DLMCSEAITSC02\_Unit01\_Question01

How many keys does Caesar’s cipher have (excluding the trivial one)?

* 25 (1 Pts)
* 12 (0 Pts)
* 13 (0 Pts)
* 26 (0 Pts)

DLMCSEAITSC02\_Unit01\_Question02

For which non-trivial key is Caesar’s cipher idempotent, that is, encrypting the ciphertext again yields the plaintext?

* 13 (1 Pts)
* 1 (0 Pts)
* 2 (0 Pts)
* 26 (0 Pts)

DLMCSEAITSC02\_Unit01\_Question03

Which cryptographic algorithm comes closest to satisfying Kerckhoff’s principle?

* one-time pad (1 Pts)
* Enigma (0 Pts)
* ADFGVX (0 Pts)
* scytale (0 Pts)

DLMCSEAITSC02\_Unit01\_Question04

Which one is an encryption algorithm?

* AES (1 Pts)
* MD5 (0 Pts)
* SHA-1 (0 Pts)
* CRC (0 Pts)

DLMCSEAITSC02\_Unit01\_Question05

Which one is a hash function that is not cryptographic?

* CRC (1 Pts)
* MD5 (0 Pts)
* SHA-1 (0 Pts)
* AES (0 Pts)

DLMCSEAITSC02\_Unit02\_Question01

Which cipher is a substitution cipher?

* Enigma (1 Pts)
* scytale (0 Pts)
* AES (0 Pts)
* DES (0 Pts)

DLMCSEAITSC02\_Unit02\_Question02

Which cipher is perfectly secure?

* one-time pad (1 Pts)
* RSA (0 Pts)
* AES (0 Pts)
* DES (0 Pts)

DLMCSEAITSC02\_Unit02\_Question03

What is the smallest key size used by AES?

* 128 (1 Pts)
* 56 (0 Pts)
* 512 (0 Pts)
* 2048 (0 Pts)

DLMCSEAITSC02\_Unit02\_Question04

Which hash function is not cryptographic?

* CRC (1 Pts)
* SHA-1 (0 Pts)
* MD4 (0 Pts)
* WHIRLPOOL (0 Pts)

DLMCSEAITSC02\_Unit02\_Question05

Which cipher is a stream cipher?

* Enigma (1 Pts)
* RSA (0 Pts)
* AES (0 Pts)
* DES (0 Pts)

DLMCSEAITSC02\_Unit03\_Question01

What is the inverse of the trapdoor function used in RSA?

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

DLMCSEAITSC02\_Unit03\_Question02

What is the fastest known algorithm to attack RSA?

* general number field sieve (1 Pts)
* Pollard’s ρ (0 Pts)
* smart attack (0 Pts)
* baby-step giant-step (0 Pts)

DLMCSEAITSC02\_Unit03\_Question03

What is the minimum key size of RSA to be currently considered secure, for example, by the NIST?

* 3072 (1 Pts)
* 1024 (0 Pts)
* 2048 (0 Pts)
* 4096 (0 Pts)

DLMCSEAITSC02\_Unit03\_Question04

What key size in ECC is as secure as a 256-bit key in AES?

* 512 (1 Pts)
* 256 (0 Pts)
* 1024 (0 Pts)
* 2048 (0 Pts)

DLMCSEAITSC02\_Unit03\_Question05

What is *88* congruent to modulo *7*?

* 11 (1 Pts)
* 1 (0 Pts)
* 16 (0 Pts)
* 24 (0 Pts)

DLMCSEAITSC02\_Unit04\_Question01

Which protocol is not a challenge-response authentication protocol?

* TAN (1 Pts)
* Digest-MD5 (0 Pts)
* CRAM (0 Pts)
* SCRAM (0 Pts)

DLMCSEAITSC02\_Unit04\_Question02

Which computationally difficult discrete mathematical function does Schnorr’s protocol rely on?

* logarithm (1 Pts)
* quadratic root (0 Pts)
* exponential (0 Pts)
* square (0 Pts)

DLMCSEAITSC02\_Unit04\_Question03

Which data does not enter the computation of the salted password in SCRAM?

* current time (1 Pts)
* password (0 Pts)
* salt (0 Pts)
* IterationCount (0 Pts)

DLMCSEAITSC02\_Unit04\_Question04

How many minutes difference does Kerberos allow for between the different authenticating parties times?

* 5 (1 Pts)
* 1 (0 Pts)
* 2 (0 Pts)
* 10 (0 Pts)

DLMCSEAITSC02\_Unit04\_Question05

How many times does a client encrypt a TCP packet before sending it to the server on the Tor network?

* as many as there are nodes (1 Pts)
* twice as many (0 Pts)
* once (0 Pts)
* twice (0 Pts)

DLMCSEAITSC02\_Unit05\_Question01

Which minimal key size is currently recommended as secure for RSA and Diffie-Hellman?

* 2048 bits (1 Pts)
* 512 bits (0 Pts)
* 1024 bits (0 Pts)
* 4096 bits (0 Pts)

DLMCSEAITSC02\_Unit05\_Question02

Which minimal key size is currently recommended as secure for Elliptic Curve Cryptography?

* 256 bits (1 Pts)
* 128 bits (0 Pts)
* 160 bits (0 Pts)
* 512 bits (0 Pts)

DLMCSEAITSC02\_Unit05\_Question03

Which minimal key size is currently recommended as secure for AES?

* 112 bits (1 Pts)
* 80 bits (0 Pts)
* 128 bits (0 Pts)
* 256 bits (0 Pts)

DLMCSEAITSC02\_Unit05\_Question04

Which computationally difficult problem is the security of RSA based on?

* prime number decomposition (1 Pts)
* discrete logarithm (0 Pts)
* point counting (0 Pts)
* quadratic residue (0 Pts)

DLMCSEAITSC02\_Unit05\_Question05

Which computationally difficult problem is the security of the Diffie-Hellman key exchange based on?

* discrete logarithm (1 Pts)
* prime number decomposition (0 Pts)
* point counting (0 Pts)
* quadratic residue (0 Pts)

DLMCSEAITSC02\_Unit06\_Question01

How many layers does the OSI model have?

* 7 (1 Pts)
* 4 (0 Pts)
* 5 (0 Pts)
* 10 (0 Pts)

DLMCSEAITSC02\_Unit06\_Question02

How many layers does the TCP/IP reference model have?

* 4 (1 Pts)
* 3 (0 Pts)
* 5 (0 Pts)
* 7 (0 Pts)

DLMCSEAITSC02\_Unit06\_Question03

Which protocol is not part of the IPsec protocol family?

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

DLMCSEAITSC02\_Unit06\_Question04

Which kind of (cryptographic) algorithm is “not” agreed on during the TLS handshake?

* an error-correction check sum such as CBC (1 Pts)
* an asymmetric algorithm such as RSA (0 Pts)
* a symmetric algorithm such as AES (0 Pts)
* a cryptographic hash algorithm such as SHA256 (0 Pts)

DLMCSEAITSC02\_Unit06\_Question05

Which security feature is neither part of the S/MIME nor OpenPGP protocol?

* perfect forward secrecy (1 Pts)
* asymmetric encryption and decryption (0 Pts)
* digital signature (0 Pts)
* integrity verification (0 Pts)

DLMCSEAITSC02\_Unit07\_Question01

Which part of a cipher is, in practice, most susceptible to being exploited?

* the pseudo-random number generator (1 Pts)
* the decryption algorithm (0 Pts)
* the encryption algorithm (0 Pts)
* the private key (0 Pts)

DLMCSEAITSC02\_Unit07\_Question02

Which algorithm is secure against a quantum computer?

* AES (1 Pts)
* RSA (0 Pts)
* ECC (0 Pts)
* Diffie-Hellman (0 Pts)

DLMCSEAITSC02\_Unit07\_Question03

For how many years is a 128-bit AES key expected to stay secure?

* 20 (1 Pts)
* 10 (0 Pts)
* 40 (0 Pts)
* 60 (0 Pts)

DLMCSEAITSC02\_Unit07\_Question04

Which AES key size does an RSA key of 2048 bits compare to?

* 192 (1 Pts)
* 80 (0 Pts)
* 112 (0 Pts)
* 128 (0 Pts)

DLMCSEAITSC02\_Unit07\_Question05

Which AES key size does an ECC key of 256 bits compare to?

* 128 (1 Pts)
* 80 (0 Pts)
* 112 (0 Pts)
* 192 (0 Pts)

DLMCSEAITSC02\_Unit08\_Question01

Which home banking protocol standard precedes FinTS?

* HBCI (1 Pts)
* IFX (0 Pts)
* OFX (0 Pts)
* SET (0 Pts)

DLMCSEAITSC02\_Unit08\_Question02

Which TAN procedure is resistant to phishing but not to man-in-the-middle attacks?

* indexed TAN (iTAN) (1 Pts)
* mobile TAN (mTAN) (0 Pts)
* basic TAN (0 Pts)
* CRAM (0 Pts)

DLMCSEAITSC02\_Unit08\_Question03

How long, on average, does the addition of a new block to the Bitcoin block chain network take?

* ten minutes (1 Pts)
* one second (0 Pts)
* one minute (0 Pts)
* one hour (0 Pts)

DLMCSEAITSC02\_Unit08\_Question04

What does the Greek word steganos translate to?

* covered (1 Pts)
* hide (0 Pts)
* obfuscate (0 Pts)
* embed (0 Pts)

DLMCSEAITSC02\_Unit08\_Question05

What routing technique does the anonymity of data transfer in the Tor network rest on?

* onion routing (1 Pts)
* star shape routing (0 Pts)
* cross routing (0 Pts)
* local routing (0 Pts)