Cryptography Unit-2

krish_srivastava@srmap.edu.in Switch account

Not shared

Draft saved

* Indicates required question

Roll number *

AP21110010302

1 * 1 point

Suppose you receive a ciphertext in Polish consisting of 5 unique letters and know that this ciphertext is produced by a Substitution Cipher. How many possible plaintexts are there that could have produced this ciphertext? Assume that there are 32 letters in the Polish alphabet.

- [ ] $32 \cdot 31 \cdot 30 \cdot 29 \cdot 28$
- [ ] 325
- [ ] 532
- [x] 32!
- [ ] None of the above
- [ ] Other:

2 *

1 point

Based on current knowledge, which of the following problems is NOT "difficult" to solve? A problem is considered to be difficult to solve when there is no known efficient algorithm that solves it.

- Given a large prime p and an integer a, finding an integer x such that a · x = 1 mod p
- Given a large composite n, finding all prime factors of n
- Given an integer a and a large composite n, finding an integer x such that x2 = a mod n
- Given integers a and b and a large prime p, finding an integer x such that ax = b mod p
- None of the above

3 *

1 point

Denote l as the effective key length for a block cipher E (). What is the effective key length of 4-E: C = E (K_1, E (K_2, E (K_3, E (K_4, P))))? Assume Ki's are keys, P is a plaintext and C is a ciphertext. (Hint: do not forget about Meet-in-the-Middle attack)

- l
- 2 · l
- 3 · l
- 4 · l
- None of the above

4 *

1 point

In Public/Private key cryptography, even the sender will no longer be able to read the message after encrypting it with the receiver's public key.

- (●) True
- ( ) False

5 *

1 point

The Data Encryption Standard (DES) is based on

- (●) Feistel Cipher
- ( ) Stream Cipher
- ( ) Rijndael Cipher
- ( ) Vigenere Cipher
- ( ) Caesar Cipher

6 * 1 point

Which of the following statements are true?

i) Stream Ciphers are fasters than Block Ciphers

ii) Block Ciphers can reuse keys

iii) Block ciphers use lesser code than stream ciphers

- (●) 1st and 2nd
- ( ) 1st only
- ( ) 2nd and 3rd
- ( ) All are true

7 * 1 point

Confusion hides the relationship between the ciphertext and the plaintext.

- (●) True
- ( ) False

8 * 1 point

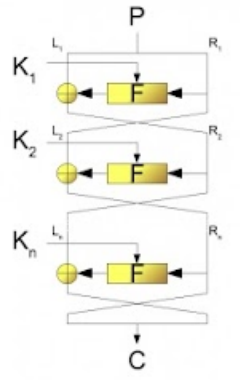
The S-Box is used to provide confusion, as it is dependent on the unknown key.

- (●) True
- ( ) False

9 *

1 point

This is an example of



- SP Networks
- Feistel Cipher
- Hash Algorithm
- Hill Cipher

10 *

1 point

Which of the following slows the cryptographic algorithm –
1) Increase in Number of rounds
2) Decrease in Block size
3) Decrease in Key Size
4) Increase in Sub key Generation

- 1 and 3
- 2 and 3
- 3 and 4
- 2 and 4

11 * 1 point

The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key

- ○ 12
- ○ 18
- ○ 9
- ◉ 16

12 * 1 point

The DES algorithm has a key length of

- ○ 128 Bits
- ○ 32 Bits
- ◉ 64 Bits
- ○ 16 Bits

13 * 1 point

. In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.

- ○ True
- ◉ False

14 1 point

In the DES algorithm the round key is _____ bit and the Round Input is _____bits.

- (●) 48, 32
- ( ) 64, 32
- ( ) 56, 24
- ( ) 32, 32

Clear selection

15 * 1 point

In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____

- (●) Scaling of the existing bits
- ( ) Duplication of the existing bits
- ( ) Addition of zeros
- ( ) Addition of ones

16 * 1 point

The number of unique substitution boxes in DES after the 48-bit XOR operation are

- (●) 8
- ( ) 4
- ( ) 6
- ( ) 12

17 1 point

In the DES algorithm the 64-bit key input is shortened to 56 bits by ignoring every 4th bit.

- ○ True
- ◉ False

Clear selection

18 * 1 point

GCD(a,b) = GCD(b,a mod b)

- ◉ True
- ○ False

19 * 1 point

Is S a ring from the following multiplication and addition tables?

+ a b x a b

a a b a a a

b b a b a b

- ◉ Yes
- ○ No
- ○ Can't Say
- ○ Insufficient Data

20 *

1 point

A very common field in this category is GF(2) with the set {1, 2} and two operations, addition and multiplication.

- ○ True
- ◉ False

21

1 point

Multiplication / Division follow which operation?

- ○ XOR
- ○ NAND
- ◉ AND
- ○ OR

Clear selection

22

1 point

How many numbers cannot be used in GF(p) in 2n where n=4?

- ○ 2
- ○ 5
- ◉ 3
- ○ 1

Clear selection

23 * 1 point

If $f(x)=x^4+x^2-x+2$ and $g(x)=x^2-x+1$, find: $f(x) - g(x)$

$x^3+2x^2 -x+3$

Option 1

x^3+x^2+3

Option 2

x^3+x+1

Option 3

x^2+2x+4

Option 4

24 * 1 point

. If $f(x)=x^4+x^2-x+2$ and $g(x)=x^2-x+1$, find: $f(x) - g(x)$

- [x] x^4+1 — Option 1
- [ ] x^2+1 — Option 2
- [ ] x^2+2x+6 — Option 3
- [ ] x^4-1 — Option 4

25 * 1 point

Find the 8-bit word related to the polynomial $x^5 + x^2 + x$

- [ ] 00010011
- [ ] 01000110
- [x] 00100110
- [ ] 11001010

26 * 1 point

Find the 8-bit word related to the polynomial $x^6 + x^5 + x^2 + x + 1$

- 00010011
- 11000110
- 00100110
- 01100111 (selected)

27 * 1 point

5/3 mod 7 =

- 2
- 3
- 4 (selected)
- 5

28 * 1 point

The polynomial x^{4+1} can be represented as –

- (x+1)(x3+x2+1)
- (x+1)(x3+x2+x)
- (x)(x2+x+1)
- None of the mentioned (selected)

29 * 1 point

-5 mod -3 =

- [ ] 3
- [ ] 2
- [x] 1
- [ ] 5

30 * 1 point

Multiply the polynomials $P_1 = x^5 + x^2 + x)$ by $P_2 = (x^7 + x^4 + x^3 + x2 + x)$ in GF(2^8) with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$. The result is

- [ ] Option 1: $x^4 + x^3 + x + 1$
- [x] Option 2: $x^5 + x^3 + x^2 + x + 1$
- [ ] Option 3: $x^5 + x^4 + x^3 + x + 1$
- [ ] Option 4: $x^5 + x^3 + x^2 + x$

Submit Clear form

Never submit passwords through Google Forms.