Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Übungsklausur

Einführung IT Security

Name:

Matrikelnr.:

Für die Klausur sind keine Hilfsmittel zugelassen.

Gesamtpunktzahl: **/90** Note:

Name:
Matrikelnr.:

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Aufgabe 1 — 15 Punkte

Aufgabe 1.1

Nennen Sie drei Schutzziele (Sicherheitsbegriffe) und erläutern Sie diese kurz (ein Satz pro Begriff).

Aufgabe 1.2

Erläutern Sie kurz den Unterschied zwischen (historischen) Substitutionschiffren und (historischen) Transpositionschiffren.

Aufgabe 1.3

Ist aus heutiger Sicht eine Transpositionschiffre sicher? Begründen Sie Ihre Antwort.

Aufgabe 2 — 10 Punkte

Gegeben sei die folgende Blockchiffre mit Blocklänge $n = 4$ für einen gegeben Schlüssel k durch die folgende Tabelle:

Klartext		Chiffrat	Klartext		Chiffrat
0000	$\leftrightarrow$	0010	1000	$\leftrightarrow$	0011
0001	$\leftrightarrow$	0101	1001	$\leftrightarrow$	1101
0010	$\leftrightarrow$	1111	1010	$\leftrightarrow$	1110
0011	$\leftrightarrow$	0111	1011	$\leftrightarrow$	1100
0100	$\leftrightarrow$	1010	1100	$\leftrightarrow$	0100
0101	$\leftrightarrow$	1001	1101	$\leftrightarrow$	0001
0110	$\leftrightarrow$	0000	1110	$\leftrightarrow$	1000
0111	$\leftrightarrow$	0110	1111	$\leftrightarrow$	1011

Der Klartext

$p = 1000\,0100\,1101\,1001\,1011$

soll im CBC-Modus mit dem Initialisierungsvektor

$IV = 0101$

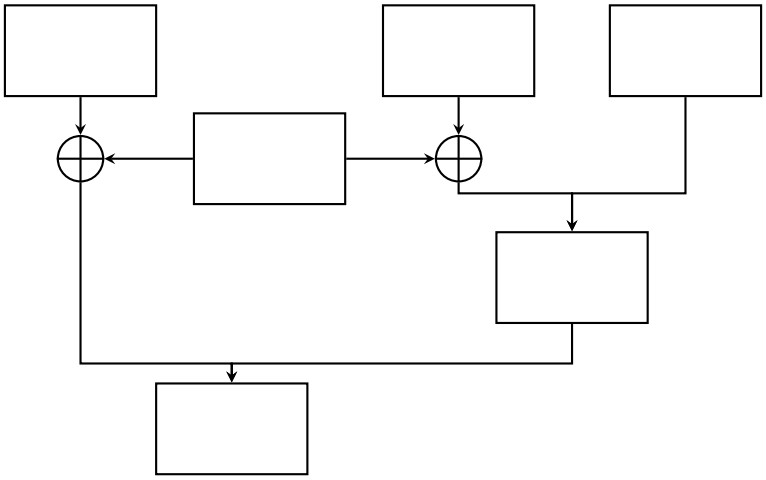
verschlüsselt werden.

Berechnen Sie das entstehende Chiffrat und geben Sie es (ohne IV) an.

Aufgabe 3 — 10 Punkte

Aufgabe 3.1

Ergänzen Sie das folgende Schaubild zur Berechnung eines HMAC und geben Sie eine Legende an, in der Sie die von Ihnen verwendeten Abkürzungen ausführen.



Aufgabe 3.2

Nennen Sie zwei Eigenschaften eines HMAC und zwei Unterschiede zu Digitalen Signaturen.

Aufgabe 4 — 15 Punkte

Städtische Büchereien verwenden häufig das Geburtsdatum als Passwort für Kundenkonten.

Aufgabe 4.1

Berechnen Sie die Entropie eines solchen Passworts. Nehmen Sie dafür an, dass jeder Monat 32 Tage und jedes Jahr 16 Monate hat. Nehmen Sie außerdem an, dass die Kunden zwischen 0 und 127 Jahre alt sind und jeder mögliche Geburtstag gleich wahrscheinlich ist.

Aufgabe 4.2

Führen die in Aufgabenteil 5.1 gemachten Angaben dazu, dass Sie die Entropie des Passwort über- oder unterschätzt haben? Würden Sie ein Passwort mit der von Ihnen berechneten Entropie für den praktischen Einsatz empfehlen? Begründen Sie Ihre Antworten kurz.

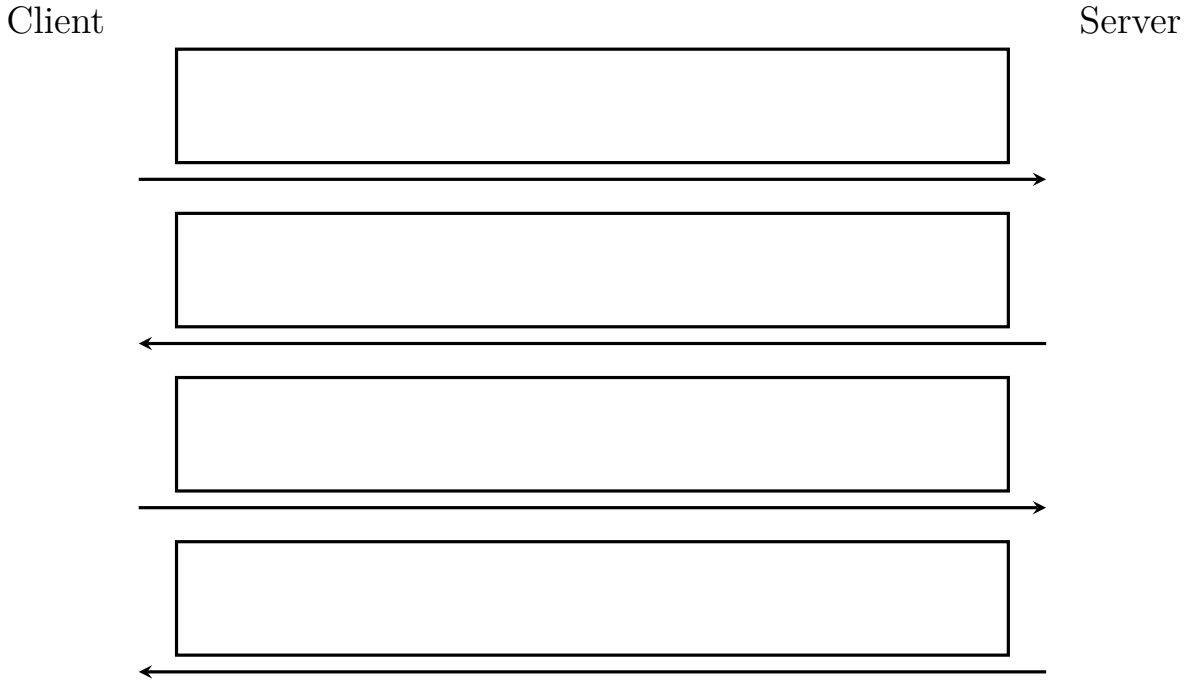
Aufgabe 4.3

Welche Gründe, unabhängig von der Entropie, können dagegen sprechen, das Geburtsdatum als Passwort zum Schutz von Kundenkonten zu verwenden. Nennen Sie zwei Gründe, die dagegen sprechen.

Aufgabe 5 — 15 Punkte

Aufgabe 5.1

Ergänzen Sie das folgende Schema der ersten vier Nachrichten eines SSH-Verbindungsaufbaus



Aufgabe 5.2

Erläutern Sie kurz die Inhalte der erste Nachricht (Client zu Server) und der zweite Nachricht (Server zu Client). Worauf haben sich Client und Server nach diesen beiden Nachrichten geeinigt?

Aufgabe 5.3

Wozu dienen die dritte Nachricht (Client zu Server) und die vierte Nachricht (Server zu Client)?

Aufgabe 6 — 15 Punkte

Bei SSH als auch TLS für der öffentliche Schlüssel des Servers für die Authentifizierung eingesetzt.

Aufgabe 6.1

Erläutern Sie kurz den Unterschied bei der Prüfung des öffentlichen Schlüssels des Servers bei einem SSH-Verbindungsaufbau zu der Prüfung des öffentlichen Schlüssels des Servers bei einem TLS-Verbindungsaufbau.

Aufgabe 6.2

Erläutern Sie kurz die zentrale Aufgabe eines Zertifikats.

Aufgabe 6.3

Erläutern Sie kurz, welche Rolle eine Certificate Revocation List (CRL) bei der Prüfung eines Zertifikats spielt.

Aufgabe 6.4

Nennen Sie zwei Vorteile und zwei Nachteile von Authentifizierungsverfahren, die biometrische Merkmale nutzen.

Aufgabe 7 — 10 Punkte

Geben Sie für die folgenden Aussagen an, ob die Aussage wahr oder falsch ist.

Hinweis zur Punktevergabe: Eine korrekte Antwort wird mit 1 Punkt bewertet, eine falsche Antwort wird mit -1 Punkt bewertet. Die Gesamtpunktzahl der Aufgabe ist dabei am Ende mindestens Null, es gibt also keine negative Gesamtpunktzahl für die Aufgabe.

Wahr	Falsch	
☐	☐	Eine Chiffre mit längerem Schlüssel ist immer besser als eine Chiffre mit kürzerem Schlüssel, da mehr verschiedene Schlüssel möglich sind und ein Brute-Force-Angriff erschwert wird.
☐	☐	Bei einer Blockchiffre im CBC-Modus kann der IV im Klartext übertragen werden, ohne die Sicherheit des Verfahren zu verringern.
☐	☐	Mit dem Begriff *Snake Oil* bezeichnet am häufig besonders sichere Verschlüsselungsverfahren.
☐	☐	Eine Stromchiffre schützt nicht nur die Vertraulichkeit sondern auch die Integrität.
☐	☐	In der Praxis werden symmetrische und asymmetrische Verfahren oft zu sogenannten hybriden Verschlüsselungsverfahren kombiniert. Das symmetrische Verschlüsselungsverfahren dient dabei dem Schlüsselaustausch.
☐	☐	Der Empfänger einer mit MAC geschützten Nachricht kann damit einem Dritten nicht zweifelsfrei nachweisen, dass der Sender genau diese Nachricht geschickt hat.
☐	☐	Ein Protokoll hat möglicherweise mehr als zwei Parteien als Protokollteilnehmer.
☐	☐	Die Sicherheit des Diffie-Hellman-Schlüsselaustauschs und des Verschlüsselungsverfahrens RSA beruhe beide auf dem *dlog*-Problem.
☐	☐	SFTP ist das Kürzel für FTP über SSH.
☐	☐	In einem Informationssicherheitsmanagementsystem (ISMS) nach IT-Grundschutz des BSI ist der oder die Informationssicherheitsbeauftragte für die Informationssicherheit verantwortlich.

Hinweis zum Ausfüllen: Wenn Sie Ihre Auswahl ändern möchten, füllen Sie das Feld Ihrer alten, zu korrigierenden Auswahl vollständig aus und kreuzen Sie Ihre neue Auswahl an. Möchten Sie erneut korrigieren, so füllen Sie das Feld Ihrer zweiten, zu korrigierenden Auswahl vollständig aus (jetzt sind beide Felder ausgefüllt), und treffen Sie Ihre neue Auswahl durch einen Kreis um das entsprechende Feld.