Kahoot – Classical EnvryptionTechniques

Q1: Decryption can be represented as C = E(K, P)

- true
- false

Q2: The OTP scheme is unbreakable.

- true
- false

Q3: In computer security DES stands for Data Entity Solutions

- true
- false

Q4: In brute force attacks every possible key must be tried in order to break the code

- true
- false

Q5: Techniques used for deciphering a message without any knowledge of the enciphering details is

- blind deciphering
- steganography
- cryptanalysis
- permutation

Q6: ___ attacks exploit the characteristics of the algorithm to try and deduce specific plaintext

- stream cipher
- OTP
- brute-force
- cryptanalytic

Q7: This is the easiest attack to defend against

- ciphertext only
- plaintext only
- known plaintext
- chosen ciphertext

Q8: The simplest transposition cipher is the

- rail fence
- Playfair matrix
- Vernam cipher
- OTP

Q9: The OTP is unconditionally secure

- false
- true

Q10: Encryption and decryption are performed using different keys in conventional encryption

- True
- False

Q11: The Playfair matrix is computationally secure

- true
- false

Q12: Symmetric encryption remains by far the most widely used of the two types of encryption

- True
- False

Q13: The earliest known substitution cipher was the

- OTP
- Caesar cipher
- Playfair cipher
- Vigenere cipher

Q14: An alteration of the plaintext by an adversary is a loss of

- confidentiality
- integrity
- credibility
- availability

Q15: In symmetric encryption the principal security problem is key secrecy

- False
- True

Q16: Nonrepudiation can be achieved by using

- a digital signature
- a Playfair scheme
- a(n) OTP
- encryption

Q17: A _____ is a potential for violation of security.

- passive attack
- active attack
- aggressive attack
- none of the above

Q18: In the US, the release of medical records is regulated by

- FERPA
- the NFL
- HIPAA
- DES

Q19: Encryption algorithms and digital signatures are examples of security services

- true
- false

Q20: Viruses and worms are examples of

- adware
- bloatware
- malware
- spyware

Q21: How many keys must be tried on average to brute force a 128-bit key?

- 2^{64}
- 2^{127}
- 128
- 1.8446744×10^{19}

Q22: If it takes 1 hour to brute force a 64 bit-key, how long will it take for a 74-bit key

- 10 hours
- 42 days
- 42 months
- 42 years

Q23: If a 128 byte message is to be sent using a stream cipher, the key must be

- at least 128 bits
- 512 bits
- 1024 bits
- 1024 bytes

Q24: Using the Playfair Matrix wih a key B, the ciphertext for the message AAA is

- WCWCWC
- CCC
- CWCWCW
- WWW

Q25: Using the Vigenere cipher, with a secret key = B and the message AAA, the ciphertext is

- BBB
- BAA
- neither
- both