SECRYPT - Item 3 Cryptography Exam - Practice Questions

Which of the following correctly encrypts the plaintext RASPBERRY using the Caesar Cipher with a single shift?
A) suhkjdfjj
B) szjiolkja
C) sbtqcfssz
D) sdighfwue
E) sbtqlksdj
ANSWER: C

Which of the following most accurately describes the modulo operation?
A) It is prime number only division.
B) It is the remainder from division.
C) It is the result from division.
D) It is the inverse of the log operation.
E) It is the inverse of exponentiation.
ANSWER: B

What is the result of the operation 23 mod 11?
A) 0
B) 1
C) 3
D) 5
E) 7
ANSWER: B

A simple mono-alphabetic substitution cipher has how many possible keys?
A) 26
B) 26!
C) 26^2
D) 26^25
E) 26! - 25!
ANSWER: B

Which of the following is most likely the plaintext decryption of the ciphertext ETTLDM ORWNRR HUTEOF SSITKA HHHEIE TOAGWD, given that it has been encrypted using a columnar transposition cipher?
A) From Fairest Creatures We Desire Increase
B) When Forty Winters Shall Besiege Thy Brow
C) Look In Thy Glass, And Tell The Face Thou Viewest
D) Unthrifty Loveliness, Why Dost Thou Spend
E) Those Hours, That With Gentle Work Did Frame
ANSWER: E

Which of the following patterns would be used in a dictionary attack on the ciphertext `njtdpmdfosjpm` when recovering the key mapping of a mono-alphabetic substitution cipher?

A) ABCDEFDGHIBEF
B) ABCDEFGHDIBEF
C) ABCDEFGHDIBEB
D) ABCCDEFGHDIBE
E) None of the above
ANSWER: A

If the index of coincidence of a cipher-text is significantly higher for keylengths 4, 8, 12, 16 than for all other numbers below 16 then which of the following is the most likely conclusion?
A) The cipher-text was encrypted using a key 3 bits long
B) The cipher-text was encrypted using a key 3 characters long.
C) The cipher-text was encrypted using a key 4 bits long.
D) The cipher-text was encrypted using a key 4 characters long.
E) The cipher-text was encrypted using a key 8 buts long.
ANSWER: D

Which of the following is a permutation of the binary value 01111010 using the following Permutation Box?

```
input:  1  2  3  4  5  6  7  8
output: 1  3  5  7  2  4  6  8
```

A) 01111100
B) 10000101
C) 10100111
D) 00111110
E) 01011100
ANSWER: A

Which of the following is a true statement with regards to the XOR cipher?
A) The ciphertext can be calculated as the XOR of the plaintext with the key.
A) The plaintext can be calculated as the XOR of the ciphertext with the key.
C) The key can be calculated as the XOR of the plaintext with the ciphertext.
D) All of the above.
E) None of the above.
ANSWER: D

Which of the following was NOT a finalist considered for adoption as the AES standard?
A) MARS,
B) DES
C) RC6
D) Serpent
E) Twofish
ANSWER: B

Which of the following are valid round operations in AES (round functions)?
A) AddRoundKey() and MixColumns()
B) ReverseColumn() and RotateKey()
C) XorSubKey() and InvertMatrix()
D) All of the above.

E) None of the above.
ANSWER: A

Which of the following is the correct decryption of the ciphertext 01010111, which was encrypted using the XOR Cipher with the key 01101011?
A) 01010000
B) 10101111
C) 01011011
D) 00111100
E) 10100000
ANSWER: D

Which of the following is a correct statement with regards to Feistel ciphers?
A) Breaks the problem of designing a good block cipher into the design of a good key expansion algorithm and a good round function
B) Breaks the problem of designing a good block cipher into the design of a good substitution function and a good permutation function
C) Feistel networks use a different key for encryption than for decryption.
D) Feistel networks use the same key for several rounds therefore increasing security.
E) None of the above
ANSWER: A

Which of the following key sizes does AES offer?
A) 128, 192 and 256 bits
B) 64, 96 and 128 bits
C) 156, 212 and 284 bits
D) 256, 446 and 512 bits
E) 128 bits only
ANSWER: A

Which of the following statements about AES is true?
A) It is more secure than RSA as it is an officially approved algorithm by the US government.
B) It always uses an initialisation vector and a key in every mode of operation.
C) The key-size is large enough for the foreseeable future to be secure.
D) All of the above.
E) None of the above.
ANSWER: C

Why is DES no longer recommended for use in new products requiring encryption?
A) DES is broken and the key can be recovered easily due to statistical anomalies.
B) The key is too short.
C) The block size is too long.
D) DES was built at the NSA and so it may have backdoors.
E) DES is still recommended.
ANSWER: B

Which of the following padding schemes is least advisable in practice?
A) Pad the message with zeros but make the last byte indicate the length of padding added.

B) Pad the message with random bytes but make the last byte indicate the length of padding added.
C) Pad the message with every byte of padding indicating the length of padding added.
D) Pad the message with all zeros.
E) None the above is less advisable than the others.
ANSWER: D

If every block of plaintext 16 byte block was the same, then AES in which mode of operation would generate ciphertext with a repeating pattern?
A) Electronic Code Book (ECB)
B) Cipher Block Chaining (CBC)
C) Galois Counter Mode (GCM)
D) Output Feedback Mode (OFB)
E) None of these.
ANSWER: A

Which of the following modes of operation provides authentication as well as confidentiality?
A) Electronic Code Book (ECB)
B) Cipher Block Chaining (CBC)
C) Galois Counter Mode (GCM)
D) Output Feedback Mode (OFB)
E) None of these.
ANSWER: C

Which of the following statements is true about a block cipher used in Cipher Block Chaining Mode?
A) The block sizes are shorter because there needs to be room for the initialisation vector.
B) It can only encrypt and cannot decrypt.
C) It uses a much smaller key than in other modes.
D) Errors may propagate to the next block.
E) Each block is encrypted independently of the others.
ANSWER: D

What is the key difference between a stream cipher and a block cipher?
A) Stream ciphers require padding, but block ciphers do not.
B) Stream ciphers use smaller prime numbers and are faster than block ciphers.
C) A block cipher is essentially an XOR cipher and so much weaker than a stream cipher.
D) A stream cipher typically encrypts one bit/byte at a time while block ciphers encrypt several bytes at once.
E) Stream ciphers protect only integrity and not confidentiality.
ANSWER: D

What is the Greatest Common Divisor (GCD) of the numbers 24 and 12?
A) 1
B) 2
C) 4
D) 6
E) 12

ANSWER: E

Which of the following statements is true about an asymmetric cipher like RSA?
A) There are two keys, you use one for encryption and one for decryption.
B) There is one key, the same key is used for decryption and encryption.
C) The key can never be re-used because the cipher uses XOR.
D) An asymmetric cipher is a very strong one-time-pad.
E) Both keys can be made public.
ANSWER: A

Which of the following is the result of encrypting the integer value 4 using RSA with exponent e=3 and modulus p=27?
A) 0
B) 7
C) 10
D) 17
E) 27
ANSWER: C

Which of the following is a cryptographic hash function?
A) A5/1
B) MD5
C) LSFR
D) 3DES
E) ECC
ANSWER: B