1. Use Caesar’s Cipher to decipher the following

HQFUBSWHG WHAW

a) ABANDONED LOCK

b) ENCRYPTED TEXT

c) ABANDONED TEXT

d) ENCRYPTED LOCK

Answer: b

Explanation: Caesar Cipher uses C =(p+3) mod 26 to encrypt.

2. Caesar Cipher is an example of

a) Poly-alphabetic Cipher

b) Mono-alphabetic Cipher

c) Multi-alphabetic Cipher

d) Bi-alphabetic Cipher

Answer: b

Explanation: Caesar Cipher is an example of Mono-alphabetic cipher, as single alphabets are encrypted or decrypted at a time.

3. Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.

a) True

b) False

Answer: b

Explanation: Monoalphabetic ciphers are easier to break because they reflect the frequency of the original alphabet.

4. Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis.

a) Random Polyalphabetic, Plaintext, Playfair

b) Random Polyalphabetic, Playfair, Vignere

c) Random Polyalphabetic, Vignere, Playfair, Plaintext

d) Random Polyalphabetic, Plaintext, Beaufort, Playfair

Answer: c

Explanation: Random Polyalphabetic is the most resistant to frequency analysis, followed by Vignere, Playfair and then Plaintext.

5. Which one of the following modes of operation in DES is used for operating short data?

a) Cipher Feedback Mode (CFB)

b) Cipher Block chaining (CBC)

c) Electronic code book (ECB)

d) Output Feedback Modes (OFB)

Answer: c

Explanation: The Electronic code book mode is used for operating on short data as the same key is used for each block. Thus repetitions in Plain Text lead to repetitions in Cipher Text.

6. Which of the following is false for ECB mode of operation

i) The Plain text is broken into blocks of size 128 bytes

ii) Blocks can be swapped, repeated, replaced without recipient noticing

iii) Good for short data

iv) Encryption of each block is done separately using a randomly generated key for each block

a) i) only

b) ii) and iii)

c) i) and iv)

d) i) ii) and iv)

Answer: c

Explanation: Block size is 64 bits. The same Key is used for each block.

7. On Encrypting “thepepsiisintherefrigerator” using Vignere Cipher System using the keyword “HUMOR” we get cipher text-

a) abqdnwewuwjphfvrrtrfznsdokvl

b) abqdvmwuwjphfvvyyrfznydokvl

c) tbqyrvmwuwjphfvvyyrfznydokvl

d) baiuvmwuwjphfoeiyrfznydokvl

Answer: b

Explanation: Cipher text:= Ci = Pi + ki mod m (mod 26).

8. On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text

a) nlazeiibljji

b) nlazeiibljii

c) olaaeiibljki

d) mlaaeiibljki

Answer: a

Explanation: Cipher text:= Ci = Pi + ki mod m (mod 26).

9. If a|b and b|c, then a|c.

a) True

b) False

Answer: a

Explanation: The statement is true. For ex, 11|66 and 66|198 = 11|198.

10. What is 11 mod 7 and -11 mod 7?

a) 4 and 5

b) 4 and 4

c) 5 and 3

d) 4 and -4

Answer: d

Explanation:11 mod 7 = 4 ; -11 mod 7 = -4 mod 7 = 3 mod 7.

11. Which of the following is a valid property for concurrency?

a) a = b (mod n) if n|(a-b)

b) a = b (mod n) implies b = a (mod n)

c) a = b (mod n) and b = c (mod n) implies a = c (mod n)

d) All of the mentioned

Answer: d

Explanation: All are valid properties of congruences and can be checked by using substituting values.

12. The multiplicative Inverse of 550 mod 1769 is

a) 434

b) 224

c) 550

d) Does not exist

Answer: a

Explanation: The multiplicative Inverse of 550 mod 1769 is 550.

13. Public key encryption/decryption is not preferred because

a) it is slow

b) it is hardware/software intensive

c) it has a high computational load

d) all of the mentioned

Answer: d

Explanation: Due to high computational load (thus being slow) public key systems are not preferred for large cryptosystems and large networks.

14. Which one of the following is not a public key distribution means?

a) Public-Key Certificates

b) Hashing Certificates

c) Publicly available directories

d) Public-Key authority

Answer: b

Explanation: Hashing certificates is some I just made up. It doesn’t exist noob.

15. What is the PGP stand for?

a) Permuted Gap Permission

b) Permuted Great Privacy

c) Pretty Good Privacy

d) None of the mentioned

Answer: d

Explanation: PGP stands for Pretty Good Privacy.

16. PGP makes use of which cryptographic algorithm?

a) DES

b) AES

c) RSA

d) Rabin

Answer: c

Explanation: PGP recommends the use of RSA.

17. Which of the following public key distribution systems is most secure?

a) Public-Key Certificates

b) Public announcements

c) Publicly available directories

d) Public-Key authority

Answer: a

Explanation: Public certificates are the most secure key distribution/management systems right now.

18. Which system uses a trusted third party interface?

a) Public-Key Certificates

b) Public announcements

c) Publicly available directories

d) Public-Key authority

Answer: a

Explanation: Public-Key certificates use a trusted third party interface.

19. Publicly Available directory is more secure than which other system?

a) Public-Key Certificates

b) Public announcements

c) Public-Key authority

d) None of the mentioned

Answer: b

Explanation: Publicly Available directory is more secure than Public announcements.

20. AES uses a ____________ bit block size and a key size of __________ bits.

a) 128; 128 or 256

b) 64; 128 or 192

c) 256; 128, 192, or 256

d) 128; 128, 192, or 256

Answer: d

Explanation: It uses a 128-bit block size and a key size of 128, 192, or 256 bits.

21. How many rounds does the AES-192 perform?

a) 10

b) 12

c) 14

d) 16

Answer: b

Explanation: AES 192 performs 12 rounds.

22. There is an addition of round key before the start of the AES round algorithms.

a) True

b) False

Answer: a

Explanation: In AES the final round contains only three transformations, and there is an initial single transformation (Add Round Key) before the first round which can be considered Round 0. Each transformation takes 4×4 matrixes as input and produces a 4×4 matrix as output.

23. How many modes of operation are there in in DES and AES?

a) 4

b) 3

c) 2

d) 5

Answer: d

Explanation: DES has 5 modes of operation.

24.Which of the following statements are true

i) In the CBC mode, the plaintext block is XORed with previous ciphertext block before encryption

ii) The CTR mode does not require an Initialization Vector

iii) The last block in the CBC mode uses an Initialization Vector

iv) In CBC mode repetitions in plaintext do not show up in ciphertext

a) iii)

b) ii) and iv)

c) All the Statements are true

d) i) ii) and iv)

Answer: d

Explanation: The first block in CBC mode uses an IV.

25. There is a dependency on the previous ‘s’ bits in every stage in CFB mode. Here ‘s’ can range from ___

a) 8-16 bits

b) 8-32 bits

c) 4-16 bits

d) 8-48 bits

Answer: b

Explanation: The range of the output of each stage of the cipher system is 8-32 bits for a 64 bit system.

26. Which of the following can be classified under advantages and disadvantages of OFB mode?

i) Transmission errors

ii) A bit error in a ciphertext segment

iii) Cannot recover from lost ciphertext segments

iv) Ciphertext or segment loss

a) Advantages: None; Disadvantages: All

b) Advantages: All; Disadvantages: None

c) Advantages: i); Disadvantages: ii) iii) iv)

d) Advantages: i); ii) Disadvantages: iii) iv)

Answer: d

Explanation: Advantages:

More resistant to transmission errors.

A bit error in a ciphertext segment affects only the decryption of that segment.

Disadvantages:

Cannot recover from lost ciphertext segments.

If a ciphertext segment is lost, all following segments will be decrypted incorrectly (if the receiver is not aware of the segment loss).

27. Which of the following modes does not implement chaining or “dependency on previous stage computations”?

a) CTR, ECB

b) CTR, CFB

c) CFB, OFB

d) ECB, OFB

Answer: a

Explanation: Only CTR and ECB do not implement chaining.

28. The counter value in CTR modes repeats are a regular interval.

a) True

b) False

Answer: b

Explanation: The Counter value in CTR mode should never be repeated, else it leads to vulnerability of the mode. We must ensure never reuse key/counter values; otherwise it could break (OFB).

29. “Rabin Cryptosystem is a variant of the Elgamal Cryptosystem”

a) True

b) False

Answer: b

Explanation: Rabin Cryptosystem is a variant of the RSA Cryptosystem.

30. Using Rabin cryptosystem with p=23 and q=7

Encrypt P=24 to find ciphertext. The Cipher text is

a) 42

b) 93

c) 74

d) 12

Answer: b

Explanation: Calculate n = p × q = 161

Plaintext P = 24

Ciphertext = C ≡ P2 (mod n)

= 242 mod 161 = 93 mod 161

Ciphertext transmitted = 93.

31. Sender chooses p = 107, e1 = 2, d = 67, and the random integer is r=45. Find the plaintext to be transmitted if the ciphertext is (28,9).

a) 45

b) 76

c) 66

d) 13

Answer: c

Explanation: P = [C2 (C1d)-1] mod p = 66.

32. ____________ is a mono-alphabetic encryption code wherein each & every letter of plain-text is replaced by another letter in creating the cipher-text.

a) Polyalphabetic Cipher

b) Caesar Cipher

c) Playfair Cipher

d) Monoalphabetic Cipher

Answer: b

Explanation: Caesar Cipher is the simplest type of substitution cipher with a mono-alphabetic encryption code wherein each letter of plain-text is replaced by another letter in creating the cipher-text.

33. _____________ is the concept that tells us about the replacement of every alphabet by another alphabet and the entire series gets 'shifted' by some fixed quantity.

a) Rolling Cipher

b) Shift Cipher

c) Playfair Cipher

d) Block Cipher

Answer: b

Explanation: Shift Cipher is the concept that tells us about the replacement of every alphabet by another alphabet and the entire series gets 'shifted' by some fixed quantity (which is the key) between 0 and 25.

34. ________________ is a cipher formed out of substitution where for a given key-value the cipher alphabet for every plain text remains fixed all through the encryption procedure.

a) Polyalphabetic Cipher

b) Caesar Cipher

c) Playfair Cipher

d) Monoalphabetic Cipher

Answer: d

Explanation: Monoalphabetic cipher is a cipher formed out of substitution where for a given key-value the cipher alphabet for every plain text remains fixed all through the encryption procedure.

35. In Playfair cipher, at first, a key table is produced. That key table is a 5 by 5 grid of alphabets which operates as the key to encrypt the plaintext.

a) Rolling Cipher

b) Shift Cipher

c) Playfair Cipher

d) Block Cipher

Answer: c

Explanation: In Playfair cipher, at first, a key table is produced. That key table is a 5 by 5 grid of alphabets which operates as the key to encrypt the plaintext. All the twenty-five alphabets have to be unique and letter J gets omitted.

36 ._____________ employs a text string as a key that is implemented to do a series of shifts on the plain-text.

a) Vigenere Cipher

b) Shift Cipher

c) Playfair Cipher

d) Block Cipher

Answer: a

Explanation: Vigenere Cipher employs a text string as a key that is implemented to do a series of shifts on the plain-text. Here the sender & the receiver settle on a single key.

37. The ________________ has piece of the keyword that has the same length as that of the plaintext.

a) Block Cipher

b) One-time pad

c) Hash functions

d) Vigenere Cipher

Answer: b

Explanation: The one-time pad has a piece of the keyword that has the same length as that of the plaintext. The keyword gets a randomly produced string of alphabets. For only once, its keyword is used.

38. In _____________ a sequence of actions is carried out on this block after a block of plain-text bits is chosen for generating a block of cipher-text bits.

a) Block Cipher

b) One-time pad

c) Hash functions

d) Vigenere Cipher

Answer: a

Explanation: In block cipher, a sequence of actions is carried out on this block after a block of plain-text bits is chosen for generating a block of cipher-text bits. Blocks in these have fixed number of bits.

39. In _______________ the plain-text is processed 1-bit at a time & a series of actions is carried out on it for generating one bit of cipher-text.

a) Block Cipher

b) One-time pad

c) Stream cipher

d) Vigenere Cipher

Answer: c

Explanation: In stream ciphers, the plain-text is processed 1-bit at a time & a series of actions is carried out on it for generating one bit of cipher-text.

40. The procedure to add bits to the last block is termed as _________________

a) decryption

b) hashing

c) tuning

d) padding

Answer: d

Explanation: For a block cipher, a chain of actions is performed on this block after a block of plain-text. In block ciphers procedure to add bits to the last block is termed as padding.

41. Which of the following is not an example of a block cipher?

a) DES

b) IDEA

c) Caesar cipher

d) Twofish

Answer: c

Explanation: In a block cipher, a sequence of actions is carried out on this block after a block of plain-text bits is chosen for generating a block of cipher-text bits. Examples of block ciphers are DES, IDEA, Twofish etc.

42. Data Encryption Standard is implemented using the Feistel Cipher which employs 16 round of Feistel structure.

a) DES

b) IDEA

c) Caesar cipher

d) Twofish

Answer: a

Explanation: Data Encryption Standard is a block cipher which implements the Feistel Cipher which employs 16 round of Feistel structure. The block size it uses is 64-bit.

43. DES stands for ________________

a) Data Encryption Security

b) Data Encrypted Standard

c) Device Encryption Standard

d) Data Encryption Standard

Answer: d

Explanation: DES which is abbreviated as Data Encryption Standard falls under the category of a block cipher that implements the Feistel Cipher which employs 16 round of Feistel structure.

44. ____________ carries out all its calculations on bytes rather than using bits and is at least 6-times faster than 3-DES.

a) AES

b) DES

c) IDEA

d) Twofish

Answer: a

Explanation: Advanced Encryption Standard is a comparatively innovative block cipher that carries out all its calculations on bytes rather than using bits and is at least 6-times faster than 3-DES.

45. AES stands for ________________

a) Advanced Encryption Security

b) Advanced Encryption Standard

c) Advanced Encrypted Standard

d) Active Encryption Standard

Answer: b

Explanation: AES is abbreviated as Advanced Encryption Standard which is a moderately innovative block cipher which carries out all its calculations on bytes rather than using bits and is at least six times faster than 3-DES.

46. Message authentication code is also known as

a) key code

b) hash code

c) keyed hash function

d) message key hash function

Answer: c

Explanation: Message authentication code is also known as keyed hash function.

47. What is a one-way password file?

a) A scheme in which the password is jumbled and stored

b) A scheme in which the password is XOR with a key and stored

c) A scheme in which the hash of the password is stored

d) A scheme in which the password is passed through a PRF, which is then stored

Answer: c

Explanation: A scheme in which the hash of the password is stored by an operating system rather than the password itself is the one-way password file system.

48. Which one of the following is not an application hash functions?

a) One-way password file

b) Key wrapping

c) Virus Detection

d) Intrusion detection

Answer: b

Explanation: Key wrapping is a separate algorithm and not an application of hash fuctions.

49. If the compression function is collision resistant, then so is the resultant iterated hash function.

a) True

b) False

Answer: a

Explanation: The statement is true. The problem of designing a secure hash function reduces to that of designing a collision resistant compression function.

50. A larger hash code cannot be decomposed into independent subcodes.

a) True

b) False

Answer: b

Explanation: Hash codes can be decomposed into independent subcodes and this was the logic behind the meet in the middle attack.