5. Handlungsschritt (20 Punkte)

Korrekturrand

In der MED GmbH soll zukünftig auch die Gesundheitskarte zum Einsatz kommen. In diesem Zusammenhang sollen Sie den Ärzten untenstehende Fragen zu Datensicherheit und Datenschutz beantworten, die die Ärzte zu folgendem Text haben.

Die elektronische Gesundheitskarte

Wie werden Gesundheitsdaten in Zukunft geschützt?

...

Hauptfunktionen

Die Prozessor-Chipkarte hat zwei Hauptfunktionen. Erstens fungiert sie als Authentifizierungswerkzeug. Dazu legt jeder Karteninhaber vor Erstverwendung eine persönliche Identifikationsnummer (PIN) nach Wahl fest. Die eigene PIN wird in verschlüsselter Form auf der Karte gespeichert.

...

Die zweite Funktion der Prozessorkarte ist die Durchführung der kryptografischen Verschlüsselungen aller Gesundheitsdaten des Versicherten. Einmal verschlüsselt, sind die Daten geschützt, unabhängig davon, wo sie sich gerade befinden. Alle Verschlüsslungen, die mit der Karte ausgeführt werden, sind vom Typ hybride Verschlüsselung.

...

Der geheime Schlüssel

Dass die gesundheitsrelevanten Informationen eines Versicherten geheim bleiben, steht und fällt mit der Geheimhaltung des privaten Schlüssels der elektronischen Gesundheitskarte. Deshalb hat man alle notwendigen Maßnahmen angewandt, um den Schutz des privaten Schlüssels des Patienten zu gewährleisten.

...

Komplexer Schlüssel

Der Schlüssel wird so komplex wie möglich gewählt: Seine Länge beträgt im Moment 2.048 Bit.

...

aa) Was wird als Authentifizierung bezeichnet? (2 Punkt)

Prüfung, ob die Person auch die ist, als die sie sich ausgibt

ab) Welche Rolle spielt die PIN bei der Authentifizierung? (4 Punkte)

- Persönliche Identifikationsnummer
- PIN darf nur dem Patienten bekannt sein, da davon ausgegangen wird, dass die Person, die die PIN kennt auch Inhaber der Gesundheitskarte ist

b) Ein Dokument wird mit hybrider Verschlüsselung übertragen. Erläutern Sie stichpunktartig den Ablauf der „hybriden Verschlüsselung". (6 Punkte)

c) Sie sollen die symmetrische Ver- und Entschlüsselung mit einem 8 Bit-Schlüssel unter Verwendung des XOR-Operators demonstrieren. Verwenden Sie hierzu den nachstehend abgebildeten Auszug aus der ASCII-Tabelle.

Korrekturrand

ca) Verschlüsseln Sie in folgender Tabelle den Buchstaben „H". (4 Punkte)

Ausgangsinformation			Schlüssel	Verschlüsselte Informationen		
Zeichen	**ASCII-hex**	**ASCII-bin**	**0000 1010**	**ASCII-bin**	**ASCII-hex**	**Zeichen**
H	48	0100 1000	0000 1010	01000010	42	B

cb) Entschlüsseln Sie in folgender Tabelle den Buchstaben „z". (4 Punkte)

Ausgangsinformation			Schlüssel	Verschlüsselte Informationen		
Zeichen	**ASCII-hex**	**ASCII-bin**	**0000 1010**	**ASCII-bin**	**ASCII-hex**	**Zeichen**
s	73	0111 0011	0000 1010	0111 1001	79	y

ASCII-Tabelle (Auszug)

Zeichen	ASCII-hex		Zeichen	ASCII-hex		Zeichen	ASCII-hex		Zeichen	ASCII-hex
A	41		N	4E		a	61		n	6E
B	42		O	4F		b	62		o	6F
C	43		P	50		c	63		p	70
D	44		Q	51		d	64		q	71
E	45		R	52		e	65		r	72
F	46		S	53		f	66		s	73
G	47		T	54		g	67		t	74
H	48		U	55		h	68		U	75
I	49		V	56		i	69		v	76
J	4A		W	57		j	6A		w	77
K	4B		X	58		k	6B		x	78
L	4C		Y	59		l	6C		y	79
M	4D		Z	5A		m	6D		z	7A