HSR InfSi1 FS14 MobileQuiz

Informationssicherheit 1

Table of Contents

«InfSi1-01-Begriffe-RisikoMgmt»

Question 1: Bei den Information Security Standards der ISO 27000 Serie versteht man unter einer Bedrohung (Threat) ...

Correct Answer	Answer content
◉	Einen möglichen Grund f ür einen ungewollten Vorfall, der das System oder die Organisation schädigen kann
O	Einen Fehler in einem Abwehrdispositiv, der zu einem Schaden führen kann.
O	Verletzlichkeiten (Vulnerabilites) in einem System
O	Den Diebstahl von Informationen

Question 2: Das operative Risikomanagement besteht aus:

Correct Answer	Answer content
◉	Risikoanalyse und Risikobewertung sowie Risikosteuerung und Risikokontrolle
O	Risikoanalyse und Risikobewertung
O	Risikosteuerung und Riskokontrolle

Question 3: Das Ziel der Risikoanalyse ist ...

Correct Answer	Answer content
O	... eine möglichst vollständige Risikobewertung.
◉	... eine möglichst vollständige Risikoidentifikation.
O	... ein möglichst vollständiger Plan um Risiken zu steuern.
O	... ein möglichst vollständiger Überwachungsplan.

Question 4: Der Begriff "Gefährdung" wurde durch folgende Organisation eingef ührt:

Correct Answer	Answer content
O	ISO
◉	BSI
O	OWASP
O	IEEE

Question 5: Die Abk ürzung ISMS steht in diesem Vorlesungsmodul f ür ...

Correct Answer	Answer content
◉	Information Security Management System
O	International Society for Mushroom Science
O	International Security Management Services
O	Indian School of Management & Studies

Question 6: Die Eintrittswahrscheinlichkeit beim Risk Map kann ...

Correct Answer	Answer content
O	... nur qualitativ bewertet werden
O	... nur mathematisch bewertet werden
◉	... mathematisch oder qualitativ bewertet werden
O	... wird gar nicht bewertet

Question 7: In welcher Reihenfolge wird Risikomanagement durchgeführt?

Correct Answer	Answer content
◉	Risiken identifizieren, Risiken bewerten, Risiken steuern, Risiken überwachen
O	Risiken bewerten, Risiken identifizieren, Risiken steuern, Risiken überwachen
O	Risiken überwachen, Risiken identifizieren, Risiken bewerten, Risiken steuern
O	Risiken identifizieren, Risiken bewerten, Risiken überwachen, Risiken steuern

Question 8: Primäre Ziele des Risikomanagements sind Sicherung des künftigen Erfolgs des Unternehmens und die Optimierung der Risikokosten.

Correct Answer	Answer content
◉	Richtig
O	FALSCH

Question 9: Das Schweizer Obligationenrecht verlangt, dass der Anhang zum Geschäftsbericht (bzw. die Jahresrechnung) Angaben über die Durchführung einer Risikobeurteilung enthält.

Correct Answer	Answer content
◉	Richtig
O	FALSCH

Question 10: Viele Kleinunternehmen verzichten auf Risikomanagement (oder führen dieses nur sporadisch durch).

Correct Answer	Answer content
◉	Richtig
O	FALSCH

Question 11: Wann sollte das strategische Risikomanagement durchgeführt werden?

Correct Answer	Answer content
O	Am Ende eines Projektes.
◉	Am Anfang eines Projekts.
O	Nach einem Zwischenfall.

Question 12: Was versteht man unter dem Begriff ein "Risiko vermeiden"?

Correct Answer	Answer content
◉	Risiko vermieden heisst Aktivitäten auf Grund des Risikopotentials einstellen.
O	Risiko vermieden heisst mögliche Schäden auf Grund des Risikopotentials auf andere übertragen.
O	Risiko vermieden heisst mögliche Schäden auf Grund des Risikopotentials durch eine Versicherung abdecken.
O	Risiko vermieden heisst mögliche Schäden auf Grund des Risikopotentials in Kauf nehmen.

Question 13: Was beschreibt gemäss Information Security Standards der ISO 27000 Serie den Begriff Wert (Asset) am besten?

Correct Answer	Answer content
◉	Alles was f ür eine Organisation von Wert ist
O	Confidentiality (Vertraulichkeit)
O	Integrity (Echtheit)
O	Reputation
O	Availability (Verfügbarkeit)

Question 14: Was sind "nicht identifizierte Risiken"?

Correct Answer	Answer content
O	Risiken die vermieden werden.
O	Risiken die bereits gesteuert und überwacht werden.
O	Risiken die nicht eintreten können.
◉	Risiken die bei der Risikoanalyse nicht erkannt wurden.

Question 15: Was versteht man bei ISMS unter "Kontrolle" (Control)?

Correct Answer	Answer content
√	Schutzmassnahme
√	Gegenmassnahme
X	Ueberwachung
X	Check

Question 16: Welche beiden Formulierungen beschreiben den Begriff "Risiko" am besten?

Correct Answer	Answer content
√	Kombination aus der Wahrscheinlichkeit eines Ereignisses (Vorfalls) und dessen Auswirkungen.
X	Gefahr, dass ein negatives Ereignis eintritt.
X	Wahrscheinlichkeit, dass eine Verletzlichkeit ausgenutzt wird.
√	Möglichkeit, dass eine Bedrohung eine Schwachstelle ausnutzen und dadurch der Institution Schaden zuf ügen könnte.
X	Gefahr eines Angriffs.

Question 17: Welcher der beiden Begriffe betrifft eher Situationen, welche effektiv zu einem Schaden f ühren?

Correct Answer	Answer content
◉	Gefährdung
O	Bedrohung

Question 18: Welche Formel passt am besten zur Berechnung des Risiko Erwartungswertes?

Correct Answer	Answer content
O	Erwartungswert = Schadenausmass - Eintrittswahrscheinlichkeit
◉	Erwartungswert = Eintrittswahrscheinlichkeit x Schadenausmass
O	Erwartungswert = Eintrittswahrscheinlichkeit / Schadenausmass
O	Erwartungswert = Eintrittswahrscheinlichkeit + Schadenausmass

Question 19: Bei der Risikomatrix sollen beim Schadensmass ...

Correct Answer	Answer content
X	... möglichst viele Bereiche von Schadenswerten unterschieden werden.
X	... Schadenswerte in Franken angegeben werden.
√	... Schadenswerte in Relation zum Jahresumsatz angegeben werden.

Correct Answer	Answer content
√	... maximal 5 Bereiche mit Schadenswerten unterschieden werden.
√	... Schadenswerte unterschiedlicher Art (z.B. finanzielle Schäden, Image, Recht) berücksichtigt werden.

Question 20: Die Risikobeurteilung im Bereich Informationssicherheit soll ...

Correct Answer	Answer content
O	... die IT-Abteilung selbständig durchführen.
◉	... die IT-Abteilung in Zusammenarbeit mit dem "Business" durchführen.
O	... "Finance und Controlling" durchführen.
O	... die Rechtsabteilung in Zusammenarbeit mit der IT-Abteilung durchführen.

Question 21: Gemäss ISO 27000 Vokabular ist das Ziel der Informationssicherheit ...

Correct Answer	Answer content
√	Die Wahrung von Vertraulichkeit, Echtheit und Verfügbarkeit von Informationen.
X	Die Minimierung von finanziellen Schäden.
X	Die Vermeidung von Reputationsschäden.
√	Die Sicherstellung von Nicht-Abstreitbarkeit.

«InfSi1-02-Standardisierung»

Hilfsmittel zur Verbesserung der Informationssicherheit, Standardisierung, ISO 27000er-Serie, BSI, ITIL, COBIT

Question 1: Beim Berufsverband Institute of Electrical and Electronic Engineers (IEEE) ...

Correct Answer	Answer content
√	kann jeder Mitglied werden
X	können nur zwei Verteter einer Firma Mitglied in einer Arbeitsgruppe sein
√	muss man an einer bestimmten Anzahl Sitzungen teilgenommen haben, um stimmberechtigt zu sein

Question 2: Dinge, welche man unbedingt erf üllen muss, um standardkonform zu sein beschreibt man mit ...

Correct Answer	Answer content
√	must
√	shall
X	should
√	required
X	recommended

Question 3: Dinge, welche man ohne spezielle Begr ündung weglassen kann und trotzdem standardkonform ist, beschreibt man mit ...

Correct Answer	Answer content
X	shall
X	should
√	may
X	recommended
√	optional

Question 4: Dinge, welche man mit guten Grü nden weglassen kann und dabei trotzdem standardkonform ist, beschreibt man mit ...

Correct Answer	Answer content
X	shall
√	should

Correct Answer	Answer content
X	may
√	recommended

Question 5: In Arbeitsgruppen des nationalen Standardisierungsgremiums American National Standards Institution (ANSI) ...

Correct Answer	Answer content
O	kann jeder Mitglied werden
◉	können nur zwei Verteter einer Firma Mitglied sein
O	muss man an einer bestimmten Anzahl Sitzungen teilgenommen haben, um stimmberechtigt zu sein

Question 6: Standardisierungsprozesse laufen in der Regel bei folgendem Gremium am schnellsten ab (Zeit von der Idee bis zum publizierten Standard):

Correct Answer	Answer content
◉	IETF
O	ISO
O	IEEE
O	ANSI

Question 7: Diese Standards sind in der Regel kostenlos erhältlich:

Correct Answer	Answer content
X	ISO Standards
√	RFCs
√	Standards des BSI Deutschland
X	IEEE Standards
X	ANSI Standards

Question 8: RFCs werden durch folgende Organisation veröffentlicht:

Correct Answer	Answer content
◉	IETF
O	IANA
O	ANSI
O	IEEE

Question 9: Ein Vorläufer des ISO 27001-Standards war ...

Correct Answer	Answer content
◉	BS 7799-2
O	BS 7799-1
O	BS ISO/IEC 17799:2000

Question 10: International gü ltige Standards im Bereich Informationssicherheit sind ...

Correct Answer	Answer content
√	ISO 27001
X	BSI Grundschutz-Handbuch
X	BS 7799
√	ISO 27002

Question 11: Bei einer "Sicherheitszertifizierung" wird überprüft, ob der folgende Standard erfüllt ist:

Correct Answer	Answer content
O	ISO 27000 Overview and Vocabulary
◉	ISO 27001 ISMS Requriements
O	ISO 27002 Code of Practice IS Controls
O	ISO 27003 ISMS Implementation Guidence
O	ISO 27006 Certification Body Requriements

Question 12: ITIL konzentriert sich auf ...

Correct Answer	Answer content
◉	IT-Service Managment
O	Information Security Management
O	Business Requirements
O	Evaluation Assurance Levels

Question 13: ISO 27001 konzentriert sich auf ...

Correct Answer	Answer content
X	IT-Service Managment
X	Information Security Management
X	Business Requirements
X	Evaluation Assurance Levels

Question 14: Common Criteria (CC) konzentriert sich auf ...

Correct Answer	Answer content
X	IT-Service Managment
X	Information Security Management
X	Business Requirements
X	Evaluation Assurance Levels

Question 15: COBIT konzentriert sich auf ...

Correct Answer	Answer content
X	IT-Service Managment
X	Information Security Management
X	Business Requirements
X	Evaluation Assurance Levels

Question 16: Zu OWASP passen die folgenden drei Begriffe am besten:

Correct Answer	Answer content
√	Anwendungssicherheit
√	Open Source
X	Security Standardisierung
X	Business Requirements
√	Ausbildung
X	Evaluation Assurance Levels

Question 17: Tiger Teams führen typischerweise nach folgende Aktionen aus:

Correct Answer	Answer content
◉	Black Box Testing
O	White Box Testing
O	Security Reviews
O	Security Audits

«InfSi1-03-Verletzlichkeiten»

Question 1: Der passendste englische Begriff für "Vertraulichkeit der Information" lautet ...

Correct Answer	Answer content
O	Secrecy
O	Privacy
◉	Confidentiality
O	Availability
O	Integrity
O	Authentication

Question 2: Der passendste englische Begriff für "Privatsphärenschutz" lautet ...

Correct Answer	Answer content
O	Secrecy
◉	Privacy
O	Confidentiality
O	Availability
O	Integrity
O	Authentication

Question 3: Der passendste englische Begriff für "Geheimhaltung" lautet ...

Correct Answer	Answer content
◉	Secrecy
O	Privacy
O	Confidentiality
O	Availability
O	Integrity
O	Authentication

Question 4: Welcher Begriff ist keines der in der Vorlesung erklärten "CIA" Sicherheitsziele?

Correct Answer	Answer content
O	Confidentiality
O	Availability

Correct Answer	Answer content
O	Integrity
◉	Authentication

Question 5: Welche der folgenden Aussagen treffen auf den Begriff "Clickjacking" zu?

Correct Answer	Answer content
X	Clickjacking heisst ein spezielles Programm, mit welchem das Einstecken von Steckern in Buchsen Mausklicks auslöst.
√	Mausklicks auf Webseiten werden zum unwissentlichen Starten von Programmen missbraucht.
√	Clickjacking nutzte Schwachstellen von Browsern aus.
X	Beim Clickjacking wird anhand des Clickgeräusches herausgefunden, welche Maushardware im Einsatz ist.

Question 6: Zum Begriff "Drive-by-Download" passen folgende Aussagen:

Correct Answer	Answer content
X	Indem man mit der Maus über bestimmte Elemente einer Webseite fährt, lädt man bösartige Programme auf seinen Rechner.
√	Der blosse Besuch einer Webseite führt zur Installation bösartiger Programme.
X	Drive-by-Download ist eine Technik zum Herunterladen kopiergeschützter Musikstücke.
√	Mittels Drive-by-Download konnten Netzwerk-Accessrouter umprogrammiert werden.

Question 7: Welche der folgenden Aussagen zu Botnets treffen zu?

Correct Answer	Answer content
X	Man weiss sehr gut, wie viele Rechner mit Bots befallen sind.
√	Um ein Botnetz nutzen zu können benötigt man keine besondere technische Kenntnisse.
X	Es ist einfach festzustellen, ob ein Rechner Teil eines Botnets ist.
√	Die Betreiber der Botnets nutzen diese meist nicht selbst für Angriffe, sondern stellen sie Interessierten gegen Bezahlung zu Verfügung.

«InfSi1-04-Massnahmen»

Question 1: Bei welcher Bundesstelle sollen Sicherheitszwischenfälle gemeldet werden?

Correct Answer	Answer content
◉	MELANI
O	KOBIK
O	SWITCH
O	SKP PSC

Question 2: Welche Aussagen treffen auf die National Vulnerability Database (NVD) zu?

Correct Answer	Answer content
√	Hilft zur Vereinheitlichung von verschiedenen, firmenspezifischen Vulnerability Scoring Systemen.
X	Liefert ein direktes Mass zum Business Impact.
√	Erleichtert die Identifikation von identischen Verletzlichkeiten, welche verschiedene Organisationen entdeckt haben.
√	Führt leicht zu falschen Statistiken, wenn man bei der Suche nicht sorfältig arbeitet.
X	Ist ein internationaler Standard zur Vermeidung von Verletzlichkeiten.

Question 3: Welcher Begriff trifft am besten auf die National Vulnerability Database (NVD) zu?

Correct Answer	Answer content
◉	Metadatenbank
O	Internationaler Standard
O	Top10 Verletzlichkeitsliste
O	Meldestelle für Verletzlichkeiten

Question 4: Welche Bundeststelle kümmert sich um die koordinierte Bekämpfung der Internet-Kriminalität?

Correct Answer	Answer content
O	MELANI
◉	KOBIK
O	SWITCH

Correct Answer	Answer content
O	SKP PSC

Question 5: Welche der folgenden Aussagen zu CERT treffen zu?

Correct Answer	Answer content
√	CERT ist die Abkürzung für Computer Emergency Response Team.
√	CERT wurde in den USA gegründet.
X	CERT gibt es nur in den USA.
X	CERT gibt es nur bei staatlichen Stellen.
X	CERT ist die Abkürzung für Coordination of Electronic Risk Technologies.

Question 6: Welche Abkürzung steht für die Datenbank/Beschreibung, mit welcher bei NVD und OSVDB die Identifikation von Verletzlichkeiten sichergestellt wird?

Correct Answer	Answer content
X	CVSS
√	CVE
X	CPE
X	CSRC

Question 7: Welche Abkürzung steht für die Datenbank/Beschreibung, mit welcher bei NVD und OSVDB die Identifikation von Produkten/Geräten/Anwendungen sichergestellt wird?

Correct Answer	Answer content
X	CVSS
X	CVE
√	CPE
X	CSRC

Question 8: Welche Abkürzung steht für die Metric zur Bewertung des Schweregrades von Verletzlichkeiten?

Correct Answer	Answer content
◉	CVSS
O	CVE
O	CPE
O	CSRC

Question 9: Geben Sie an, welche Aussagen zur "Just Culture" as an atmosphere of trust in which people are encouraged (even rewarded) for providing essential

safety-related information, but in which they are also clear about where the line must be drawn between acceptable and unacceptable behavior

Correct Answer	Answer content
X	Förderung der Information über sicherheitsrelevante Zwischenfälle
X	aktive Erkennung und Meldung von Sicherheitszwischenfällen
X	Meldekultur, welche sich bei Piloten etabliert hat.
X	Vermeidung von Fehlern durch eine etablierte Strafkultur

«InfSi1-05-InfoTheorie-KlassVe»

Question 1: Wie viele mögliche Schlüssel gibt es beim Caesar-Code?

Correct Answer	Answer content
◉	26
O	26^2
O	26!

Question 2: Wie viele mögliche Schlüssel gibt es beim Vigenère-Code mit n Zeichen Schlüssellänge?

Correct Answer	Answer content
O	26
O	26*n
O	26!
◉	26^n

Question 3: Bei welchem Verfahren ist die typische Buchstabenhäufigkeit einer Sprache im Chiffrat weniger klar ersichtlich?

Correct Answer	Answer content
O	Caesar
◉	Vigenère

Question 4: Security by Obscurity heisst, ...

Correct Answer	Answer content
◉	dass die Sicherheit des Verfahrens darauf basiert, dass das Verfahren geheim gehalten wird.
O	dass sehr komplexe Verfahren eingesetzt werden sollen.
O	dass möglichst ungewöhnliche Verschlüsselungsverfahren verwendet werden sollen.

Question 5: Bei welchem Verfahren zeigt die Autokorrelation der mit dem Schlüssel "thequickbrown" verschlüsselten Zeichenfolge des Märchentextes "Ali Baba und die 40 Räuber" Periodizitäten?

Correct Answer	Answer content
O	Caesar
◉	Vigenère

Question 6: Welche Werte liefert die Autokorrelation einer sehr langen, zufälligen Zeichenfolge bestehend aus 100 verschiedenen Zeichen bei der Verschiebung um mindestens ein Zeichen?

Correct Answer	Answer content
O	etwa 7% Übereinstimmungen
O	etwa 4% Übereinstimmungen
◉	etwa 1% Übereinstimmungen
O	periodisch kleine und dann wieder grössere Werte

Question 7: Angreifer können das Chiffrat eines deutschen Textes am besten entschlüsseln, wenn ...

Correct Answer	Answer content
◉	der Klartext viel Redundanz enthält.
O	die Entropie des Klartexts 4.7 Bit beträgt.
O	alle Zeichen des Chiffrats gleich häufig auftreten.

Question 8: Beim One-Time-Pad Verschlüsselungsverfahren ...

Correct Answer	Answer content
√	ist der Schlüssel gleich lang wie der Klartext.
X	müssen alle Chiffratzeichen gleich häufig auftreten.
√	darf der Schlüssel nicht mehrfach verwendet werden.
X	wird der Schlüssel in Abhängigkeit von der Zeit gewechselt.

Question 9: Der Informationsgehalt eines (einzelnen) Zeichens ist dann am höchsten, ...

Correct Answer	Answer content
◉	wenn das Zeichen sehr selten vorkommt.
O	wenn das Zeichen gleich häufig vorkommt, wie alle anderen Zeichen.
O	wenn das Zeichen sehr häufig vorkommt.

Question 10: Die Entropie einer Zeichenfolge (bzw. der mittlere Informationsgehalt der Zeichenfolge) ist dann am höchsten, ...

Correct Answer	Answer content
O	wenn einige Zeichen sehr selten vorkommen.
◉	wenn alle Zeichen gleich häufig vorkommen.
O	wenn einige Zeichen sehr häufig vorkommen.

Question 11: Der Informationsgehalt eines Symbols, welches mit der Wahrscheinlichkeit 1/68 vorkommt, beträgt ...

Correct Answer	Answer content
O	5.1 Bit
O	6 Bit
◉	6.09 Bit
O	7.2 Bit
O	8 Bit

Question 12: 16 zufällig gewählte Hex-Zeichen haben einen Informationsgehalt von...

Correct Answer	Answer content
O	4 Bit
O	16 Bit
O	32 Bit
◉	64 Bit
O	128 Bit

Question 13: Das Caesar Verschlüsselungsverfahren ...

Correct Answer	Answer content
X	ist ein Transpositionsverfahren.
√	is ein Substitutionsverfahren.
√	verwendet monoalphabethische Verschlüsselung.
X	verwendet polyalphabethische Verschlüsselung.

Question 14: Das Vigenère Verschlüsselungsverfahren ...

Correct Answer	Answer content
X	ist ein Transpositionsverfahren.
√	is ein Substitutionsverfahren.
X	verwendet monoalphabethische Verschlüsselung.
√	verwendet polyalphabethische Verschlüsselung.

Question 15: Dass die Sicherheit eines Verschlüsselungssystems einzig und allein von der Sicherheit des geheimen Schlüssels abhangen soll, wurde gefordert von ...

Correct Answer	Answer content
◉	Auguste Kerckhoffs
O	Claude Shannon

Correct Answer	Answer content
O	Alain Touring
O	Gilbert Vernam

Question 16: Unter Berücksichtigung des Zusammenhangs aufeinanderfolgender Zeichen beträgt die Entropie englischer Texte etwa ...

Correct Answer	Answer content
O	8 Bit
O	5 Bit
O	3 Bit
◉	1 Bit

Question 17: Dass die statistische Verteilung des Klartextes im Chiffretext nicht mehr ersichtlich sein soll, wurde gefordert von ...

Correct Answer	Answer content
O	Auguste Kerckhoffs
◉	Claude Shannon
O	Alain Touring
O	Gilbert Vernam

Question 18: Welche Aussagen treffen zu "Steganographie" zu?

Correct Answer	Answer content
√	Steganogrphie wird auch mit "Covert Channel" umschrieben.
X	Eine mit Steganographie verarbeitete Nachricht, kann nur bei Kenntnis des richtigen Schlüssels gelesen werden.
√	Bei der Steganographie benötigt man ein Hostfile.
√	Die Methode der Steganographie kommt bei modernen Farb-Laser-Druckern zum Einsatz.

Question 19: Wenn man die Länge eines Schlüssels um ein Bit erhöht ...

Correct Answer	Answer content
√	verdoppelt sich die Scherheit des Systems.
X	verdoppelt sich der Informationsgehalt des Schlüssels.
√	nimmt der Informationsgehalt des Schlüssels um ein Bit zu.
X	wird die Sicherheit des Systems vier mal grösser.

Question 20: Wer gilt als Begründer der Informationstheorie und hat die Einheit zum Informationsgehalt definiert?

Correct Answer	Answer content
O	Auguste Kerckhoffs
◉	Claude Shannon
O	Alain Touring
O	Gilbert Vernam

«InfSi1-06-Verschluesselung»

Question 1: Bei welchen Block Cipher Betriebsmodi wird kein Initialvektor verwendet?

Correct Answer	Answer content
◉	Electronic Codebook Mode (ECM)
O	Cipher Block Chaining (CBC)
O	Cipher Feedback Mode (CFB)
O	Counter Mode (CTR)

Question 2: Bei welchem Block Cipher Betriebsmodus bleiben Periodizitäten im Klartext erhalten?

Correct Answer	Answer content
◉	Electronic Codebook Mode (ECM)
O	Cipher Block Chaining (CBC)
O	Cipher Feedback Mode (CFB)
O	Counter Mode (CTR)

Question 3: Welche der folgenden Begriffe beschreiben AES?

Correct Answer	Answer content
X	Stream Cipher
√	Block Cipher
√	Advanced Encryption Standard
X	American Encryption Standard
√	Symmetric Key
X	public Key

Question 4: Welche der folgenden Verfahren sind Public Key Verfahren?

Correct Answer	Answer content
X	RC4
X	RC5
X	AES
X	DES
√	RSA
√	ECC

Question 5: Welche der folgenden Verfahren sind Symmetric Key Verfahren?

Correct Answer	Answer content
√	RC4
√	RC5
√	AES
√	DES
X	RSA
X	ECC

Question 6: Welche Eigenschaften zeichnen symmetrische Verfahren gegenüber asymmetrischen Verfahren aus?

Correct Answer	Answer content
√	kürzere Schlüssel
√	einfachere Berechnung
X	längere Schlüssel
X	komplexere Berechnung
√	benötigt grössere Anzahl geheimer Schlüssel
X	benötigt kleinere Anzahl geheimer Schlüssel

Question 7: Welche Teile eines Kryptosystems müssen geheim gehalten werden?

Correct Answer	Answer content
O	Verschlüsselungsalgorthmus
O	Entschlüsselungsalgorithmus
O	Ciphertext
◉	Schlüssel

Question 8: Was ergibt die Verknüpfung y = a EXOR b EXOR a ?

Correct Answer	Answer content
O	1
O	a
◉	b
O	0 oder 1 abhängig von a

Question 9: Welche (effektive) Schlüssellänge wird bei "normaler" DES-Verschlüsselung verwendet?

Correct Answer	Answer content
O	40 Bit

Correct Answer	Answer content
◉	56 Bit
O	64 Bit
O	112 Bit
O	128 Bit
O	192 Bit

Question 10: Welche (effektive) Schlüssellänge wird bei Triple-DES-Verschlüsselung verwendet?

Correct Answer	Answer content
O	192 Bit
O	168 Bit
O	128 Bit
◉	112 Bit
O	64 Bit
O	56 Bit

Question 11: Nach wie vielen Bit wiederholt sich die von einem Linear Feedback Shiftregister (LFSR) Generator der Länge k produzierte Schlüsselsequenz spätestens wieder?

Correct Answer	Answer content
O	k!
O	k^2
◉	2^k - 1
O	2^k

Question 12: Welche Aussagen treffen auf "Hybride Verschlüsselungssysteme" zu?

Correct Answer	Answer content
X	sind sicherer als symmetrische Verschlüsselungssysteme
X	Sind sicherer als asymmetrische Verschlüsselsungssysteme
√	werden bei TLS/SSL eingesetzt
√	arbeiten mit Public Key und Symmetric Key Verfahren

Question 13: Welchen Teil des Schlüssels muss der Sender einer Nachricht bei der Verschlüsselung mit einem Public Key Verfahren verwenden?

Correct Answer	Answer content
◉	den public Key des Empfängers

Correct Answer	Answer content
O	den Public Key des Senders
O	den Private Key des Empfängers
O	den Private Key des Senders
O	den Public und den Private Key des Empfängers
O	den Public und den Private Key des Senders

Question 14: Welchen Teil des Schlüssels muss der Empfänger einer Nachricht bei der Entschlüsselung mit einem Public Key Verfahren verwenden?

Correct Answer	Answer content
O	den Public Key des Empfängers
O	den Public Key des Senders
◉	den Private Key des Empfängers
O	den Private Key des Senders
O	den Public und den Private Key des Empfängers
O	den Public und den Private Key des Senders

«InfSi1-07-PublicKey-Hash»

Question 1: Wie viele Primzahlen gibt es?

Correct Answer	Answer content
O	endlich viele
◉	unendlich viele

Question 2: Die heute bekannten Erfinder des ersten Public Key Verschlüsselungsverfahrens heissen?

Correct Answer	Answer content
O	Diffie, Hellman
O	Rivest, Shamir, Adleman
◉	Ellis, Cocks, Williamson

Question 3: Welche Namen stecken hinter dem bekanntesten Public Key Austauschverfahren?

Correct Answer	Answer content
◉	Diffie, Hellman
O	Rivest, Shamir, Adleman
O	Ellis, Cocks, Williamson

Question 4: Um jemandem (einem Empfänger) eine verschlüsselte Meldung schicken zu können, brauche ich (der Sender) ...

Correct Answer	Answer content
◉	den public Key des Empfängers
O	den secret Key des Empfängers
O	den Public Key des Senders
O	den secret Key des Senders

Question 5: 33 mod (7) ist gleich

Correct Answer	Answer content
◉	5
O	2
O	3

Correct Answer	Answer content
O	1

Question 6: 33 mod (13) ist gleich

Correct Answer	Answer content
◉	7
O	6
O	20
O	5

Question 7: Die (multiplikativ) inverse Zahl von 5 mod (7) ist gleich

Correct Answer	Answer content
O	1/7
O	1/5
O	2
◉	3
O	4
O	6

Question 8: Um jemandem (einem Empfänger) eine signierte Meldung schicken zu können, brauche ich (der Sender) ....

Correct Answer	Answer content
O	den Public Key des Empfängers
O	den secret Key des Empfängers
O	den Public Key des Senders
◉	den secret Key des Senders
O	den public und den secret Key des Empfängers
O	den public und den secret Key des Senders

Question 9: Die Signatur einer Person kann der Empfänger einer von dieser Person signierten Meldung überprüfen mit ...

Correct Answer	Answer content
√	dem public Key der signierenden Person
X	dem secret Key der signierenden Person
X	dem public Key des Empfängers
X	dem secret Key des Empfängers
√	dem public Key der Organisation, welche das Zertifikat der signierenden Person ausgestellt

Correct Answer	Answer content
	hat
X	dem secret Key der Organisation, welche das Zertifikat der signierenden Person ausgestellt hat

Question 10: Welche sind Abkürzungen von Hashverfahren?

Correct Answer	Answer content
√	MD5
√	SHA
X	RSA
X	DH
√	RIPEMD
X	RC4

Question 11: Es soll zu einer vorgegebenen Meldung m_i keine andere Meldung m_j mit gleichem Hash-Wert gefunden werden können.

Correct Answer	Answer content
◉	Preimage-Resistenz
O	Kollisionsfreiheit
O	Nicht-Umkehrbarkeit

Question 12: Es darf nicht effizient möglich sein, zwei Meldungen m_x und m_y mit demselben Hash-Wert h=H(m_x)=H(m_y) zu finden.

Correct Answer	Answer content
O	Preimage-Resistenz
◉	Kollisionsfreiheit
O	Nicht-Umkehrbarkeit

Question 13: Welches Hashverfahren sollte gemäss US CERT seit Ende 2008 nicht mehr verwendet werden?

Correct Answer	Answer content
◉	MD5
O	SHA-2
O	MD6
O	SHA-1
O	SHA-3
O	RIPEMD-160

Question 14: Bei welcher Schlüssellänge erzielt RSA eine vergleichbare Sicherheit wie 3DES?

Correct Answer	Answer content
O	112 Bit
O	256 Bit
◉	2048 Bit
O	15360 Bit

Question 15: Bei welcher Schlüssellänge erzielt RSA eine vergleichbare Sicherheit wie AES-256?

Correct Answer	Answer content
O	256 Bit
O	2048 Bit
O	3072 Bit
◉	15360 Bit

«Zwischentest-InfSi01»

Question 1: Ein "Zertifikat" enthält ...

Correct Answer	Answer content
√	Public Key und die Unterschrift einer Zertifizierungsstelle
X	Angaben zum Symmetric Key Algorithmus, der verwendet werden soll
X	Public Key und Private Key
√	Angaben zum eingesetzten Public Key Algorithmus

Question 2: Ein Freund hat Ihnen per eMail sein Zertifikat zugeschickt. Welche der folgenden Aussagen trifft zu?

Correct Answer	Answer content
X	Mit diesem Zertifikat kann ich Mails an diesen Freund verschlüsseln.
X	Mit diesem Zertifikat kann ich Mails signieren.
√	Mein Browser bzw. mein eMail-Programm kann überprüfen, ob das Zertifikat gültig ist.
√	Im Zertifikat ist angegeben, welcher Public Key Algorithmus zu verwenden ist.

Question 3: Ein Root-Zertifikat muss folgende Eigenschaft(en) haben:

Correct Answer	Answer content
√	Self-signed
X	Grosse Schlüssellänge
X	Signiert von Verisign
√	Herausgeber und Antragsteller sind identisch

Question 4: Welche Aussagen treffen auf Hybride Verschlüsselungssysteme zu?

Correct Answer	Answer content
X	sind sicherer als symmetrische Verschlüsselulngssysteme
√	werden bei TLS/SSL eingesetzt
√	arbeiten mit Public Key und Symmetric Key Verfahren
√	werden beim Mail-Verschlüsselung eingesetzt

Question 5: Welche Schlüssellänge gilt 2013 gemäss NIST für symmetrische Verschlüsselung am ehesten als minimal erforderliche Schlüssellänge für ausreichende Sicherheit?

Correct Answer	Answer content
O	40 Bit
O	80 bit
◉	128 bit
O	1024 bit

Question 6: Welche Teile eines Kryptosystems müssen geheim gehalten werden?

Correct Answer	Answer content
O	Verschlüsselungsalgorthmus
O	Entschlüsselungsalgorithmus
O	Ciphertext
◉	Schlüssel

Question 7: Welchen Teil des Schlüssels muss der Empfänger einer Nachricht bei der Verschlüsselung mit einem Public Key Verfahren verwenden?

Correct Answer	Answer content
O	den Public Key des Empfängers
◉	den Private Key des Empfängers
O	den Public und den Private Key des Empfängers
O	den Public Key des Senders
O	den Private Key des Senders
O	den Public und den Private Key des Senders

Question 8: Welchen Teil des Schlüssels muss der Sender einer Nachricht bei der Verschlüsselung mit einem Public Key Verfahren verwenden?

Correct Answer	Answer content
◉	den public Key des Empfängers
O	den Private Key des Empfängers
O	den Public und den Private Key des Empfängers
O	den Public Key des Senders
O	den Private Key des Senders
O	den Public und den Private Key des Senders

Question 9: Welcher dieser Algorithmen bildet die Grundlage zu Public Key Verfahren?

Correct Answer	Answer content
◉	Rivest Shamir Adleman (RSA)
O	Advanced Encryption Standards (AES)
O	Data Encryption Standard (DES)

Question 10: Das Bundesamt fü r Sicherheit in der Informationstechnik (BSI) ...

Correct Answer	Answer content
√	ist eine deutsche Bundesstelle
√	fördert angemessenen IT-Grundschutz
X	erstellt Vorgaben, welche von allen deutschen Firmen beachtet werden m üssen.

Question 11: Ein Informationssicherheitsmanagementsystem (ISMS) ...

Correct Answer	Answer content
X	bezieht sich vorwiegend auf die Informationstechnik (IT)
√	wird zum Beispiel durch die Anforderungen in ISO 27001 beschrieben
√	wird in den Vorschriften des EDOEB zur Zertifizierung eines DSMS über den Bezug zu ISO 27001 referenziert

Question 12: Risiken werden beschrieben durch ...

Correct Answer	Answer content
√	Schutzziele (Werte/Assets), Verwundbarkeiten/Schwachstellen, Ereignisse, Schadenausmass, Ablauf/Szenario
√	Eintretenswahrscheinlichkeit und Schadenausmass von Ereignissen
X	Schutzziele (Werte/Assets), Schadenausmass, Verfahren fürs Krisenmanagement

Question 13: Welche beiden Formulierungen beschreiben den Begriff "Risiko" am besten?

Correct Answer	Answer content
√	Kombination aus der Wahrscheinlichkeit eines Ereignisses (Vorfalls) und dessen Auswirkungen.
X	Gefahr, dass ein negatives Ereignis eintritt.
X	Wahrscheinlichkeit, dass eine Verletzlichkeit ausgenutzt wird.
√	Möglichkeit, dass eine Bedrohung eine Schwachstelle ausnutzen und dadurch der Institution Schaden zuf ügen könnte.
X	Gefahr eines Cyber-Angriffs

Question 14: Bei welchem Block Cipher Betriebsmodus bleiben Periodizitäten im Klartext erhalten?

Correct Answer	Answer content
◉	Electronic Codebook Mode (ECM)
O	Cipher Block Chaining (CBC)
O	Cipher Feedback Mode (CFB)
O	Counter Mode (CTR)

Question 15: Welche der folgenden Begriffe beschreiben AES?

Correct Answer	Answer content
X	Stream Cipher
√	Block Cipher
√	Advanced Encryption Standard
X	American Encryption Standard
√	Symmetric Key
X	public Key

Question 16: Welche der folgenden Verfahren sind Public Key Verfahren?

Correct Answer	Answer content
X	RC4
X	RC5
X	AES
X	DES
√	RSA
√	ECC

Question 17: Welche der folgenden Verfahren sind Symmetric Key Verfahren?

Correct Answer	Answer content
√	RC4
√	RC5
√	AES
√	DES
X	RSA
X	ECC

Question 18: Welche Eigenschaften zeichnen symmetrische Verfahren gegenüber asymmetrischen Verfahren aus?

Correct Answer	Answer content
√	kürzere Schlüssel
√	einfachere Berechnung
X	längere Schlüssel
X	komplexere Berechnung
√	benötigt grössere Anzahl geheimer Schlüssel
X	benötigt kleinere Anzahl geheimer Schlüssel

Question 19: Welche Teile eines Kryptosystems müssen geheim gehalten werden?

Correct Answer	Answer content
O	Verschlüsselungsalgorthmus
O	Entschlüsselungsalgorithmus
O	Ciphertext
◉	Schlüssel

Question 20: Was ergibt die Verknüpfung y = a EXOR b EXOR a ?

Correct Answer	Answer content
O	1
O	a
◉	b
O	0 oder 1 abhängig von a

Question 21: Welche (effektive) Schlüssellänge wird bei "normaler" DES-Verschlüsselung verwendet?

Correct Answer	Answer content
O	40 Bit
◉	56 Bit
O	64 Bit
O	112 Bit
O	128 Bit
O	192 Bit

Question 22: Welche (effektive) Schlüssellänge wird bei Triple-DES-Verschlüsselung verwendet?

Correct Answer	Answer content
O	192 Bit
O	168 Bit
O	128 Bit
◉	112 Bit
O	64 Bit
O	56 Bit

Question 23: Welche Aussagen treffen auf "Hybride Verschlüsselungssysteme" zu?

Correct Answer	Answer content
X	sind sicherer als symmetrische Verschlüsselungssysteme
X	Sind sicherer als asymmetrische Verschlüsselsungssysteme
√	werden bei TLS/SSL eingesetzt
√	arbeiten mit Public Key und Symmetric Key Verfahren

Question 24: Welchen Teil des Schlüssels muss der Sender einer Nachricht bei der Verschlüsselung mit einem Public Key Verfahren verwenden?

Correct Answer	Answer content
◉	den public Key des Empfängers
O	den Public Key des Senders
O	den Private Key des Empfängers
O	den Private Key des Senders
O	den Public und den Private Key des Empfängers
O	den Public und den Private Key des Senders

Question 25: Welchen Teil des Schlüssels muss der Empfänger einer Nachricht bei der Entschlüsselung mit einem Public Key Verfahren verwenden?

Correct Answer	Answer content
O	den Public Key des Empfängers
O	den Public Key des Senders
◉	den Private Key des Empfängers
O	den Private Key des Senders
O	den Public und den Private Key des Empfängers
O	den Public und den Private Key des Senders

«InfSi1-08-Zertifikate»

Question 1: Welche Elemente sind in einem Zertifikat enthalten?

Correct Answer	Answer content
√	Identifikation des Besitzers
√	Identifikation des Herausgebers
X	secret Key des Besitzers des Zertifikats
X	public Key des Besitzers des Zertifikats
√	Gültigkeitsdatum
√	Fingerprint

Question 2: Was ist die Hauptaufgabe einer Registrationsstelle?

Correct Answer	Answer content
◉	Überprüfung der Echtheit des Besitzers eines Public Keys
O	Signierung und Aushändigung des Zertifikats
O	Registrierung des Herausgebers des Zertifikats
O	Überprüfung der Echtheit des Herausgebers eines Zertifikats
O	Erstellung des Zertifikats

Question 3: In welchem der folgenden Zertifikatfiles dürfte auch der private Key enthalten sein?

Correct Answer	Answer content
O	cert.pem
◉	cert.p12
O	cert.der
O	cert.cer

Question 4: Ein Root-Zertifikat hat folgende Eigenschaft(en)

Correct Answer	Answer content
√	Ist Self-signed
X	Hat eine Schlüssellänge von 256 Bit
X	Muss von Verisign signiert worden sein.
√	Herausgeber und Antragsteller sind identisch
X	Muss einen Diffie-Helman Public Key enthalten

Correct Answer	Answer content
X	Muss einen AES-Key enthalten

Question 5: Welches der folgenden Zertifikatfiles ist eine Folge von ASCII-Zeichen?

Correct Answer	Answer content
◉	cert.pem
O	cert.p12
O	cert.der

Question 6: Was ist die Hauptaufgabe einer Certificate Authority?

Correct Answer	Answer content
O	Überprüfung der Echtheit des Besitzers eines Public Keys
◉	Signierung und Aushändigung des Zertifikats
O	Registrierung des Herausgebers des Zertifikats

Question 7: Welcher Begriff hat keine rechtliche Bedeutung (im Rahmen des Schweizer Signaturgesetztes)?

Correct Answer	Answer content
◉	digitale Signatur
O	elektronische Signatur
O	fortgeschrittene elektronische Signatur
O	qualifizierte elektronische Signatur

Question 8: Welche Organisation wurde in der Schweiz dafür akkreditiert, Zertifikate Diensteanbieter anzuerkennen?

Correct Answer	Answer content
O	Verisign
◉	KPMG
O	SwissSign
O	Swisscom

Question 9: Welche Signatur ist der handschriftlichen Signatur rechtlich gleichgestellt?

Correct Answer	Answer content
O	digitale Signatur
O	elektronische Signatur

Correct Answer	Answer content
O	fortgeschrittene elektronische Signatur
◉	qualifizierte elektronische Signatur

Question 10: Welche Aussagen treffen für die Signatur mit dem Gratiszertifikat von StartSSL oder Comodo zu?

Correct Answer	Answer content
X	Damit kann man die Person identifizieren, welche die Unterschrift geleistet hat.
√	Damit kann man den Inhaber der E-Mail-Adresse identifizieren, welche mit dieser Signatur verknüpft ist.
X	Damit kann man eine "qualifizierte elektronische Signatur" im juristischen Sinne erstellen.
√	Damit kann man überprüfen, ob der Inhalt einer Mail auf dem Übertragungsweg verändert worden ist.
√	Damit kann man Meldungen verschlüsseln, so dass diese nur vom Inhaber des Zertifikats wieder entschlüsselt werden können.

Question 11: Welche Aussagen treffen für einen PKCS#12 "Transport Container" zu?

Correct Answer	Answer content
√	Enthält alle Zertifikate der Certificate Chain
√	Enthält den Private Key

«InfSi1-09-TLS-SSL-Grundlagen»

Question 1: Welche Seite entscheidet bei Transport Layer Security Verbindungen, mit welchem Verschlüsselungsverfahren gearbeitet werden soll?

Correct Answer	Answer content
O	Client
◉	Server

Question 2: Auf dem Network Layer des ISO-OSI Modells arbeitet folgendes Verschlüsselungsverfahren:

Correct Answer	Answer content
◉	IPsec
O	SSH
O	TLS
O	S/MIME
O	PGP
O	WPA2

Question 3: Auf dem Datalink Layer des ISO-OSI Modells arbeitet folgendes Verschlüsselungsverfahren:

Correct Answer	Answer content
O	IPsec
O	SSH
O	TLS
O	S/MIME
O	PGP
◉	WPA2

Question 4: Auf dem Transport Layer des ISO-OSI Modells arbeitet folgendes Verschlüsselungsverfahren:

Correct Answer	Answer content
O	IPsec
O	SSH
◉	TLS
O	S/MIME

Correct Answer	Answer content
O	PGP
O	WPA2

Question 5: Auf dem Application Layer des ISO-OSI Modells arbeiten folgende Verschlüsselungsverfahren:

Correct Answer	Answer content
X	IPsec
√	SSH
X	TLS
√	S/MIME
√	PGP
X	WPA2

Question 6: Von welcher Organisation waren 2013 am meisten SSL/TLS-Server-Zertifikate im Einsatz?

Correct Answer	Answer content
◉	Symantec
O	Comodo
O	StartSSL
O	Go Daddy
O	Thawte

Question 7: Welche Information wird beim TLS Session Resume nicht übertragen?

Correct Answer	Answer content
O	SessionID
O	ClientHello.random (Challenge)
O	CipherListOffer
◉	Server Certificate

Question 8: Welche Aussagen treffen für das Online Certificate Status Protocol (OCSP) zu?

Correct Answer	Answer content
√	Mit OCSP werden Anfragen zum Herausgeber von Zertifikaten geschickt.
X	Falls OCSP keine Antwort liefert, wird das Zertifikat immer als ungültig erklärt.
X	Beim OCSP erhält man nur signierte Antworten.
√	OCSP ist optional, d.h. muss nicht unbedingt immer genutzt werden.

Question 9: Welche Aussagen zu TLS treffen zu?

Correct Answer	Answer content
O	TLS verwendet meistens auch Datenkompression.
◉	Gegenwärtig (2013) ist TLS1.2 die höchste von Browsern unterstützte TLS-Version.
O	TLS wurde von der ISO standardisiert.
O	TLS 1.0 ist kompatibel mit SSL3.0.

Question 10: Welches Verfahren stellt bei der TLS Cipher Suite TLS_DHE_DSS_WITH_DES_CBC_SHA die Echtheit des Servers sicher?

Correct Answer	Answer content
◉	DSS
O	DHE
O	DES
O	CBC
O	SHE

Question 11: Welche Aussagen treffen auf das Padding beim TLS Record Body zu?

Correct Answer	Answer content
√	Padding ist nötig, wenn Block Ciphers verwendet werden.
X	Padding ist nötig, um die Anpassung an den RSA-Modulus sicherzustellen.
√	Padding kann gemüss Standard maximal 255 Bytes lang sein.
X	Padding wird unverschlüsselt übertragen.

Question 12: Wie viele Cipher Suites bietet ein Browser im TLS Client Hello so typisch an?

Correct Answer	Answer content
O	1
O	5
◉	20
O	50
O	100

Question 13: Wie viele Cipher Suites bietet ein Server im TLS Server Hello so typisch an?

Correct Answer	Answer content
◉	1

Correct Answer	Answer content
O	5
O	20
O	50
O	100

Question 14: Welche Aussagen treffen zu, wenn TLS Session Resume verwendet wurde?

Correct Answer	Answer content
√	Im Client Hello ist eine Session ID enthalten.
X	Im Server Hello muss das Server Zertifikat gesendet werden.
√	Der Client hatte schon früher einmal eine TLS-Verbindung zum Server eröffnet.
X	Vor der Verschlüsselung müssen die Daten komprimiert werden.

Question 15: Welche Stelle kann entscheiden, ob ein Session Resume gemacht werden soll?

Correct Answer	Answer content
O	Nur der Client
O	Nur der Server
◉	Client und Server

Question 16: Bei TLS/SSL verwendete Server Zertifikate sollten ...

Correct Answer	Answer content
O	einen MD5-Hash enthalten.
◉	Von einer Trusted Certificate Authority ausgegeben sein
O	Self-signed sein
O	Neben dem Servernamen auch die IP-Adresse des Servers enthalten.

«InfSi1-11-Authentication»

Question 1: Authentisierung auf Basis "What you know" ist in folgenden Verfahren enthalten:

Correct Answer	Answer content
√	Computer Logon mit Passwort
√	Authentisierung am Bankomat
X	Fingerprint Reader
X	One-Time-Password Token
X	Mobile TAN
X	Streichlisten Codes

Question 2: Bei welchen Systemen kommt die Password-Based Key Derivation Function (PBKDF) zum Einsatz:

Correct Answer	Answer content
√	WPA/WPA2
X	Windows 7
√	WinZip
√	MAC OS X

Question 3: Bei welchen Systemen kommt 2-Factor Authentication zum Einsatz:

Correct Answer	Answer content
√	Bankomat
X	HSR Login
X	Windows Login
√	Kreditkartenzahlung im Hotel (Card Present Zahlung)

Question 4: Authentisierung auf Basis "What you have" ist in folgenden Verfahren enthalten:

Correct Answer	Answer content
X	Computer Logon mit Passwort
√	Authentisierung am Bankomat
X	Fingerprint Reader
√	One-Time-Password Token
√	Mobile TAN

Question 5: Welche Aussagen treffen für den Einsatz einer "Salt" zu?

Correct Answer	Answer content
◉	Die Erstellung von Rainbow-Tables wird aufwändiger
O	Die Erstellung von Rainbox-Tables ist nicht mehr möglich
O	Brute Force Attacken werden aufwändiger
O	Brute Force Attacken sind nicht mehr möglich

Question 6: Welche Aussagen treffen auf Password-Hashing Verfahren zu?

Correct Answer	Answer content
O	Das Hashing Verfahren soll möglichst schnell sein.
◉	Das Hashing Verfahren soll möglichst langsam sein.
O	Das Hashing Verfahren soll nicht bekannt sein.

Question 7: Bei einem System ist die Geheimzahl aus einer völlig zufällig gewählten Kombination mit vier Zeichen aus dem Zeichensatz 0, ..., 9 erstellt, d.h. es sind Geheimcodes zwischen "0000" und "9999" möglich. Welche Entropieangabe liegt am nächsten bei der Entropie des daraus abgeleiteten Schlüssels?

Correct Answer	Answer content
O	4 Bit
O	10 Bit
◉	13 Bit
O	20 Bit
O	40 Bit

Question 8: Welche Aussagen treffen für die Authentisierung mittels Fingerprint zu?

Correct Answer	Answer content
√	Fingerprint gelten als unsicher, weil sie einfach gefälscht werden können.
X	Die False Acceptance Rate (FAR) ist immer grösser als die False Rejection Rate (FRR).
X	Eineiige Zwillinge haben den gleichen Fingerabdruck.
√	Fingerprint sind "nicht besonders geheim", weil man an sehr vielen Stellen Fingerabdrücke hinterlässt.

Question 9: Welches der folgenden Verfahren eignet sich insgesamt am besten für die biometrische Authentisierung? (Ist in Bezug auf Einsetzbarkeit, Genauigkeit, Fälschungssicherheit und Kosten am besten geeignet für die Authentisierung?)

Correct Answer	Answer content
O	Fingerprint
O	Iris Scan
◉	Hand Venen Scan
O	Spracherkennung

Question 10: Welche Aussagen treffen für die Basic Authentication zu (ohne Spezialmassnahmen und TLS)?

Correct Answer	Answer content
O	Passworte werden verschlüsselt übertragen.
O	Passworte werden beim Server verschlüsselt abgespeichert.
◉	Passworte müssen mit jedem HTTP-Request wieder neu übertragen werden.

Question 11: Welche Aussagen treffen betreffend Password Recovery zu, wenn mit einem Salt gearbeitet wird?

Correct Answer	Answer content
O	Der Systemadministrator kann mir mein Passwort wiederherstellen, wenn ich es vergessen habe.
◉	Bei einem Passwortwechsel kann nicht überprüft werden, ob sich das neue Passwort mehr als ein Zeichen vom alten unterscheidet.
O	Das Passwort könnte einfach angegeben werden, wenn es kein Salt gäbe.

Question 12: Authentication gehört unter den folgenden CIA-Begriff.

Correct Answer	Answer content
O	C
◉	I
O	a

Question 13: Bei welcher Zuordnung von Identifier zu Subjekt können nur ausgewählte Kreise aus der ID auf das Subjekt zurückschliessen?

Correct Answer	Answer content
O	Identity
◉	Pseudonymity
O	Anonymity

Question 14: Wann spricht man von "Strong Authentication"?

Correct Answer	Answer content
◉	Wenn für die Authentifizierung zwei verschiedene Faktoren angegebenwerden müssen.
O	Wenn für die Authentifizierung Schlüssellängen von mehr als 40Bit verwendet werden.
O	Wenn man für die Authentifizierung einen Hardware Token vorweisen muss.

Question 15: In welcher Zeit konnte 2012 ein Standard Windows Passwort, zu welchem der Hash bekannt ist, geknackt werden?

Correct Answer	Answer content
X	in wenigen Minuten
X	innert Stunden
X	innert Tagen
X	innert Wochen
X	innert Jahren