Dr.-Ing. Jörg Schneider, Frank Rustemeyer
Henning Seidler, Carsten Schubert
Wintersemester 2021/22

Security in Telecommunications
Technische Universität Berlin

Klausur Grundagen der Rechnersicherheit

Name, Vorname: _____

Studiengang: _____

Matrikel-Nr.: _____

Aufgabe:	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Punkte:														
maximal	5	5	2	3	6	4	2	2	4	2	4	3	6	2

Summe: **Note:**

Punkte: Insgesamt sind in dieser Klausur **50** Punkte zu erreichen.
Bearbeitungszeit: Die Bearbeitungszeit beträgt **90** Minuten. Zusätzlich gibt es eine "Technikzeit" von 5 Minuten.
Hilfsmittel: Open-Book-Klausur, also alles
Form der Abgabe: Schreiben Sie die Lösung zu jeder Aufgabe unter die Aufgabe oder fertigen Sie ein separates Dokument an. Sollten die Antworten zu einzelnen Aufgaben an anderer Stelle stehen, fügen Sie bitte einen Vermerk ein. Verwenden Sie keine rote Farbe in der Abgabe.

Aufgabe 1

5 Punkte

Bitte kreuzen Sie bei den folgenden Aussagen jeweils an, ob sie wahr oder falsch sind.

Jede richtige Antwort gibt 1 Punkt, jede falsche Antwort, sowie jedes nicht angekreuzte Feld, gibt 0 Punkte.

		Wahr	Falsch
1.	Bei RSA ist es niemals möglich, die Nachricht zu einer Chiffre zu finden, wenn man den privaten Schlüssel nicht kennt.	◯	◯
2.	Aus dem Header einer Mail kann man einfach ablesen, von welcher Adresse die Mail verschickt wurde.	◯	◯
3.	Eine vorhandene Schwachstelle führt immer irgendwann zu einem Fehler (englisch Error).	◯	◯
4.	Eine qualifizierte Signatur ist grundsätzlich rechtlich äquivalent zur handschriftlicher Unterschrift.	◯	◯
5.	Im IT-Grundschutz-Sicherheitskonzept haben in der Regel die meisten vorhandenen Komponenten einen hohen, aber nicht sehr hohen, Schutzbedarf.	◯	◯

Aufgabe 2

3+2 Punkte

Der öffentliche RSA-Schlüssel von Alice lautet $(n, e) = (65, 5)$.

(i) Wie lautet der zugehörige private Schlüssel?

(ii) Sie erhalten die angeblich von Alice signierte Nachricht $(m, s) = (42, 3)$. Überprüfen Sie die Gültigkeit der Signatur.

Geben Sie jeweils den Rechenweg mit an.

Aufgabe 3

2 Punkte

Was ist die Same-Origin-Policy und wozu ist das gut?

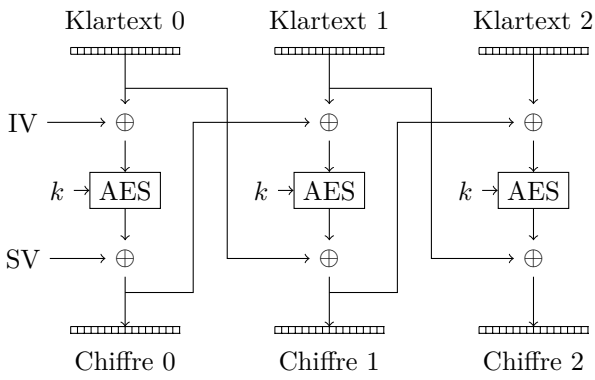
Aufgabe 4 3 Punkte

Um mit AES Texte zu verschlüsseln, die länger sind als ein Block, brauchen wir einen Modus, wie die Verschlüsselung der Blocke zusammen hängt. Links ist das Schema für die Verschlüsselung im AFC Modus gegeben. Dabei ist IV der "Initialisation Vector", SV der "Subsequent Vector" und k der Schlüssel.

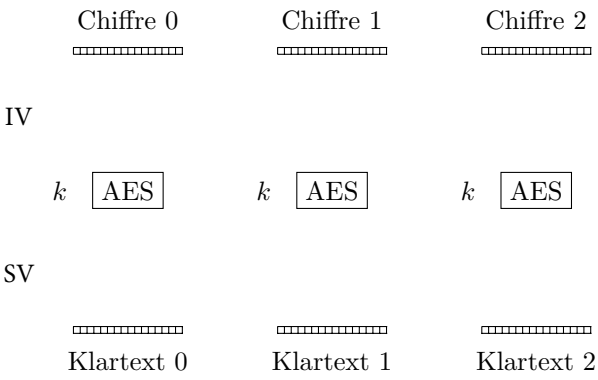
Tragen Sie rechts das Schema ein, wie man aus der Chiffre wieder den Klartext erhält.

AFC:

Verschlüsseln:



Entschlüsseln:



Aufgabe 5 6 Punkte

Die Firma LoSolutions plant den Einsatz einer Firewall für ihr Firmennetzwerk. Welche der folgenden Szenarien sind mit einem Paketfilter umsetzbar? Wenn nicht, ist es mit einer Application Level Firewall umsetzbar? Geben Sie jeweils eine kurze Begründung an.

(i) Ein Rechner darf nur auf das interne Netz zugreifen.

(ii) Wenn eine Datei empfangen wird, die auf dem Zielrechner Schaden anrichten würde, sollen die Pakete verworfen werden.

(iii) Die Firewall soll nur Pakete hindurch lassen, die von Mitarbeitern der Firma LoSolutions kommen.

Aufgabe 6 4 Punkte

Viele Compiler bauen von alleine sogenannte Canaries in Programme ein.

(i) Was ist das?

(ii) Warum ist das heutzutage gängige Praxis?

(iii) Entstehen dadurch auch Nachteile? Wenn ja, welche?

Aufgabe 7 2 Punkte

Warum werden im forensischen Prozess oft kryptographische Prüfsummen auf Papier geschrieben und archiviert?

Aufgabe 8 2 Punkte

Sowohl beim Signieren von Nachrichten als auch bei Passwort basierter Authentifikation sollte man Hash-Funktionen einsetzen. Wieso sollte man für beide Szenarien verschiedene Hash-Funktionen nutzen?

Aufgabe 9 4 Punkte

Im folgenden Text beschreiben wir kurz eine Situation. Finden Sie vier der möglichen Mängel im ISMS bzw. Bobs Verhalten. Beschreiben Sie diese kurz.

> Bob ist Informations-Sicherheitsbeauftragter der Firma LoSolutions. Letzte Woche gab es einen Sicherheitsvorfall, um den Bob sich jetzt kümmern muss. Sein Kollege Charlie ist auf Social Engineering herein gefallen und hat einen Anhang einer Mail geöffnet, der eine Ransomware auf seinem Rechner gestartet hat.
>
> Zuerst holt Bob aus dem Archiv die Informationssicherheits-Leitlinie, welche seine Vorgängerin Alice mal erstellt hat. Die Leitlinie besagt, dass man in diesem Fall alle infizierten Rechner neu aufsetzen soll. Da dies kein großer Aufwand ist, beschließt Bob, dass er das Notfallmanagement selbst übernimmt. Also installiert er auf Charlies Rechner erneut das Betriebssystem und alle nötigen Anwendungen. Daraufhin kann Charlie weiter arbeiten und auch für Bob ist der Fall erledigt.

Aufgabe 10 2 Punkte

Bei LoSolutions wird jedes Jahr am 1.1. ein komplettes Backup gemacht. Jeden Monat werden am 1. und am 15. differentielle Backups gemacht und jeden Tag inkrementelle Backups. Wie viele Schritte benötigt man, um den Zustand vom 24.12.2021 einzuspielen? Geben Sie auch eine kurze Erklärung an.

Aufgabe 11 4 Punkte

Die Firma LoSolutions möchte einen neuen Dienst zum Austausch von öffentlichen Nachrichten und Katzenbildern anbieten. Der Informations-Sicherheitsbeauftragte Bob erstellt dafür einige Design-Richtlinien.

> Der gesamte Dienst läuft auf einem einzigen Server, damit man nur ein Gerät absichern muss. Die Nutzer können im Browser per http (nur ohne Anmeldung) oder https (mit Anmeldung) auf den Dienst zugreifen. Die Administratoren greifen per SSH auf den Server zu. Da Port 22 häufig abgetastet wird, läuft der SSH-Zugriff über den zufällig festgelegten Port 42455. Die Autorisierung der Admins erfolgt über ein Passwort von mindestens 20 Zeichen oder per Public/Private Key. Damit Fehler möglichst schnell gefixt werden können, hat jeder Admin Zugriff auf alle Komponenten des Dienstes. Für Notfälle, in denen den Admins kein SSH zur Verfügung steht, gibt es eine Notabschaltung über die URL
>
> `www.losolutions.com/Y2F0c2FyZWJldHRlcnRoYW5kb2dz`
>
> welche nur den Admins bekannt ist. Außerdem tauschen sich auch die Mitarbeiterinnen und Mitarbeiter von LoSolutions über diesen Dienst aus. Damit ihre Nachrichten nicht öffentlich sind, können sie einen Haken setzen, der sie als "extra sicher" markiert.

Finden Sie zwei Stellen, an denen seine Vorschläge den Prinzipien für sichere Software widersprechen und beschreiben Sie kurz, was man stattdessen tun sollte.

Aufgabe 12 3 Punkte

Eine Strategie zur Abwehr von Social Engineering sollte drei Bereiche haben. Nennen Sie zu jedem Bereich eine beispielhafte Schutzmaßnahme!

Aufgabe 13 4+2 Punkte

a) Zu welcher der vier grundlegenden Arten für Authentisierung gehören Passwörter? Geben Sie für jede der *anderen* Kategorien ein Beispiel an.

b) Die Firma LoSolutions möchte eine neue Passwortrichtlinie erstellen. Bisher sollten die Angestellten 8 zufällige Zeichen aus den 4 Kategorien Großbuchstaben A-Z, Kleinbuchstaben a-z, Ziffern, und Sonderzeichen "/" und "+" nehmen (die 64 Base64-Zeichen).

Die neuen Passwörter sollen nur aus Unicode Emojis (aus Version 14) bestehen. Aus wie vielen Emojis müssen die Passwörter bestehen, um mindestens das gleiche Sicherheitsniveau gegen Brute-Force-Angriffe zu haben, wie das alte Schema?

Aufgabe 14 2 Punkte

Erläutern Sie den *Verteilungseffekt* im IT-Grundschutz anhand eines Beispiels!