DLMCSEAITSC02\_Unit01\_Question01

Wie viele Schlüssel hat die Cäsar-Chiffre (mit Ausnahme des trivialen Schlüssels)?

* 25 (1 P.)
* 12 (0 P.)
* 13 (0 P.)
* 26 (0 P.)

DLMCSEAITSC02\_Unit01\_Question02

Für welchen nicht-trivialen Schlüssel ist die Cäsar-Chiffre idempotent, d. h. eine erneute Verschlüsselung des Geheimtextes ergibt den Klartext?

* 13 (1 P.)
* 1 (0 P.)
* 2 (0 P.)
* 26 (0 P.)

DLMCSEAITSC02\_Unit01\_Question03

Welcher kryptografische Algorithmus kommt dem Kerckhoffs‘schen Prinzip am nächsten?

* One-Time-Pad (1 P.)
* Enigma (0 P.)
* ADFGVX (0 P.)
* Skytale (0 P.)

DLMCSEAITSC02\_Unit01\_Question04

Welcher der folgenden ist ein Verschlüsselungsalgorithmus?

* AES (1 P.)
* MD5 (0 P.)
* SHA-1 (0 P.)
* CRC (0 P.)

DLMCSEAITSC02\_Unit01\_Question05

Welcher der folgenden ist eine nicht kryptografische Hashfunktion?

* CRC (1 P.)
* MD5 (0 P.)
* SHA-1 (0 P.)
* AES (0 P.)

DLMCSEAITSC02\_Unit02\_Question01

Welche Chiffre ist eine Substitutions-Chiffre?

* Enigma (1 P.)
* Skytale (0 P.)
* AES (0 P.)
* DES (0 P.)

DLMCSEAITSC02\_Unit02\_Question02

Welche Chiffre ist absolut sicher?

* One-Time-Pad (1 P.)
* RSA (0 P.)
* AES (0 P.)
* DES (0 P.)

DLMCSEAITSC02\_Unit02\_Question03

Welche ist die kleinste von AES verwendete Schlüsselgröße?

* 128 (1 P.)
* 56 (0 P.)
* 512 (0 P.)
* 2048 (0 P.)

DLMCSEAITSC02\_Unit02\_Question04

Welche Hashfunktion ist nicht kryptografisch?

* CRC (1 P.)
* SHA-1 (0 P.)
* MD4 (0 P.)
* WHIRLPOOL (0 P.)

DLMCSEAITSC02\_Unit02\_Question05

Welche Chiffre ist eine Stromchiffre?

* Enigma (1 P.)
* RSA (0 P.)
* AES (0 P.)
* DES (0 P.)

DLMCSEAITSC02\_Unit03\_Question01

Was ist die Umkehrung der Falltürfunktion, die im RSA-Algorithmus verwendet wird?

* x↦x1/e (1 P.)
* log (0 P.)
* esp (0 P.)
* x↦x2 (0 P.)

DLMCSEAITSC02\_Unit03\_Question02

Was ist der schnellste bekannte Algorithmus zum Angriff auf RSA?

* Allgemeines Zahlkörpersieb(1 P.)
* Pollard-Rho-Methode (0 P.)
* Smart Attack (0 P.)
* Babystep-Giantstep-Algorithmus (0 P.)

DLMCSEAITSC02\_Unit03\_Question03

Wie groß muss der RSA-Schlüssel mindestens sein, damit er z. B. vom NIST als sicher angesehen wird?

* 3072 (1 P.)
* 1024 (0 P.)
* 2048 (0 P.)
* 4096 (0 P.)

DLMCSEAITSC02\_Unit03\_Question04

Welche Schlüsselgröße bei ECC ist genauso sicher wie ein 256-Bit-Schlüssel bei AES?

* 512 (1 P.)
* 256 (0 P.)
* 1024 (0 P.)
* 2048 (0 P.)

DLMCSEAITSC02\_Unit03\_Question05

Zu was ist *88* kongruent modulo 7?

* 11 (1 P.)
* 1 (0 P.)
* 16 (0 P.)
* 24 (0 P.)

DLMCSEAITSC02\_Unit04\_Question01

Welches Protokoll ist kein Challenge-Response-Authentifizierungsprotokoll?

* TAN (1 P.)
* Digest-MD5 (0 P.)
* CRAM (0 P.)
* SCRAM (0 P.)

DLMCSEAITSC02\_Unit04\_Question02

Auf welche rechnerisch schwierige, diskrete mathematische Funktion stützt sich das Schnorr-Protokoll?

* Logarithmus (1 P.)
* Quadratwurzel (0 P.)
* Exponentialfunktion (0 P.)
* Quadrat (0 P.)

DLMCSEAITSC02\_Unit04\_Question03

Welche Daten fließen nicht in die Berechnung des mit einem Salt versehenen Passworts in SCRAM ein?

* Aktuelle Uhrzeit (1 P.)
* Passwort (0 P.)
* Salt (0 P.)
* IterationCount (0 P.)

DLMCSEAITSC02\_Unit04\_Question04

Wie viele Minuten Zeitdifferenz lässt Kerberos zwischen den verschiedenen authentifizierenden Parteien zu?

* 5 (1 P.)
* 1 (0 P.)
* 2 (0 P.)
* 10 (0 P.)

DLMCSEAITSC02\_Unit04\_Question05

Wie oft verschlüsselt ein Client ein TCP-Paket, bevor er es im Tor-Netzwerk an den Server sendet?

* so oft wie es Knotenpunkte gibt (1 P.)
* doppelt so häufig (0 P.)
* einmal (0 P.)
* zweimal (0 P.)

DLMCSEAITSC02\_Unit05\_Question01

Welche minimale Schlüsselgröße wird derzeit als sicher für RSA und Diffie-Hellman empfohlen?

* 2048 Bit (1 P.)
* 512 Bit (0 P.)
* 1024 Bit (0 P.)
* 4096 Bit (0 P.)

DLMCSEAITSC02\_Unit05\_Question02

Welche minimale Schlüsselgröße wird derzeit für die Elliptic Curve Cryptography als sicher empfohlen?

* 256 Bit (1 P.)
* 128 Bit (0 P.)
* 160 Bit (0 P.)
* 512 Bit (0 P.)

DLMCSEAITSC02\_Unit05\_Question03

Welche minimale Schlüsselgröße wird derzeit für AES als sicher empfohlen?

* 112 Bit (1 P.)
* 80 Bit (0 P.)
* 128 Bit (0 P.)
* 256 Bit (0 P.)

DLMCSEAITSC02\_Unit05\_Question04

Auf welchem rechnerisch schwierigen Problem basiert die Sicherheit von RSA?

* Primzahlzerlegung (1 P.)
* Diskreter Logarithmus (0 P.)
* Punktzählung (0 P.)
* Quadratischer Rest (0 P.)

DLMCSEAITSC02\_Unit05\_Question05

Auf welchem rechnerisch schwierigen Problem basiert die Sicherheit des Diffie-Hellman-Schlüsselaustauschs?

* Diskreter Logarithmus (1 P.)
* Primzahlzerlegung (0 P.)
* Punktzählung (0 P.)
* Quadratischer Rest (0 P.)

DLMCSEAITSC02\_Unit06\_Question01

Wie viele Schichten hat das OSI-Modell?

* 7 (1 P.)
* 4 (0 P.)
* 5 (0 P.)
* 10 (0 P.)

DLMCSEAITSC02\_Unit06\_Question02

Wie viele Schichten hat das TCP/IP-Referenzmodell?

* 4 (1 P.)
* 3 (0 P.)
* 5 (0 P.)
* 7 (0 P.)

DLMCSEAITSC02\_Unit06\_Question03

Welches Protokoll ist nicht Teil der IPsec-Protokollfamilie?

* Session Traversal Utilities for NAT (STUN) (1 P.)
* Internet Key Exchange (IKE) (0 P.)
* Authentication Header (AH) (0 P.)
* Encapsulated Security Payload (ESP) (0 P.)

DLMCSEAITSC02\_Unit06\_Question04

Welche Art von (kryptografischem) Algorithmus wird beim TLS-Handshake „nicht“ vereinbart?

* eine Fehlerkorrekturprüfsumme wie z. B. CBC (1 P.)
* ein asymmetrischer Algorithmus wie RSA (0 P.)
* ein symmetrischer Algorithmus wie AES (0 P.)
* ein kryptografischer Hash-Algorithmus wie SHA256 (0 P.)

DLMCSEAITSC02\_Unit06\_Question05

Welche Sicherheitsfunktion ist weder Teil des S/MIME- noch des OpenPGP-Protokolls?

* Perfect Forward Secrecy (1 P.)
* asymmetrische Verschlüsselung und Entschlüsselung (0 P.)
* digitale Signatur (0 P.)
* Integritätsnachweis (0 P.)

DLMCSEAITSC02\_Unit07\_Question01

Welcher Teil einer Chiffre ist in der Praxis am anfälligsten für Angriffe?

* der Pseudo-Zufallszahlengenerator (1 P.)
* der Entschlüsselungsalgorithmus (0 P.)
* der Verschlüsselungsalgorithmus (0 P.)
* der private Schlüssel (0 P.)

DLMCSEAITSC02\_Unit07\_Question02

Welcher Algorithmus ist sicher vor einem Quantencomputer?

* AES (1 P.)
* RSA (0 P.)
* ECC (0 P.)
* Diffie-Hellman (0 P.)

DLMCSEAITSC02\_Unit07\_Question03

Wie viele Jahre lang wird ein 128-Bit-AES-Schlüssel voraussichtlich sicher bleiben?

* 20 (1 P.)
* 10 (0 P.)
* 40 (0 P.)
* 60 (0 P.)

DLMCSEAITSC02\_Unit07\_Question04

Mit welcher AES-Schlüsselgröße ist ein RSA-Schlüssel von 2048 Bit vergleichbar?

* 192 (1 P.)
* 80 (0 P.)
* 112 (0 P.)
* 128 (0 P.)

DLMCSEAITSC02\_Unit07\_Question05

Mit welcher AES-Schlüsselgröße ist ein ECC-Schlüssel von 256 Bit vergleichbar?

* 128 (1 P.)
* 80 (0 P.)
* 112 (0 P.)
* 192 (0 P.)

DLMCSEAITSC02\_Unit08\_Question01

Welcher Homebanking-Protokollstandard geht FinTS voraus?

* HBCI (1 P.)
* IFX (0 P.)
* OFX (0 P.)
* SET (0 P.)

DLMCSEAITSC02\_Unit08\_Question02

Welches TAN-Verfahren ist resistent gegen Phishing- aber nicht gegen Man-in-the-Middle-Angriffe?

* indizierte TAN (iTAN) (1 P.)
* mobile TAN (mTAN) (0 P.)
* einfache TAN (0 P.)
* CRAM (0 P.)

DLMCSEAITSC02\_Unit08\_Question03

Wie lange dauert es im Durchschnitt, einen neuen Block in das Bitcoin-Blockchain-Netzwerk einzufügen?

* zehn Minuten (1 P.)
* eine Sekunde (0 P.)
* eine Minute (0 P.)
* eine Stunde (0 P.)

DLMCSEAITSC02\_Unit08\_Question04

Was bedeutet das griechische Wort steganos?

* verdeckt (1 P.)
* verstecken (0 P.)
* verschleiern (0 P.)
* einbetten (0 P.)

DLMCSEAITSC02\_Unit08\_Question05

Auf welcher Routing-Technik beruht die Anonymität der Datenübertragung im Tor-Netzwerk?

* Onion-Routing (1 P.)
* Star-Shape-Routing (0 P.)
* Cross-Routing (0 P.)
* Local-Routing (0 P.)