Hochschule RheinMain
Studiengang Informatik - Technische Systeme
Prof. Dr. Marc Stöttinger

Probeklausur Security (LV4120)

Sommersemester 2023

Nachname:	Vorname:
Matrikelnummer:	
Datum: 18.06.2023	**Unterschrift:**

Sie erhalten eine geheftete Klausur. **Bitte lösen Sie die Heftung nicht**. Bitte tragen Sie zu Beginn der Bearbeitungszeit Ihren Namen und Ihre Matrikelnummer an den dafür vorgesehenen Stellen ein und unterschreiben Sie die Klausur. Die Klausur ist **nur mit Unterschrift** gültig. Die Klausur muss mit dem Verlassen des Raumes abgegeben werden.

Zum Bestehen der Klausur sind 45 Punkte (50%) notwendig

Im Falle nicht ausreichenden Platzes benutzen Sie bitte zusätzliche Blätter, die Sie mit Name und Matrikelnummer versehen. Machen Sie bitte eindeutig kenntlich, auf welche Aufgabe sich Ihre Antwort bezieht.

Dauer: 90 min (Klausur)
Hilfsmittel: eigene Formelsammlung von maximal einer doppelseitig handschriftlich beschriebenen DIN A4 Seite.

Punkte:

Aufgabe	**Soll-Punkte**	**Ist-Punkte**
1	10	
2	20	
3	20	
4	20	
5	20	
Gesamt	90	

Note:

"IT-Sicherheit beschäftigt sich mit der Absicherung von technischen Systemen durch angemessene Maßnahmen auf ein tragbares Maß."
Bsp: Netzwerk, EMail, Server

Aufgabe 1: (10 Punkte)

Systemen zur informationsverarbeitendung, - speicherung und -lagerung." Bsp: Verschlussakten, Personenkontrolle,

Beantworten Sie bitte folgende Fragen (je 1 P):

Frage	Antwort
Ist IT-Sicherheit ein Bestandteil von Informationssicherheit?	Ja
Was ist ein Asset?	Eine Asset ist jede Komponente, jedes System, alle Daten, jede Anwendung oder jede Ressource, die für ein System, ein Unternehmen oder eine Organisation von immenser Bedeutung ist und geschützt werden muss.
Zu welcher Klasse (Anwender, Hacktivist, Kriminelle ,...) von Angreifern gehört ein Botnet?	Krimineller
Ist Assembler eine architekturabhängige Programmiersprache?	Ja
Wird Phishing immer nur mit Hilfe von Emails ausgeführt?	Nein (SMS)
Was sichern Schutz- oder Sicherheitsziele ab?	Assets Schutzziele definieren abstrakte Sicherheitsanforderungen an ein Asset
Was ist der Hauptinhalt vom BSI Dokument 200-4?	Business Continuity Management (Community Draft)
Wofür steht PDCA?	Plan Do Check Act
Kann das Sicherheitsziel Vertraulichkeit mit Hilfe einer Hash-Funktion und einem Geheimnis erfüllt werden?	
Ist eine MAC eine symmetrische Signatur und gleichwertig zu einer asymmetrischen Signatur?	

Sicherheitsziel | Sicherheitsziel (eng.) | Bedrohung | Bedrohung (eng.)Vertraulichkeit | Co

Aufgabe 2: (20 Punkte)

a) Nennen Sie die Schutzziele des Sicherheitsziel-Modells von STRIDE, welche nicht Teil von CIAA sind. (1P.)

Verschiedene gängige Sicherheitsziel-Modelle: CIA: Confidentiality, Integrity, Availability CIAA: CIA + Authenticity

b) Welche drei wesentlichen Schritte werden bei einer Bedrohungsanalyse durchgeführt? (2P.)

1. Assets identifizieren
2. Schutzbedarfsanalyse
3. Schadensanalyse

c) Wo für steht DREAD im DREAD-Modell?Nennen Sie die einzelnen Komponenten und beschrieben Sie diese kurz mit Satz? (5P.)

Bewertung	Gering	Mittel	Hoch
Damage: Schaden	Verarbeitung unbedeutender Information ist möglich	Verbreitung relevanter Informationen ist möglich	Sicherheitslücke untergraben und vollständige Bescheinigungen erlangt
Reproducibility: Reproduzierbarkeit	Nur mit Kenntnis der Sicherheitslücke schwer reproduzierbar	Angriff kann innerhalb eines bestimmten Zeitfensters reproduziert werden	Angriff kann jederzeit reproduziert werden.
Exploitability: Ausnutzbarkeit	Nur Experten mit Fachwissen können den Angriff durchführen	Erfahrene Programmierer können den Angriff ausführen	Programmieranfänger kann den Angriff in kurzer zeit durchführen.
Affected users: Betroffene	Ein sehr geringer Prozentsatz von Benutzern ist betroffen	Einzelne sind betroffen; keine Standardkonfiguration	Alle Benutzer sind betroffen; Standardkonfiguration
Discoverability: Auffindbarkeit	Der Fehler ist unbekannt und es ist unwahrscheinlich, dass Benutzer das Schadenspotential erkennen.	Die Sicherheitslücke befindet sich in einem selten verwendeten Teil des Produkts. Die bösartige Verwendbarkeit ist nur mit einigem Aufwand erkennbar.	Angriff wird über öffentlich zugängliche Medien erklärt. Die Sicherheitslücke findet sich in einer viel verwendeten Funktion und ist leicht wahrnehmbar.

[HEAVENS] Faktoren	Kritisch(3)	Hoch(2)	Mittel(1)	Niedrig(0)
Zugriffsmöglichkeiten	Internet	Lokales Netzwerk	Systemzugriff	Physischer Zugriff
Expertise	Laie	Kompetent	Experte	Mehrere Experten
Wissen über das Ziel	Öffentlich	Branchenspezifisch	Unternehmensspezifisch	Geheim
Benötigte Geräte	Standard	Spezialisierte Geräte	Speziell Produzierte Geräte	Mehrere Speziell Produzierte Geräte

d) Vervollständigen Sie Eintrittswahrscheinlichkeiten des gegebenen Angriffsbaums auf der nächsten Seite. Nutzen Sie für die Bestimmung der drei Blattknoten ohne Angaben die gegebene Beschreibung und das HEAVENS Modell, welches Sie aus der Vorlesung kennen. Vervollständigen Sie erst die Eintrittswahrscheinlichkeit in der Tabelle basierende auf der Beschreibung. Begründen Sie die Einstufung jedes Faktor kurz. (12P.)

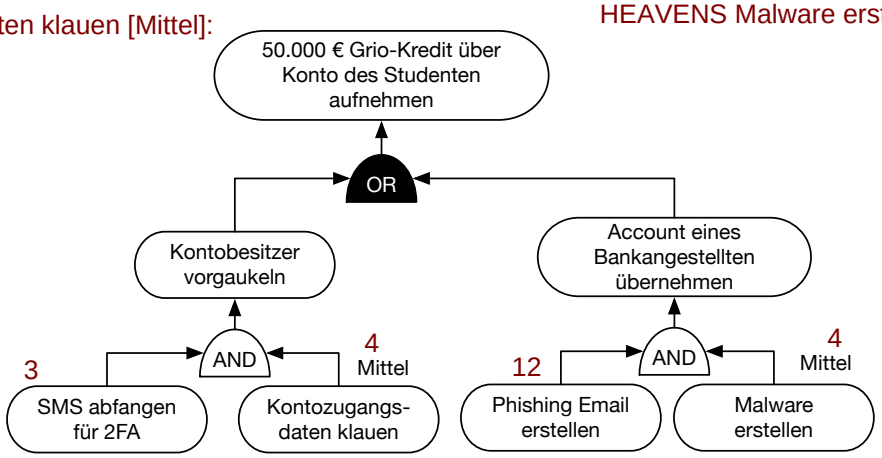
a SMS abfangen für 2FA:
Um die 2FA zu umgehen, benötigt man den physikalischen Zugang zu dem Mobiltelefon und Expertenwissen, damit man sich ohne Kenntnis der Pins anmelden kann, um die SMS mit dem 2FA-Code lesen zu können. Ebenso ist quasi geheim, wo sich das Mobiltelefon befindet oder an welche Mobiltelefonnummer die SMS gesendet wird.

b Phishing Email erstellen, um Account eines Bankangestellten zu übernehmen:
Mit Chat-GPT kann jeder Laie eine Phishing Email mit seinem Standardrechner erstellen. Die meisten Banken haben die Emailadresse Ihrer Ansprechpartner für Konten öffentlich auf der Webseite und sind somit quasi öffentlich.

Faktor	a: SMS abfangen für 2FA	b: Phishing Email erstellen
Zugriffs-möglichkeiten	Niedrig 0	Internet (3)
Expertise	Mehrere Experten (0)	Kritisch (3)
Wissen über das Ziel	Geheim [redacted] (0)	Öffentlich (3)
Benötigte Geräte	Standard (3)	Kritisch (3)
Summe	3	12

HEAVENS Kontozugangsdaten klauen [Mittel]:
(1, 1, 1, 1) = 4

HEAVENS Malware erstellen [Mittel]:



Aufgabe 3: (20 Punkte)

a) Nennen Sie ein Verschlüssungsverfahren, was theoretisch beweisbar perfekte Geheimhaltung garantiert. (1P.)

One-Time-Pad

b) Was ist der Unterschied zwischen einer monoalphabetischern und einer polyalphabetischern Substitution Chiffre. (2P.)

Im Gegensatz zur monoalphabetischen Substitution werden hier viele („poly“) Geheimalphabete zum Ersetzen der Buchstaben genommen:

c) Nennen Sie die in der Vorlesung behandelten Angriffsmodelle auf kryptographische Verfahren und erläutern Sie diese in einem Satz. (4P.)

Angriffsmodel	Beschreibung	Beispiel Szenario
Ciphertext-Only	Eve ist nur der Ciphertext bekannt	Nur verschlüsselte Zugangsdaten sind bekannt.
Known-Plaintext	Eve erhält zufällige Plaintext/Ciphertext Paare	Alice loggt sich auf ihrem Konto ein und surft auf bekanntem Teil von stud.ip
Chosen-Plaintext	Eve hat Zugriff auf ein Verschlüsselungsorakel, das beliebige Plaintexte verschlüsselt	Eve sendet eine Nachricht an Alice. Alice loggt sich ein und ruft Eve's Nachricht ab.
Chosen-Ciphertext	Eve hat Zugriff auf ein Entschlüsselungsorakel, das beliebige Ciphertexte entschlüsselt	Eve hat für begrenzte Zeit Zugriff auf Alice's Gerät mit verschlüsselter Sitzung (ohne bestehenden Login) und lässt sich manipulierte verschlüsselte Nachricht entschlüsseln. Alice kommt später wieder und loggt sich auf Webseite ein.

d) In der folgenden Aufgabe betrachten wir die abelsche zyklische Gruppe $\mathbb{Z}_7^*$.

d1) Listen Sie alle möglichen Elemente der Gruppe $\mathbb{Z}_7^*$ auf. (1P.)

d2) Was ist die Ordnung oder Kardinalität der Gruppe $\mathbb{Z}_5^*$? (1P.)

d3) Begründen Sie, warum $\mathbb{Z}_7^*$ kein Körper ist sondern nur eine Gruppe. (2P.)

d4) Erläutern Sie, was ein Generator in einer zyklischen Gruppe ist. (1P.)

d5) Zeigen Sie, dass das Element α=3 in $\mathbb{Z}_7^*$ ein Generator der zyklischen Gruppe ist. (3P.)

d6) Berchenen Sie das inverse Element zu 23 über $\mathbb{Z}_7^*$. (5P.)

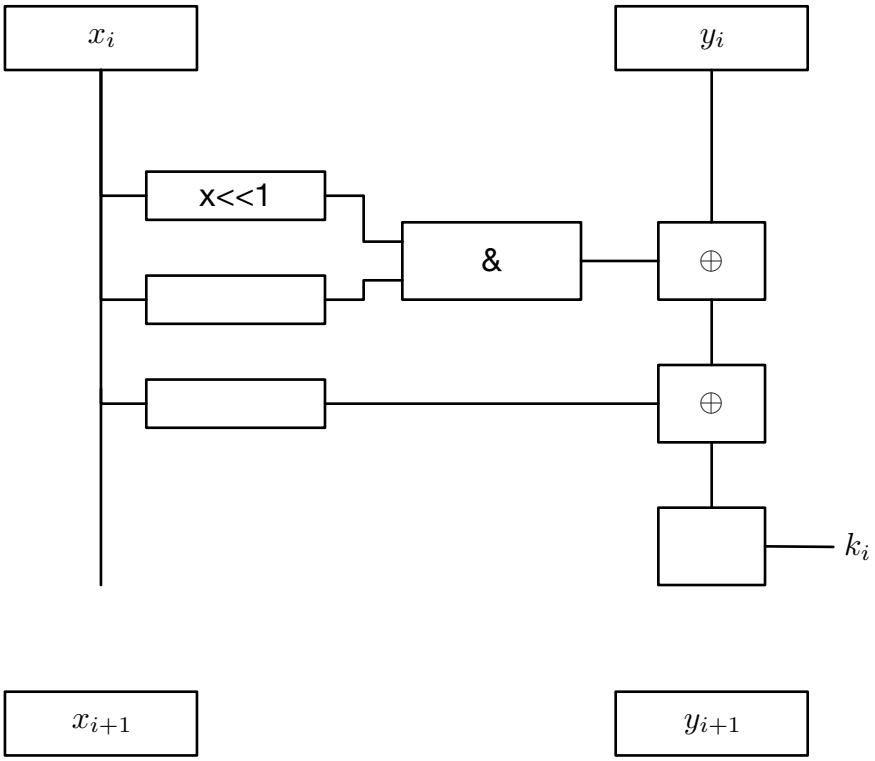
Aufgabe 4: (20 Punkte)

a) Der Cipher `SIMON32/64` ist ein Blockcipher und führt 32 Runden pro Ver- oder Entschlüsselung von einem 32bit Block aus. Bei einer Verschlüsselung führt der Algorithmus pro i-te Runde folgende Operation $R(x, y)$ aus:
$R(x_{i+1}, y_{i+1}) = ((y_i \oplus f(x_i) \oplus k_i), x_i)$.

Bei einer Entschlüsselung führt der Algorithmus pro i-te Runde folgende Operation $R^{-1}(x, y)$aus:
$R(x_{32-i-1}, y_{32-i-1}) = (y_{32-i}, (x_{i-32} \oplus f(y_{i-32}) \oplus k_{32-i}))$.

$\oplus$ ist einen `XOR`-Operation, k_i ist der it-te Rundenschlüssel und die Rundenfunktion $f(x) = (x << 1)\&(x << 8) \oplus (x << 2)$, wobei & eine `AND`-Operation ist und $(x << n)$ eine `Shift`-Operation nach links um n Bits ist.

a1) Vervollständigen Sie das Blockschaltbild einer Rundenoperation bei einem Verschlüsselungsvorgang. (5P.)



a2) Zu welcher Klasse von Blockchiffren gehört `SIMON`? (2P.)

Feistel-Chiffre

a3) Was ist charakteristisch für diese Art von Cipher? (3P).

Plaintext wird in 2 gleichgroße Blöcke aufgeteilt

b) Skizzieren Sie den Ablauf des DHKE-Protokolls für einen Schlüsselaustausch zwischen Alice und Bob. (5P.)

c) Gegeben seien folgende Parameter für einen DH Schlüsselaustausch: $p = 7, g = 3$. Zeigen Sie, dass, wenn Bob als privaten Schlüssel $b = 3$ wählt und Alice $a = 4$, die beiden einen gemeinsamen Sessionschlüssel $K_{Session}$ ableiten können. (5P.)

Aufgabe 5: (20 Punkte)

a) Erklären Sie, was schwache Kollisionsresistenz ist. (2P.)

b) Erklären Sie, was starke Kollisionsresistenz ist. (2P.)

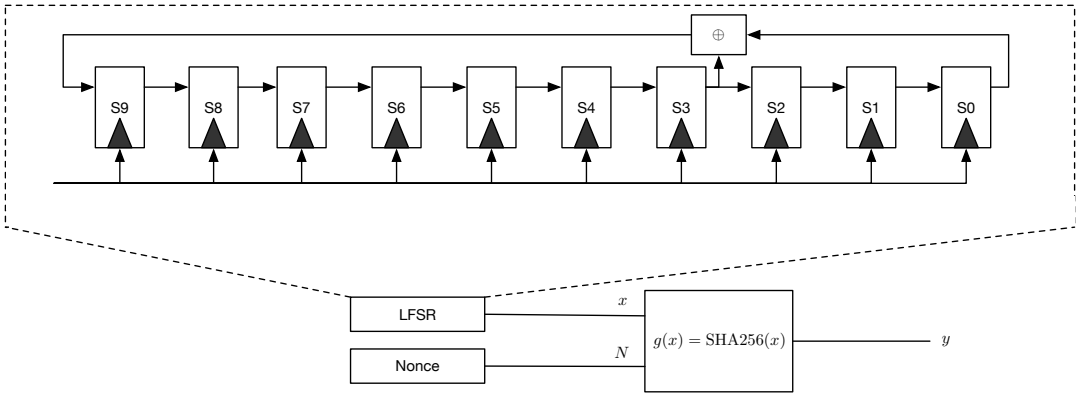
c) Gegeben sei folgende Funktion $f(x) = (g^x \mod N) \mod 2^{192}$, mit $N = p \cdot q$. Die Basis g ist bekannt, p und q sind unbekannte Primzahlen, der 2048-bit große Modulus N ist bekannt.

c1) Prüfen Sie, ob die Funktion $f(x)$ eine Einwegfunktion ist. Sie können sich in ihrer Argumentation auch auf aus der Vorlesung bekannte Probleme und deren Lösbarkeit beziehen. (4P.)

c2) Prüfen Sie, ob die Funktion $f(x)$ das Kriterium einer schwachen Kollisionsresistenz erfüllt. Sie können sich in ihrer Argumentation auch auf aus der Vorlesung bekannte Probleme und deren Lösbarkeit beziehen. (4P.)

c3) Prüfen Sie, ob die Funktion $f(x)$ das Kriterium einer starke Kollisionsresistenz erfüllt. Sie können sich in ihrer Argumentation auch auf aus der Vorlesung bekannte Probleme und deren Lösbarkeit beziehen. (4P.)

d) Gegeben sei folgendes Blockschaltbild eines Zufallszahlengenerators. Dieser besteht aus der Hashfunktion SHA-256 und einem Linearen-Feedback-Schift-Register (LFSR). Der 10-Bit Ausgang der LFSR (x) wird mit einer 502 bit großen Nonce (N) konkanteniert und danach durch die Hashfunktion $g(x)$ zu einer 256-bit Zufallszahl komprimiert $z = g(x|N) = \text{SHA256}(x|N)$.



d1) Handelt es sich hierbei um einen deterministischen, echten oder hybriden Zufallszahlengenerator? Begründen Sie ihre Aussage. (1P.)

d2) Bestimmen Sie das primitive Polynom $P(x)$, auf dem der LFSR beruht.(1P.)

d3) Wieviele verschiedene Ausgabewerte generiert dieser Zufallszahlengenerator, wenn N einmalig gesetzt wird und statisch ist? (1P.)

d4) Erfüllt dieser Zufallszahlengenerator die Kriterien für einen krypotgraphischen Zufallszahlengenerator, wenn man diesen zum Generieren von einmalig maximal 256 Zufallswerten benutzen möchte? (1P.)