuche bei der PIN-Eingabe sind limitiert, sensitive Daten werden bei nicht erlaubten Zugriffen zerstört, ...)
 - Berechnungen finden auf der Karte statt, der private Schlüssel muss die Karte nie verlassen.
 - Die Karte ist eine eigene Komponente, d.h. sie kann mitgenommen werden (muss nicht im Rechner verbleiben) und sie kann nicht kopiert werden, ein Dieb muss also die Karte entwenden.

Softtoken bieten das entsprechend nicht.

- b) Ablauf der Ver- und Entschlüsselung:
 - Ver- und Entschlüsselung erfolgen aus Gründen der Geschwindigkeit hybrid (Platzprobleme bestehen dabei nicht, da die auch die asymmetrischen Verfahren Blockchiffren darstellen).

- Die Verschlüsselung erfolgt *nicht* auf der Karte, weil dazu der private Schlüssel *nicht* benötigt wird. Es wird zufällig ein symmetrischer Sitzungsschlüssel gewählt. Damit wird die Email symmetrisch verschlüsselt. Danach wird der Sitzungsschlüssel mit dem öffentlichen Schlüssel *des Empfängers* verschlüsselt und der Mail angehängt. Dies geschieht alles auf dem PC
- Die Entschlüsselung geht wie folgt:
 1. PIN-Eingabe am PC (Kartenleser hat kein PIN-Pad)
PIN wird über den Kartenleser an die Karte geschickt.
 2. Der asymmetrisch verschlüsselte Sessionkey wird der Email entnommen und über den Kartenleser an die Email gesendet.
 3. Auf der Karte wird der Sitzungsschlüssel mit dem privaten Schlüssel entschlüsselt. Der entschlüsselte Sitzungsschlüssel wird zurück an den PC gesendet.
 4. Dort wird die Mail symmetrisch entschlüsselt.
- Es gibt *keine* Ressourcenprobleme.

Aufgabe 5: Web of Trust (10 Punkte)

Die Benutzerin Alice(A) möchte sich der Authentizität des öffentlichen Schlüssels ihres Kommunikationspartners Bob(B) versichern. Ihr steht ein Web of Trust zwischen den Personen $\{A, B, W, X, Y, Z\}$ zur Verfügung.

Alice' Kenntnisstand $View_A$ ist gegeben durch:

$$View_A = \{Aut_W, Aut_Y, Cert_{X,B}, Cert_{Y,Z}, Cert_{Z,B}, \\ Trust_{W,3}, Trust_{Y,1}, Rec_{W,X,1}, Rec_{Y,Z,2}\}$$

- Zeigen Sie, wie aus $View'_A := View_A \cup \{Trust_{Z,1}\}$ die Aussage Aut_B abgeleitet werden kann.
- Für welches Alpha muss das Zertifikat $Cert_{\alpha,X}$ zu $View_A$ hinzugefügt werden, um daraus Aut_B ableiten zu können? Geben Sie für jede Lösung α an, wie die Aussage Aut_B abgeleitet werden kann.

Hinweis: Es gibt zwei Lösungen.

- Eine Vertrauensstufe $Trust_{\alpha,i}$ nennen wir *stärker* als $Trust_{\alpha,j}$ falls $i > j$. Erhöhen Sie eine der Vertrauensstufen $Trust_{\alpha,i}$ in $View_A$ derart, dass daraus Aut_B abgeleitet werden kann.

Geben Sie einen Wert für α , das minimale i und die verwendeten Regeln an.

Bemerkung:

Diese Aufgabe verwendet die selben Begriffe und Definitionen der Aufgabe 3 von Übungsblatt 4.

Hier sind zur Erinnerung die Ableitungsregeln noch einmal angegeben:

- (1) $\forall X \forall Y : Aut_X, Trust_{X,1}, Cert_{X,Y} \vdash Aut_Y$
- (2) $\forall X \forall Y \forall i \geq 1 : Aut_X, Trust_{X,i+1}, Rec_{X,Y,i} \vdash Trust_{Y,i}$
- (3) $\forall X \forall 1 \leq k < i : Trust_{X,i} \vdash Trust_{X,k}$
- (4) $\forall X \forall Y \forall 1 \leq k < i : Rec_{X,Y,i} \vdash Rec_{X,Y,k}$

Lösungsvorschlag

a)

$$\begin{array}{l} \text{Aut}_Y, \text{Trust}_{Y,1}, \text{Cert}_{Y,Z} \vdash \text{Aut}_Z \quad \text{Regel 1} \\ \text{Aut}_Z, \text{Trust}_{Z,1}, \text{Cert}_{Z,B} \vdash \text{Aut}_B \quad \text{Regel 1} \end{array}$$

b) Lösung 1: $\alpha = W$

$$\begin{array}{l} \text{Trust}_{W,3} \vdash \text{Trust}_{W,1} \quad \text{Regel 3} \\ \text{Aut}_W, \text{Trust}_{W,1}, \text{Cert}_{W,X} \vdash \text{Aut}_X \quad \text{Regel 1} \\ \text{Aut}_X, \text{Trust}_{X,1}, \text{Cert}_{X,B} \vdash \text{Aut}_B \quad \text{Regel 1} \end{array}$$

Lösung 2: $\alpha = y$

$$\begin{array}{l} \text{Aut}_Y, \text{Trust}_{Y,1}, \text{Cert}_{Y,X} \vdash \text{Aut}_X \quad \text{Regel 1} \\ \text{Aut}_X, \text{Trust}_{X,1}, \text{Cert}_{X,B} \vdash \text{Aut}_B \quad \text{Regel 1} \end{array}$$

c) Lösung: $\alpha = Y$ und $i = 2$.

$$\begin{array}{l} \text{Aut}_Y, \text{Trust}_{Y,2}, \text{Rec}_{Y,Z,1} \vdash \text{Trust}_{Z,1} \quad \text{Regel 2} \\ \text{Aut}_Z, \text{Trust}_{Z,1}, \text{Cert}_{Z,B} \vdash \text{Aut}_B \quad \text{Regel 1} \end{array}$$

Aufgabe 6: Angriffe (10 Punkte)

- a) Welche Gefahr bestehen, wenn man ein aus dem Internet geladenes Programm ausführt? Mit welchen Mitteln kann man dieser Gefahr begegnen?
- b) Wie heißen die Schichten des vereinfachten Schichtenmodells und in welcher Reihenfolge bauen sie aufeinander auf? Nennen Sie für mindestens zwei Schichten ein Protokoll und einen möglichen Angriff darauf!
- c) Ein in der Vorlesung behandelter Angriff war das DNS-Spoofing. Beschreiben Sie, wie man diesen Angriff mit PKI-Mitteln abwehren kann! Nennen Sie die beteiligten Kommunikationspartner, wer welche Schlüssel benötigt und welche Nachrichten wie gesichert werden!

Lösungsvorschlag

- a) Die Authentizität und die Integrität des Programs können nicht sichergestellt werden. D.h. Das Programm kann modifiziert sein oder gar nicht das, was ich suche. Ich weiß auch nicht sicher, von wem das Programm ist. Das Problem kann behoben werden, indem der Hersteller des Programms dieses signiert. Es reicht nicht aus, die Kommunikation mit dem Server zu sichern.
- b) Anwendungsschicht, Transportschicht, Vermittlungsschicht, Sicherungsschicht, Bitübertragungsschicht.
Angriff auf Sicherungsschicht: Framesniffing
Angriff auf Vermittlungsschicht: IP-Spoofing
- c) Beim DNS-Spoofing wird ausgenutzt, dass die Authentizität der Antworten auf DNS-Anfragen nicht ausreichend gesichert ist. Das kann man beheben, indem der DNS-Server seine Antworten signiert. Dazu braucht jeder DNS-Server einen privaten Schlüssel und jeder Client muss in der Lage sein, sich authentisch den zugehörigen öffentlichen Schlüssel zu besorgen.