University of Jordan
Computer Engineering Department
Information and network security

date: 18 May 2023

Name: Number

Consider the following RSA usage for the next three questions.

Ali's Setup: p = 11 and q = 3. Ali chooses his private key =3.

Ali's public key is: 7 ✓

$\frac{20(i)+1}{3}$ ~~$\frac{24(i)+1}{3}$~~

Ali's Setup: p = 11 and q = 3. Ali's public key is 3:

Rabab sends him message M=14. The message received by Ali will be: 5 ✓

$M^3 \bmod 33 = 14^3 \bmod 33$

Ali's Setup: • p = 11 and q = 3, private key =3

Mohammad sends to Ali cipher text =19

The real message received by Ali is: 28 ✓

$C^d \bmod 33 = 19^3 \bmod 33$

The AES algorithm includes operations: Sub Byte, Shift rows, Mix Columns, Add round key and Key schedule. *Each of these operations provides confusion or diffusion* or both. Fill the following table with √ or x

Operation	Confusion	Diffusion
Sub Byte	✓ ✓	
Shift rows		✓ ✓
Mix Columns		✓
Add round key	✓ ✓	✓
Key schedule	✓ ✓	✓

1.5

4.5

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

128; 128 or 256	64; 128 or 192	) 256; 128, 192, or 256	[✓ 128; 128, 192, or 256]

Like DES, AES also uses Feistel Structure.

a) True

[✓ b) False]

How many rounds does the AES-192 perform?

10	[✓ 12]	14	16

How many rounds does the AES-256 perform?

10	12	[✓ 14]	16

Today is Thursday. What day it will be after 200 days: Monday

Now it is 12 o'clock.

After 100 hours the time will be: (writ your answer in 24 hours format) 16 o'clock

A cyclic group is built using prime number p=5.

The cardinality of this group is: 4

A cyclic group is built using prime number p=5.

The number of elements that have a cycle length of 1 is:

0	1	[✓ 2]	3	4

A cyclic group is built using prime number p=5.

The number of elements that have a cycle length of 2 is:

0	1	[✓ 2]	3	4

7

A cyclic group is built using prime number p=5.

The number of elements that have a cycle length of 3 is:

0	[✓ 1]	2	3	4

A cyclic group is built using prime number p=5.

The number of elements that have a cycle length of 4 is:

0	1	[✓ 2]	3	4

A cyclic group is built using prime number p=5.

Possible generator(s) is (are):

If you know that 13x11 =143

Then 9^{361} mod 143 is:

97 and 269 are prime numbers

23^{2680} mod 269 is: 19

Which trees are used in Blockchain technology?

In relation to Blockchain define Merkle root.

What are the important traits (features) of Blockchain technology?

Decentralization	Immutability	Transparency	[✓ All of the mentioned]

What are the advantages of Blockchain technology?

Security and speed	User control over data	[✓ Cost-effective transactions]	All of the mentioned

What is the name of the first block in a Blockchain?

[✓ Genesis block]	Origin block	Block one	None of the above

What is the incentive for miners to validate transactions?

Appreciation of the community	Nonce	Additional memory	[✓ Block rewards]

Find the least positive value of x such that $78 + x \equiv 3 \pmod{5}$

$\boxed{7}$

Ali and Rima wanted to agree on a shared key. They decided to use Diffie-Helman algorithm for that purpose. They agreed to use prime number p=23 and generator α=5.

Ali chose his private key as $\overset{X_A}{6}$ and Rima chose her private key as $\overset{X_B}{15}$.

The shared key will be: