

Take-Home-Klausur Security by Design

Name: Radloff Vorname: Matz
 Matr.-Nr.: 6946325 Studiengang: Informatik

Ihre Bearbeitung der folgenden 4 Aufgaben ist nach spätestens **180 Minuten** einzureichen. Insgesamt können 64 Punkte erreicht werden. Die Lösung ist **handschriftlich** und **eigenhändig ohne fremde Hilfe** anzufertigen. Als Hilfsmittel zugelassen sind sämtliche schriftlichen Unterlagen sowie ein nicht programmierbarer Taschenrechner. Bitte antworten Sie kurz, stichpunktartig und präzise.

Falls Sie über einen Drucker verfügen, können Sie diese Aufgabenstellung im Format DIN A4 ausdrucken und ihre Lösung darauf anfertigen. Ansonsten nutzen Sie bitte weißes, ggf. kariertes Papier im Format DIN A4 zur Lösung der Aufgaben. Bitte **bewahren** Sie das **Papier** Ihrer schriftlichen Bearbeitung auch nach der Klausur **auf**.

Alle Lösungsblätter sind von Ihnen mit einem Scanner, einer Scan-App oder notfalls einer Fotokamera zu digitalisieren und in einer PDF-Datei zu speichern. Bitte **überprüfen** Sie die PDF-Datei auf **gute Lesbarkeit und Vollständigkeit**. Spätestens bis zum Ablauf der 180 Minuten ist Ihre Bearbeitung als PDF-Dokument im Moodle einzureichen: <https://lernen.min.uni-hamburg.de/course/view.php?id=1065>. Der letztmögliche Zeitpunkt der Abgabe ist im Moodle angegeben. Sollte eine Abgabe im Moodle aus technischen Gründen nicht möglich sein, können Sie Ihre Bearbeitung **notfalls** per E-Mail einreichen: wichmann@informatik.uni-hamburg.de. Auch in diesem Fall ist der **Zeitpunkt des Empfangs durch den Informatik-Mailserver** bindend. Der Zeitraum von 180 Minuten umfasst bereits einen Puffer für eventuell auftretende technische Probleme. Eine Verlängerung dieses Zeitraumes kann daher nicht gewährt werden.

Während dieser Klausur steht der Zoom-Raum der Vorlesung zur Verfügung: <https://uni-hamburg.zoom.us/j/99114889675?pwd=WXc5ZVRFZWw5QzQvc2RUeUc1QIB6UT09>. Dort werden ggf. einzelne organisatorische Bearbeitungshinweise gegeben und es besteht die Möglichkeit, im Chat oder in Breakout-Räumen Rückfragen an die Lehrenden zu stellen.

Folgende Eigenständigkeitserklärung ist von Ihnen zwingend mit der Unterschrift zu bestätigen. Sollten Sie nicht über einen Drucker verfügen, geben Sie diese Erklärung im **identischen Wortlaut** in Ihrer handschriftlichen Bearbeitung ab.

Hiermit versichere ich, Matz Radloff
 (Vorname Nachname), dass ich die vorliegende Prüfungsleistung eigenständig erbracht
 und ausschließlich unter Verwendung der erlaubten Hilfsmittel bearbeitet habe.

M. Radloff (Unterschrift)

Viel Erfolg!

Aufgabe	1	2	3	4	Summe
Punkte					

1)

a)

C1: Substitution, da jedes Zeichen des Klartexts in der gleichen Reihenfolge mit einer Farbwert ersetzt wird. Sie ist polyalphabetisch, weil pro Zeichen aus f aus mehreren möglichen Farben ausgewählt wird. Sie ist monoalphabetisch, da immer nur ein Zeichen und keine Zeichengruppen ersetzt werden.

C2: Produktchiffre, zusammengesetzt aus einer monoalphabetischen und monoalphabetischen Substitution und einer freien Permutation - Transposition, weil einen Zeichen nur eine Farbe zugeordnet ist, und weil alle Pixelpositionen ~~jetzt~~ auf einmal getauscht werden; nicht pro Zeile oder Block.

C3: ~~Produktchiffre aus einer polyalphabetischen und polygraphischen Substitution und einer Spaltentransposition~~, der ~~jedes~~ Zeichen durch das zu fällige r ; mehrere Zuweisungen besitzt. Polygraphisch, weil jeweils drei Zeichen zu einem verschlüsselten Wert gepackt werden. Transposition, weil die Pixel spaltenweise gepackt werden.

C4: Produktchiffre aus einer monoalphabetischen (weil Z-fallweise pro Zeichen polyalphabetischen (weil durch Z-falls Wert gleich es mehrere Abbildungen pro Klartextzeichen) und polygraphischen (J-Werte pro Farbe) Substitution und einer Spaltentransposition (J-spalten werden vertauscht).

- b) Durch eine Häufigschaftsanalyse könnte man zuerst die Zuordnung von Zeichen zu Farbe herausfinden. Danach könnte man durch zufällige Permutationen versuchen eben Häufigkeit zu erhalten.
- c) Da jedes Zeichen an jede beliebige andere Stelle getauscht werden kann gibt es $n!$ mögliche Verkennungen.
- d) Nein, da es in menschlichen Sprachen nur bestimmte Anordnungen von Zeichen gibt, die den Suchraum stark verringern.
- e) ~~Nein~~, ^{nein} zwar, weil die Zuflusswerte v_i unabhängig erzeugt werden und man so keine Rückschlüsse auf das verschlüsselte Zeichen ziehen kann, aber durch die Bedingung $PQ(z_i) + v_i$ für haben Zeichen mit höherer Position auch eine durchschnittlich höheren verschlüsselten Wert. So können Rückschlüsse gezogen werden und die Chiffre ist nicht informationstheoretisch sicher.

2)

a)

$$m = 011 \cancel{110} 01010$$

L

R

 k_1

F

$$\text{Runde 0: } 0110 \quad 1010$$

$$\text{Runde 1: } 1010 \quad 1000 \quad 0100 \quad (1010 \oplus 0100) \wedge 1110 = \cancel{1110}$$

$$\text{Runde 2: } 1000 \quad 1000 \quad 1011 \quad (1000 \oplus 1011) \wedge 1010 = 0010$$

$$\text{Runde 3: } 1000 \quad 1110 \quad 1110 \quad (1000 \oplus 1110) \wedge 1110 = 0110$$

Ausgabe: 1110 1000

b)

~~$$\text{Runde 1: } 1000 \quad 0010 \quad 0100 \quad (1000 \oplus 0100) \wedge 1110 = 1100$$~~

~~$$\text{Runde 2: } 0010 \quad 0000 \quad 1011 \quad (0010 \oplus 1011) \wedge 1110 = 1000$$~~

~~$$\text{Runde 3: } 0000 \quad 1100 \quad 1110 \quad (0000 \oplus 1110) \wedge 1110 = 1110$$~~

b)

$$\text{Runde 1: } 1000 \quad 1000 \quad k_1 = 1110 \quad (1000 \oplus 1110) \wedge 1110 = 0110$$

$$\text{Runde 2: } 1000 \quad 1010 \quad k_2 = 1011 \quad (1000 \oplus 1011) \wedge 1110 = 0010$$

$$\text{Runde 3: } 1010 \quad 0110 \quad k_3 = 0100 \quad (1010 \oplus 0100) \wedge 1110 = 1110$$

Ausgabe 01101010

c) Da das letzte Bit 0 immer mit über XOR mit dem letzten Bit von L verarbeitet wird, kommt dabei immer dieses letzte Bit unverändert heraus:

$$X \oplus 0 = X$$

d) Da F beliebig kompliziert gewählt werden kann, nicht linear sein sollte und nicht umkehrbar sein muss, kann ein hohes Sicherheitsniveau erreicht werden (z.B. Einwegfunktion). Da das letzte Bit der jeweiligen Hälfte L unverändert bleibt, können Rückschlüsse auf den Klartext gezogen werden, und erweitert das Rückwärtsverfahren von F.

D)

- a) In einem hierarchischen Zeitstiftversorgungssystem wird immer nur eine Richtung zertifiziert, sodass ein eindeutiger Pfad entsteht. ~~Um aufzubauen~~ wird ein Schlüssel immer nur von einer Stelle zertifiziert.

Im Web of Trust werden Schlüssel von mehreren Stellen zertifiziert, sodass mehrere Pfade entstehen und alle Teilnehmer gleichzeitig gleich wichtig sind.

- b) ~~Web~~ Ein Vorteil der hierarchischen Zertifizierung ist die klare Zuverlässigkeit im Falle eines Konflikts.
Ein Web of Trust hat den Vorteil, dass es einfacher zu nutzen ist, da jeder Teilnehmer von jedem anderen zertifiziert werden kann.

- c) Es reicht, wenn C_{A_2} vertraut wird, da das transitive Vertrauen bedeutet, dass C_{A_1} automatisch vertraut wird.

- d) Explizit muss C_{A_2} und C_{A_3} vertraut werden. Durd C_{A_3} wird transitiv auch C_{A_4} vertraut und mit C_{A_4} und C_{A_2} auch C_{A_1} .

- e) C_{A_4} wurde von C_{A_1} zertifiziert, kann also durch C_{A_1} ersetzt werden. Über Zeitstempel kann sichergestellt werden, dass C_{A_4} C_{A_3} vor der Komprimierung zertifiziert hat.

- f) Vorteile: Einfache Nutzung, da automatisch. Schritt gut, solange der erste Schlüssel korrekt ist.

Nachteile: Anfällig für Mitmehrgriff bei initialen Kontakt.

Bei legitimer Schlüsseländerung müssen alle Kommunikationspartner den Schlüssel manuell tauschen.

4)

- a) Im VPN wird von ~~dem~~ der Firma festgelegter DNS-Server verwendet, der angefragte Domain-Namen zu IP-Adressen auflost. Stattdessen korrekten Adressen gibt dieser hier die IP-Adresse der internen Firmen ~~seite~~ zurück
DNS (Domain Name System) (-Spoofing)

b)

Vertraulichkeit, da die Firma die (DNS-) Anfragen mitlesen kann.

Integrität, da eine falsche Website über augenscheinlich korrekten Domain zugeordnet werden kann und so potentiell eine gefälschte Seite aufgerufen wird.

Verfügbarkeit, da ~~die~~ Kommunikation geblockt werden kann.

- c) HTTPS stellt sicher, dass ~~der~~ der Server der Webseite für die angefragte Domain zertifiziert ist und verschlüsselt den Datenverkehr mit TLS.

- d) Staatl. Aut. können ISPs (Internet Service Provider) unter Umständen zwingen Datenverkehr am bestimmt IP-Adresse zu blockieren (z.B. externe DNS-Server) oder eigene DNS-Server so zu manipulieren, dass bestimmte Domains nicht in IP-Adressen umgewandelt werden können.

- e) Die Benutzung eines separaten DNS-Servers würde die korrekte Website-IP erreichen. Falls diese auch blockiert werden könnte man für (DNS-) Anfragen ein weiteres VPN oder einen Proxy-Server verwenden.