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

Probeklausur Security (LV4120)

Sommersemester 2023

Nachname: **Mustermeier**	Vorname: **Theo**
Matrikelnummer: **VOID**	
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:

Aufgabe 1: (10 Punkte)

Beantworten Sie bitte folgende Fragen (je 1 P):

Frage	**Antwort**
Ist IT-Sicherheit ein Bestandteil von Informationssicherheit?	**Ja**
Was ist ein Asset?	**Ein Asset ist alles (materielle oder immaterielle) von besonderem Wert.**
Zu welcher Klasse (Anwender, Hacktivist, Kriminelle ,...) von Angreifern gehört ein Botnet?	**Zu keiner Klasse da es kein Mensch ist.**
Ist Assembler eine architekturabhängige Programmiersprache?	**Ja**
Wird Phishing immer nur mit Hilfe von Emails ausgeführt?	**Nein**
Was sichern Schutz- oder Sicherheitsziele ab?	**Werte und Assets**
Was ist der Hauptinhalt vom BSI Dokument 200-4?	**Business Continuity Management**
Wofür steht PDCA?	**Plan, Do, Check, Act**
Kann das Sicherheitsziel Vertraulichkeit mit Hilfe einer Hash-Funktion und einem Geheimnis erfüllt werden?	**Nein**
Ist eine MAC eine symmetrische Signatur und gleichwertig zu einer asymmetrischen Signatur?	**Nein, eine MAC ist keine Signatur und sie erfüllt nur das Schutzziel Authentizität und nicht Verbindlichkeit.**

Aufgabe 2: (20 Punkte)

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

- **Autorisierung -> Authorization**
- **Verbindlichkeit -> Non-Repudiation**

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

b1) Bestimmung der Assets im zu analysierenden System.

b2) Bestimmung der Schutz-/Sicherheitsziele pro Asset.

b3) Bestimmung des Schadens, wenn das Schutzziel verletzt wird.

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

- **Damage (Schaden): Wie schwer ist der verursachte Schaden durch den Angriff?**
- **Reproducibility (Reproduzierbarkeit): Wie leicht lässt sich der Angriff reproduzieren/anwenden/wiederholen?**
- **Exploitability (Ausnutzbarkeit): Wie schwer ist es, den Angriff durchzuführen?**
- **Affected users (Betroffene): Wie viele Personen/Systeme/Komponenten sind vom Angriff betroffen?**
- **Discoverability (Auffindbarkeit): Wie einfach kann die Angriffsprozedur gefunden werden?**

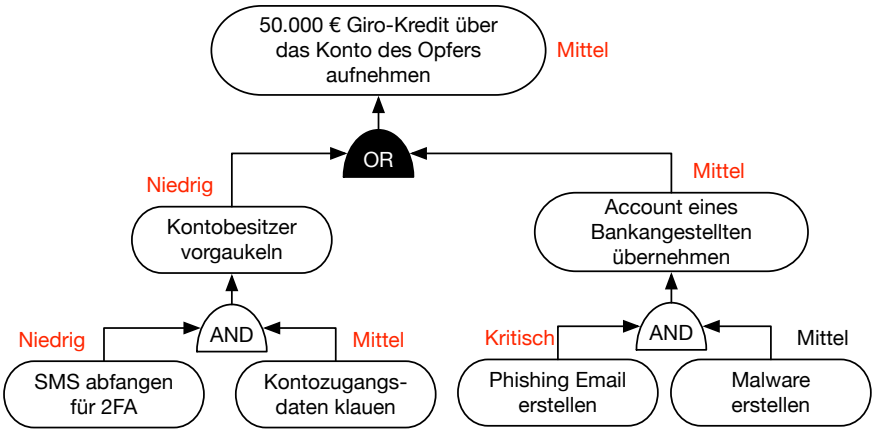
d) Vervollständigen Sie Eintrittswahrscheinlichkeiten des gegebenen Angriffsbaums auf der nächsten Seite. Nutzen Sie für die Bestimmung der drei Blattknoten ohne Angaben die gegebene Beschreibung und das HEAVENS Modell, welches Sie aus der Vorlesung kennen. Vervollständigen Sie erst die Eintrittswahrscheinlichkeit 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	**Physikalisch (0)**	Internet (3)
Expertise	**Experte (1)**	**Laie (3)**
Wissen über das Ziel	Geheim (0)	Öffentlich (3)
Benötigte Geräte	Standard (3)	**Standard (3)**
Summe	**Niedrig (4)**	**Kritisch (12)**

a) Zugriffsmöglichkeiten: Physikalisch, weil der Angreifer direkten Zugriff auf das Mobiltelefon haben muss.
a) Expertise: Experte, weil man Zugriff auf die SMS bekommen muss, selbst wenn der Angreifer das Mobiltelefon physisch hat.
b) Expertise: Laie, es existieren Werkzeug zum Erzeugen von Phishing Email ohne spezielles Wissen.
b) Benötigte Geräte: Standard, Es wird nur ein Rechner mit Internetverbindung benötigt.


50.000 € Giro-Kredit über das Konto des Opfers aufnehmen
Mittel
OR
Niedrig
Kontobesitzer vorgaukeln
Mittel
Account eines Bankangestellten übernehmen
Niedrig
AND
Mittel
SMS abfangen für 2FA
Kontozugangs-daten klauen
Kritisch
AND
Mittel
Phishing Email erstellen
Malware erstellen

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 Chiffre werden bei polyalphabetischen Substitution Chiffre nicht nur ein geheimes Alphabet zum Ersetzen der Buchstaben des ursprünglichen Alphabete verwendet, sondern viele („poly“) Geheimalphabete.

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

A Ciphertext-Only: Der Angreifer hat nur Zugriff auf Ciphertexte.

B Known-Plaintext: Der Angreifer hat Zugriff auf passende Plaintext und Ciphertext-Paare.

C Chosen-Plaintext: Der Angreifer hat Zugriff auf ein Verschlüsselungsorakel, das beliebige Plaintexte verschlüsselt.

D Chosen-Chiphertext: Der Angreifer hat Zugriff auf ein Entschlüsselungsorakel, das beliebige Ciphertexte entschlüsselt.

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.)
$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$.

d2) Was ist die Ordnung oder Kardinalität der Gruppe $\mathbb{Z}_5^*$? (1P.)
$|\mathbb{Z}_7^*|$ **=6.**

d3) Begründen Sie, warum $\mathbb{Z}_7^*$ kein Körper ist sondern nur eine Gruppe. (2P.)
$\mathbb{Z}_7^*$ **hat als Operator nur Multiplikation als Operator auf der Menge. Ein Körper hat neben der Multiplikation auf die Operation Addition als Mengenoperator.**

d4) Erläutern Sie, was ein Generator in einer zyklischen Gruppe ist. (1P.)
Ein Generator ist ein Element α **einer zyklischen Gruppe, welches die gleiche Ordnung hat, wie die Ordnung der Gruppe.**

d5) Zeigen Sie, dass das Element α=3 in $\mathbb{Z}_7^*$ ein Generator der zyklischen Gruppe ist. (3P.)
$\alpha^1 = 3 \mod 7 \equiv 3$
$\alpha^2 = 9 \mod 7 \equiv 2$
$\alpha^3 = 27 \mod 7 \equiv 6$
$\alpha^4 = 81 \mod 7 \equiv 4$
$\alpha^5 = 243 \mod 7 \equiv 5$
$\alpha^6 = 729 \mod 7 \equiv 1$

$\rightarrow ord(\alpha) = |\mathbb{Z}_5^*| = 6$

d6) Berchenen Sie das inverse Element zu 23 über $\mathbb{Z}_7^*$. (5P.)
$23^{-1} \mod 7 \equiv 2^{-1} \mod 7 \equiv 2^{7-2} \mod 7 \equiv 2^5 \mod 7$
$\equiv 32 \mod 7 \equiv 4 \mod 7$
Das inverse Element zu 23 über $\mathbb{Z}_5^*$ ist 4.

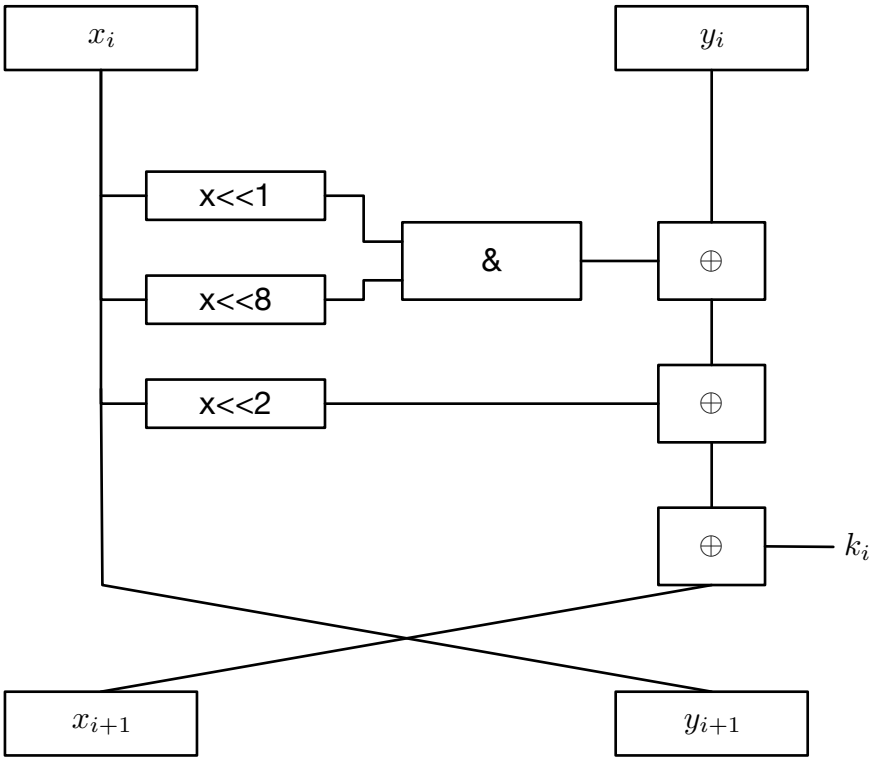
Aufgabe 4: (20 Punkte)

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.)
`SIMON` ist ein Feistel-Cipher.

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

- **Der Plaintext wird in zwei Blöcke (L und R) aufgeteilt, die nach jeder Runde vertauscht werden.**
- **Die Ver- und Entschlüsselung kann mit den gleichen Rundenfunktionen $f(x)$ ausgeführt werden.**
- **Das Design von der Rundenfunktion ist schwieriger als bei SPN-Chifferen.**

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

Alice		**Bob**
Wähle $a =\in \{2, \ldots, p-2\}$		**Wähle** $b =\in \{2, \ldots, p-2\}$
Berechne $A \equiv g^a \mod p$		**Berechne** $B \equiv g^b \mod p$
	$\xrightarrow{A \equiv g^a \mod p}$	
	$\xleftarrow{B \equiv g^b \mod p}$	
$K_{AB} = B^a \mod p$		$K_{AB} = A^b \mod p$
	$\xleftrightarrow{C = ENC_{K_{AB}}(P)}$	

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.)
Berechnung der öffentlichen Schlüssel:
$B = g^b \mod p = 3^3 \mod 7 \equiv 27 \mod 7 \equiv 6$
$A = g^a \mod p = 3^4 \mod 7 \equiv 81 \mod 7 \equiv 4$

Bob berechnet den $K_{Session}$:
$K_{Session_{Bob}} = A^b \mod p \equiv 4^3 \mod 7 \equiv 64 \mod 7 \equiv 1 \mod 7$

Bob berechnet den $K_{Session}$:
$K_{Session_{Alice}} = B^a \mod p \equiv 6^4 \mod 7 \equiv 1296 \mod 7 \equiv 1 \mod 7$

$\rightarrow K_{Session_{Bob}} = K_{Session_{Alice}}$

Aufgabe 5: (20 Punkte)

a) Erklären Sie, was schwache Kollisionsresistenz ist. (2P.)
Bei schwacher Kollisionsresistenz (second pre-image resistance) darf es nicht möglich sein, zu einem m ein anderes m' zu finden mit $m \neq m'$ und $H(m) = H(m')$.

b) Erklären Sie, was starke Kollisionsresistenz ist. (2P.)
Bei starke Kollisionsresistenz (collision resistance) darf es nicht möglich sein, zwei beliebige m und m' zu finden mit $m \neq m'$ und $H(m) = H(m')$

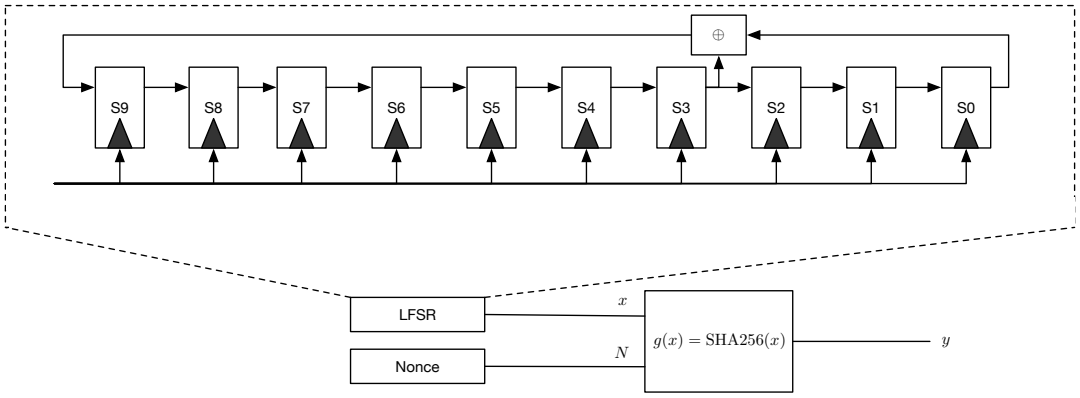
c) Gegeben sei folgende Funktion $f(x) = (g^x \mod N) \mod 2^{192}$, mit $N = p \cdot q$. Die Basis g ist bekannt, p und q sind unbekannte Primzahlen, der 2048-bit große Modulus N ist bekannt.

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.)
Die Einwegeigenschaft ist gegeben, da wir die Invertierbarkeit von $f(x)$ auf das diskrete Logarithmenproblem zurückführen können: Um $f(x)$ zu invertieren, müssten wir $x = log_g f(x) \mod N$ berechnen. Für große Werte von N (2048-bit) stoßen wir hier allerdings auf rechnerische Probleme, da wir das diskrete Logarithmenproblem für das Finden der Inversen lösen müssten, welches für große Werte als schwer bekannt ist. Da wir $f(\cdot)^{-1}$ also nicht empirisch berechnen können, ist die Einwegeigenschaft von $f(x)$ gegeben.

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.)
Die schwache Kollisionsresistenz ist gegeben, da wir $\phi(N) = \phi(p) \cdot \phi(q) = (p-1) \cdot (q-1)$ nicht berechnen können, da die Primzahlen p und q nicht bekannt sind. Das hier vorliegende Problem lässt sich auf das Problem der Faktorisierung mit großen Primzahlen zurückführen.

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.)
Die starke Kollisionsresistenz ist gegeben, da wir das Problem des Findens einer Kollision zwischen zwei beliebigen 192 bit langen Ausgaben der Funktion $f(x)$ mit dem Geburtstagsparadoxon abschätzen können und der rechnerische Aufwand zum Finden einer Kollision bei $2^{\frac{192}{2}} = 2^{96}$ ist. Damit liegt der rechnerirsche Aufwand über 2^{80}, was aktuell als sicher gilt.

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.)
Jedes y ist mit der Kenntnis von N und x berechenbar und deswegen ist es ein deterministischer Zufallszahlengenerator.

d2) Bestimmen Sie das primitive Polynom $P(x)$, auf dem der LFSR beruht.(1P.)
$P(x) = x^{10} + x^3 + 1$**.**

d3) Wieviele verschiedene Ausgabewerte generiert dieser Zufallszahlengenerator, wenn N einmalig gesetzt wird und statisch ist? (1P.)
Dieser Zufallszahlengenerator generiert $2^{10} - 1 = 1023$ **verschiedene Ausgabewerte, da sich nur die Ausgabe des LFSR ändert.**

d4) Erfüllt dieser Zufallszahlengenerator die Kriterien für einen krypotgraphischen Zufallszahlengenerator, wenn man diesen zum Generieren von einmalig maximal 256 Zufallswerten benutzen möchte? (1P.)
Ja, da durch die Hashfunktion und dem LFSR die Nichtvorhersehbakreit und die Bedingung der Gleichverteilung erfüllt ist. Hinzu kommt, dass durch die Eigenschaften der Hashfunktion und die zufällig gewählt Nonce die einzeln erzeugten Zufallszahlen unabhängig voneinander wirken.