CS4363/6373 - ASSIGNMENT – 4 ANSWER ALL QUESTIONS

In the context of cryptography or number theory, this is usually interpreted as the order of the number 36 in some multiplicative group $Z *_n$, but the group is not specified here.

Interpretation: Bit length of 36

Binary of 36 = 100100

That's 6 bits.

So, ||36|| = 6

Explanation:

The bit length of an integer n is:

$$\parallel n \parallel = \lfloor log_2(n) \rfloor + 1$$

Let's compute:

$$log_2(36) \approx 5.17$$

$$\lfloor log_2(36) \rfloor = 5$$

Final Answer:

Multiplicative group Z* n

The multiplicative group Z^*_n is the set of integers from 1 to n-1 that are coprime to n. The number of elements in this group is given by Euler's totient function $\varphi(n)$.

1. **Z** *₅₃

Since 53 is a prime number, all numbers from 1 to 52 are coprime to 53.

So:

$$\phi(53) = 53 - 1 = 52$$

There are 52 elements in the multiplicative group $Z *_{53}$.

$2. Z *_{15}$

Now 15 is not prime, so we must use Euler's totient function:

$$\phi(15) = \phi(3 \times 5) = \phi(3) \times \phi(5) = (3-1)(5-1) = 2 \times 4 = 8$$

Now, let's list all elements from 1 to 14 that are coprime to 15:

Coprime numbers: 1, 2, 4, 7, 8, 11, 13, 14

Answer: There are 8 elements, and they are:

$3.Z*_{851}$

First, factor 851:

$$851 = 23 \times 37(Both \ are \ primes)$$

Use Euler's formula:

$$\phi(851) = \phi(23) \times \phi(37) = (23 - 1)(37 - 1) = 22 \times 36 = 792$$

There are 792 elements in the multiplicative group $Z *_{851}$.

a procedure (in plain steps or pseudocode) to generate the elements of the multiplicative group Z^*N , where $N=p\times q$, and both p and q are prime numbers.

List all integers *a* such that:

- 1≤a<N
- gcd(a,N)=1

These elements form $Z *_N$.

Step-by-Step Procedure (Pseudocode Style):

Input: Two prime numbers p and q

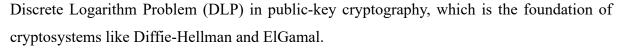
Output: List of elements in $Z *_N where N = p * q$

- 1. Set N = p * q
- 2. Create an empty list Z_star
- 3. For a in range from 1 to N-1:

If
$$gcd(a, N) == 1$$
:

Append a to Z_star

4. Return Z_{star}



Discrete Logarithm Setup:

working in a multiplicative group

Zq*, where:

q is a large prime

g is a generator of the group

You choose a secret/private number x

Then compute

 $y=gx \mod q$

So, in public-key cryptography based on DLP:

Public Key:

(g,q,y)

Private Key:

 χ

Why?

Because given g,q,y, it is computationally hard to find x such that:

$$g^x modq = y$$

This is the discrete logarithm problem, and that difficulty ensures security.

Answer:

• Private key: xxx

• Public key: (g,q,y)(g,q,y)(g,q,y)

To built on the difficulty of factoring a large number N = pq, where p and q are large primes.

1. Key Generation:

- Choose two large primes: ppp, qqq
- Compute $N=p\times q$
- Compute $\phi(N)=(p-1)(q-1)$
- Choose eee, such that $gcd(e,\phi(N))=1$
- Compute ddd, the modular inverse of emod $\phi(N)$

$$d \equiv e^{-1} mod \ \phi(N)$$

Public Key:

- N: the product of two primes
- e: the encryption exponent

Private Key:

- d: the decryption exponent
- (Alternatively, p and q, because they allow calculation of d)