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.

ab) Welche Rolle spielt die PIN bei der Authentifizierung? (4 Punkte - Pasanlide Ideal i Livationsummer - PIN darf ver den Patienten bekannt sehn, die deren ausgebeitend, dass die Person, die die PIN kunst auch himber der Geser alheitskabe ist Dein Dokument wird mit hybrider Verschlüsselung übertragen. Erläutern Sie stichpunktartig den Ablauf der "hybriden Ver-		
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 Verschlüssslungen, 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 des Patienten zu gewährleisten Komplexer Schlüssel des Patienten zu gewährleisten Komplexer Schlüssel des Patienten zu gewährleisten aa) Was wird als Authentifizierung bezeichnet? (2 Punkt Prüffg ob die Person auch die ist aus die sich aus die sich ausgebet Der Schlüssel wird so komplex wie möglich gewählt: Seine Länge beträgt im Moment 2.048 Bit ab) Welche Rolle spielt die PIN bei der Authentifizierung? (4 Punkte Prüffg ob die Person auch die jit aus die sich aus die sich ausgebet Prozentide Idan in Judic der Authentifizierung? Prozentide Idan in Judic der Authentifizierung in Derivertiden Idan in Judic der Authentifizierung in Derivertiden Idan in Judic der Authentifizierung in Derivertiden Idan in D	Die elektronische Gesundheitskarte	
Die Prozessor-Chipkarte hat zwei Haupfunktionen. Erstens fungiert sie als Authentifizierungswerkzeug. Dazu legt jeder Karteninhaber vor Erstverwendung eine persönliche Identifikationsnummer (PIN) nach Wähl 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 verschlüsselungen, die mit der Karte ausgeführt werden, sind vom 1yp hybride Verschlüsselung. Der geheime Schlüssel Der geheime Schlüssel ses eilektronischen Gesundheitskarte. Deshalb hat man alle notwendigen Maßnahmen angewandt, um den Schutz 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 Person of die Person auch de ist odie Se Jah augescht Personida Idan filodorungen Prodorf vor der Patienten der Authentifizierung? (4 Punkte Personida Idan filodorungen PIN darf vor der Patienten Dekant seh bekant seh haber der Geschelbesche ist die PIN bei der Authentifizierung bezeichnet? Bekant seh das der geschlüssel und der "Hohnber der Geschelbesche ist der PIN kunkt auch haber der Geschelbesche ist die PIN bei der Authentifizierung bekant seh haber der Geschelbesche ist die PIN bei der Authentifizierung bei Dokument wird mit hybrider Verschlüsselung übertragen. Erläutern Sie stichpunktartig den Ablauf der "hybriden Ver-	Wie werden Gesundheitsdaten in Zukunft geschützt?	
Einmal verschlüsselt, sind die Daten geschützt, unabhängig davon, wo sie sich gerade befinden. Älle 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 Profig. ob die Person auch de ist als die se sich augescht Ab) Welche Rolle spielt die PIN bei der Authentifizierung? (4 Punkter Posenlide Idan filvahommen PIN darf vor den Patienten PIN darf vor den Patienten PIN darf vor den Patienten Carrendheitslande ist Gesteralheitslande ist Die in Dokument wird mit hybrider Verschlüsselung übertragen. Erläutern Sie stichpunktartig den Ablauf der "hybriden Ver-	Die Prozessor-Chipkarte hat zwei Hauptfunktionen. Erstens fungiert sie als Authentifizierungswerkzeug. Dazu legt jeder Karteninha verwendung eine persönliche Identifikationsnummer (PIN) nach Wahl fest. Die eigene PIN wird in verschlüsselter Form auf der Kar 	te gespeichert.
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 Prüfen ob die Person auch de ist als die se sich augescht ab) Welche Rolle spielt die PIN bei der Authentifizierung? (4 Punkte Prosentide John fill alsonnen ausgebetragen bekant seh, die der Authentifizierung? PIN darf vor dem Patienten bekant seh, die deren ausgebetragen der Authentifizierung? Ein Dokument wird mit hybrider Verschlüsselung übertragen. Erläutern Sie stichpunktartig den Ablauf der "hybriden Ver-	Einmal verschlüsselt, sind die Daten geschützt, unabhängig davon, wo sie sich gerade befinden. Alle Verschlüsslungen, die mit d	
Der Schlüssel wird so komplex wie möglich gewählt: Seine Länge beträgt im Moment 2.048 Bit. aa) Was wird als Authentifizierung bezeichnet? (2 Punkt Prifag, 05 die Person auch die ist als die se sich aug obt ab) Welche Rolle spielt die PIN bei der Authentifizierung? (4 Punkte Prosenliche Identifizierung bekant sch, da ohren ausge PIN darf vor den Patierten bekant sch, da ohren ausge uird, dass die Person die PIN kant auch hinder der Cresendheitsliche ist De bekant sich hinder der Cresendheitsliche ist Cresendheitsliche ist einer Sie stichpunktartig den Ablauf der "hybriden Ver-	Dass die gesundheitsrelevanten Informationen eines Versicherten geheim bleiben, steht und fällt mit der Geheimhaltung des pri Schlüssels der elektronischen Gesundheitskarte. Deshalb hat man alle notwendigen Maßnahmen angewandt, um den Schutz de	
ab) Welche Rolle spielt die PIN bei der Authentifizierung? (4 Punkte - Pasanlide Ideal i Livationsummer - PIN darf ver den Patienten bekannt sehn, die deren ausgebeitend, dass die Person, die die PIN kunst auch himber der Geser alheitskabe ist Dein Dokument wird mit hybrider Verschlüsselung übertragen. Erläutern Sie stichpunktartig den Ablauf der "hybriden Ver-	Der Schlüssel wird so komplex wie möglich gewählt: Seine Länge beträgt im Moment 2.048 Bit.	
ab) Welche Rolle spielt die PIN bei der Authentifizierung? (4 Punkte - Pasanliche Identifikationsmanner - PIN darf nur dem Patienten bekannt sahn, da ohnen ausge wird, dass die Pesan, die die PIN kunnt auch haber der Gesenchheitskate ist Die Dokument wird mit hybrider Verschlüsselung übertragen. Erläutern Sie stichpunktartig den Ablauf der "hybriden Ver-	aa) Was wird als Authentifizierung bezeichnet?	(2 Punkt
- Personlide Identifikationsnummer - PIN darf nur den Patierten bekannt sehn, da ohnen ausge vird, dass die Person, die die PIN kunnt auch hinder der Gescralheitskate ist Die Dokument wird mit hybrider Verschlüsselung übertragen. Erläutern Sie stichpunktartig den Ablauf der "hybriden Ver-		
PIN darf nur den Patierten bekannt sehn, da daven ausser wird, dass de Person, die die PIN kund auch haber der Geseralheitskate ist. Die Dokument wird mit hybrider Verschlüsselung übertragen. Erläutern Sie stichpunktartig den Ablauf der "hybriden Ver-	ab) Welche Rolle spielt die PIN bei der Authentifizierung?	(4 Punkte
Overandheitskate ist Describentskate ist Die Dokument wird mit hybrider Verschlüsselung übertragen. Erläutern Sie stichpunktartig den Ablauf der "hybriden Ver-		
	wird, lass de Person, die die PIN kunt auch hhabe	ossage der
		en Ver- (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.

ca) Verschlüsseln Sie in folgender Tabelle den Buchstaben "H".

(4 Punkte)

Aus	Ausgangsinformation			Verschlüsselte Informationen		
Zeichen	ASCII-hex	ASCII-bin	0000 1010	ASCII-bin	ASCII-hex	Zeichen
Н	48	0100 1000	0000 1010	01000010	42	ß

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	٧

ASCII-Tabelle (Auszug)

Zeichen	ASCII-hex	Zeichen	ASCII-hex	Zeichen	ASCII-hex	Zeichen	ASCII-hex
А	41	N	4E	а	61	n	6E
В	42	0	4F	b	62	0	6F
С	43	Р	50	С	63	р	70
D	44	Q	51	d	64	q	71
Е	45	R	52	е	65	r	72
F	46	S	53	f	66	S	73
G	47	Т	54	g	67	t	74
Н	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	Х	58	k	6B	Х	78
L	4C	Y	59	ı	6C	у	79
М	4D	Z	5A	m	6D	Z	7A