4

502470 - Einführung in Sicherheit und Privatheit

Übung: Grundlagen der Kryptographie

— Disskussion der Lösung während der Übung: 04. Juli 2019 —

1 Grundlagen

Frage 1: Erklären Sie kurz was unter Kryptographie, Kryptoanalyse, Kryptologie und Steganographie verstanden wird.

Frage 2: Nach welchen Kriterien lassen sich Kryptosysteme einteilen?

2 Kryptoanalyse

Frage 3: In der Kryptoanalyse lassen sich im Allgemeinen Angriffe auf kryptografische Systeme danach klassifizieren, welche Informationen einem Kryptoanalytiker über das System zur Verfügung stehen.

a) Welche Angriffsarten lassen sich nach dem Kenntnisstand oder der Wahl von Nachrichten unterscheiden?

b) Was wird durch solche Angriffe erreicht?

Frage 4: Im Dateiverzeichnis zur Vorlesung finden Sie eine Textdatei **„enc_msg.txt“**. Diese Textdatei beinhaltet einen verschlüsselten Text, der mit der Substitutionschiffre verschlüsselt wurde. Ihre Aufgabe ist es nun, das Chiffrat zu entschlüsseln, um damit den ursprünglichen Klartext zu erhalten. Bearbeiten Sie hierzu folgende Teilaufgaben:

a) Bestimmen Sie die relativen Häufigkeiten für die Buchstaben A bis Z inklusive der Umlaute und dem Eszett des Chiffrates.

b) Entschlüsseln Sie einen der Absätze des Chiffrates aus der Textdatei **„enc_msg.txt“** unter Zuhilfenahme der folgenden Tabelle. Die Tabelle repräsentiert die Verteilung der relativen Häufigkeiten des deutschen Alphabets ohne andere Zeichen (Prozentangaben). Das bedeutet, dass die von Ihnen bestimmten relativen Häufigkeiten etwas von den in der Tabelle dargestellten Werten abweicht.

c) Geben Sie die verwendete Substitutionstabelle an.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

P	Q	R	S	T	U	V	W	X	Y	Z	Ä	Ö	Ü	ß

Buchstabe	rel. Häufigkeit	Buchstabe	rel. Häufigkeit	Buchstabe	rel. Häufigkeit
A	6.01	K	1.54	U	3.92
B	2.15	L	3.79	V	0.92
C	2.69	M	2.80	W	1.43
D	4.72	N	9.66	X	0.05
E	16.01	O	2.68	Y	0.11
F	1.83	P	1.05	Z	1.24
G	3.06	Q	0.03	Ä	0.55
H	4.25	R	7.74	Ö	0.27
I	7.75	S	6.34	Ü	0.68
J	0.30	T	6.37	ß	0.17

Quelle: `http://www1.ids-mannheim.de`

d) Über welche Persönlichkeit wird in der verschlüsselten Textdatei geschrieben?

e) Ist die Substitutionschiffre ein sicheres Verschlüsslungsverfahren? Begründen Sie Ihre Antwort.

Hinweis: Die Bearbeitung der Aufgaben kann elektronisch erfolgen. Sie könnten bspw. ein Programm schreiben, welches für Sie die relativen Häufigkeiten bestimmt. Es empfiehlt sich zudem während der händischen Entschlüsselung Klein- durch Großbuchstaben zu ersetzen.

Frage 5: Die CEASAR Chiffre auch bekannt als Verschiebechiffre ist ein antikes Verschlüsselungsverfahren, welches jeden Klartextbuchstaben durch einen anderen ersetzt. Durch die Verschlüsselung mit der Verschiebechiffre wird jedes Zeichen in einem geordneten Alphabet zyklisch um eine bestimmte Anzahl z.B. $k = 7$ nach rechts verschoben (z.B. $A \mapsto H, B \mapsto I, C \mapsto J, \dots$) und damit letztendlich der Klartext kodiert.

a) Gehen Sie davon aus, dass Ihnen das Alphabet von A bis Z, sowohl als Klartext als auch als Chiffrat vorliegt. Wie müssten Sie, wenn Sie eine Verschiebeverschlüsselung mit k=12 anwenden, sinnvoll die Buchstaben O bis Z des Chiffrats mit den Buchstaben des Klartextes belegen?

b) Verschlüsseln Sie das Wort „`Computersicherheit`“ mit der Verschiebechiffre und einem $k = 12$

c) Entschlüsseln Sie die Chiffre „`TVMZEXLIMX`“ mit dem Ihnen bekannten $k = 4$

d) Handelt es sich bei der Verschiebechiffre um ein sicheres Verfahren?

3 Asymmetrische Chiffren

Frage 6: Was ist die Grundidee asymmetrischer Chiffren?

Frage 7: Worauf beruht die derzeitige Sicherheit des RSA-Verfahrens?

Frage 8: In der Vorlesung wurden Ihnen bereits die Schritte zur RSA Schlüsselgenerierung vorgestellt. Zur Bearbeitung der folgenden Aufgaben sind zwei verschieden große Primzahlen mit $p = 11$ und $q = 23$ gegeben.

`Schritt 1: Erstellung des öffentlichen Schlüssels`

a) Berechnen Sie n

b) Berechnen Sie $\phi(n)$

c) Geben Sie die Bedingung an, die e erfüllen soll. Nehmen Sie folgend $e = 13$ an.

`Schritt 2: Erstellung des privaten Schlüssels`

d) Berechnen Sie d

e) Geben Sie den öffentlichen Schlüssel (e, n) und den privaten Schlüssel (d, n) an.

`Schritt 3: Ver- und Entschlüsseln von Nachrichten`

f) Sie wollen einen Klartext $M = 150$ mit der RSA-Verschlüsselung verschlüsseln, ist Ihnen dies mit dem zuvor berechneten n möglich?

g) Alice übersendet Ihnen den Chiffretext $C = 76$. Entschlüsseln Sie den Chiffretext mithilfe der RSA Entschlüsselung und ihrem zuvor berechneten d. Gehen Sie davon aus, dass es sich bei dem entschlüsselten Chiffretext um ein ASCII Zeichen handelt. Welches ASCII Zeichen hat Ihnen Alice übersendet?

Frage 9: Sie fangen eine verschlüsselte Nachricht $C = 22$ ab. Ihnen ist neben $n = 55$ auch der öffentliche Schlüssel $e = 7$ bekannt. Zur Entschlüsselung dieser verschlüsselten Nachricht C benötigen Sie jedoch auch den private Schlüssel d. Dieser lässt sich durch $d = e^{-1} \, mod \, \phi(n)$ berechnen. Zum Berechnen des Ihnen unbekannten privaten Schlüssels d benötigen Sie zudem die Kenntnis über die Ihnen unbekannten Primzahlen p und q. Ihnen ist jedoch bekannt, dass für $n = p * q$ gilt. Um nun die beiden Primzahlen p und q zu bestimmen, müssen Sie n faktorisieren.

a) Versuchen Sie nun die Verschlüsselung zu brechen indem Sie $n = 55$ faktorisieren (finden Sie die Primzahlen deren Produkt n ergibt).

$p =$ _____ $q =$ _____

b) Berechnen Sie den privaten Schlüssel d.

c) Entschlüsseln Sie nun die verschlüsselte Nachricht $C = 22$. Gehen Sie davon aus, dass es sich bei dem entschlüsselten Chiffrentext um ein ASCII Zeichen handelt. Welches ASCII Zeichen haben Sie abgefangen?

4 Digitale Signatur

Frage 10: Ergänzen Sie nachfolgenden Abschnitt.

Das Ziel der digitalen Signatur ist der _____ eines Dokumentes. Die Signaturverfahren sind analog zu Hashfunktionen. DSA, ECDA sind Beispiele für die _____ wohingegen RSA ein Beispiel für die _____ ist. Während der RSA-Ver- und Entschlüsselung steht K_{sig} für den _____ und K_{veri} für den öffentlichen Verifikationsschlüssel.

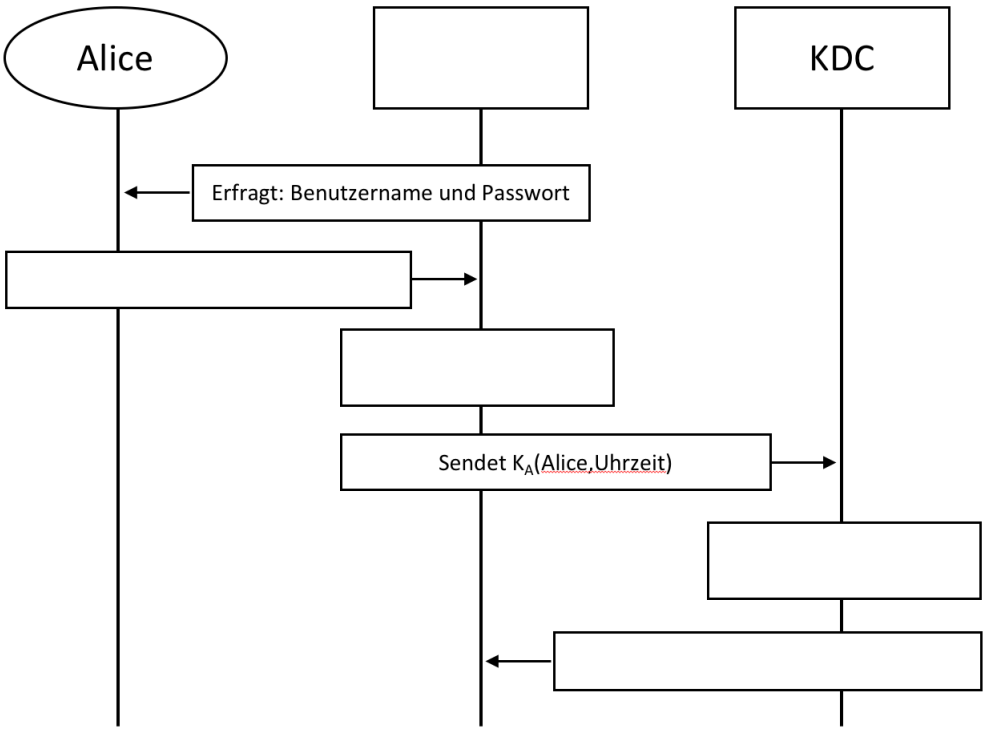
Frage 11: Warum werden für RSA nicht Nachrichten sondern Hash-Werte signiert?

Frage 12: Beschreiben Sie den typischen Ablauf einer RSA-Signatur.

5 Authentifikation von IT-Systemen durch IT-Systeme

Frage 13: Beschreiben Sie kurz die Grundlagen der symmetrischen Verschlüsselung. Gehen Sie dabei auch auf das Problem der sicheren Kommunikation ein.

Frage 14: Ergänzen Sie die fehlenden Bereiche der folgenden Abbildung die schematisch ein Kerberos-Authentifikationssystem repräsentiert. Entscheiden Sie zunächst um welche Version es sich auf der Darstellung handelt.

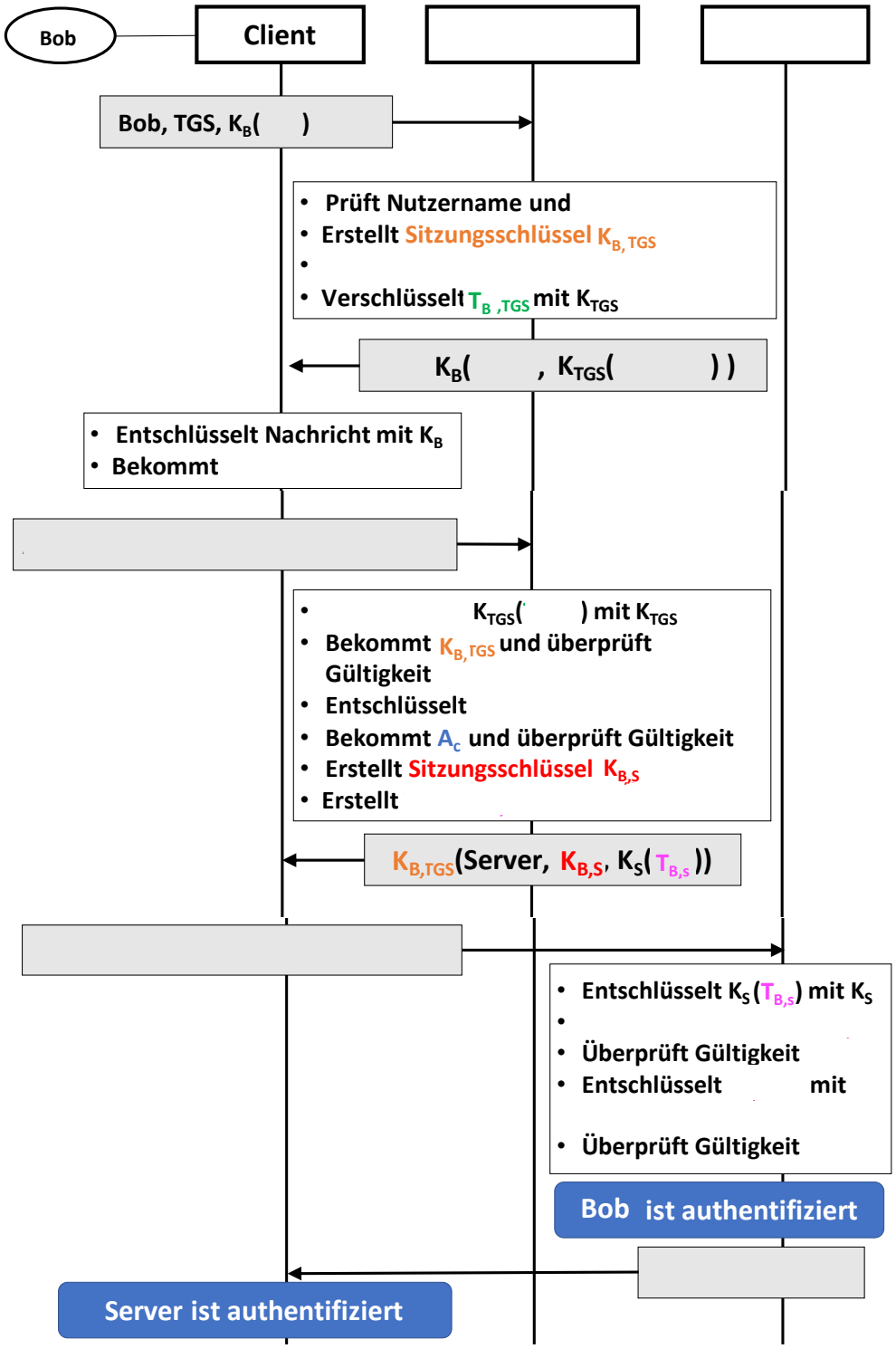


Frage 15: Innerhalb des Kerberos-Authentifikationssystems dienen Tickets zur authentifizierten Nutzung eines Dienstes und ermöglichen damit dem Clienten C auf einen Server S zuzugreifen. Was beinhaltet in diesem Zusammenhang ein Ticket und durch wen wird es ausgestellt? Beschreiben Sie zusätzlich das weitere Vorgehen mit diesem Ticket.

Frage 16: Worin besteht der Vorteil beim Einsatz von Tickets?

Frage 17: Nennen Sie Vor- und Nachteile von Kerberos.

Frage 18: Ergänzen Sie die fehlenden Inhalte des schematisch in folgender Abbildung dargestellten Protokolls des Kerberos-Authentifikationssystem.



Quelle: Diese Übung wurde teilweise inspiriert durch die Übung zur Vorlesung „Kryptografie und Datensicherheit I“ von Prof. Dr.-Ing. Christof Paar der Ruhr-Universität Bochum.