Given:

$a_1 = 2$, $a_2 = 3$, $a_3 = 1$

$x \equiv 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 1 \cdot 12 \cdot 3 \mod 60$

$x \equiv 80 + 135 + 36 = 251 \mod 60$

$x \equiv 251 \mod 60 \Rightarrow x \equiv 11 \mod 60$

Q.4: charmichael number:

$a^{n-1} \equiv 1 \mod n$

step-1

561 = 3 x 187 = 3 x 11 x 17

561 prime factors: 3, 11, 17

step-2:

prime factorization: 3, 11, 17

1. n is square-free (no repeated prime factors)

2. For every time p dividing n, p-1 divides n-1

- p-1 divide 561-1 = 560

Step-3:

$a^{560} \equiv 1 \mod 561$

- a=2

$2^{560} \mod 561 = 1$

- a=10:

$10^{560} \mod 561 = 1$

- a=13:

$13^{560} \mod 561 = 1$

Q.5:

step-1

- $\phi(p) = p-1$
- $\{g^1, g^2 \ldots, g^{p-1}\} \mod p = \{1, 2, \ldots, p-1\}$
- $p-1 \mod p$

p=17,

$\phi(17) = 16$

$g^k \not\equiv 1 \mod 17$ for all $k < 16$, but $g^{16} \equiv 1 \mod 17$

step-2:

- $g^{16/q} \not\equiv 1 \mod 17$, q of 16

$16 = 2^4 \Rightarrow q = 2 \Rightarrow g^8, g^4, g^2 \not\equiv 1 \mod 17$

Step-3:

- $3^1 \bmod 17 = 3$
- $3^2 = (3)^2 = 9 \bmod 17 = 9$
- $3^4 = (3^2)^2 = 81 \bmod 17 = 13$
- $3^8 = (3^4)^2 = 13^2 = 169 \bmod 17 = 16$
- $3^{16} = (3^8)^2 = 16^2 = 256 \bmod 17 = 1$

powers = 1, only $3^{16} \equiv 1 \bmod 17$

Q-6:

$3^x \equiv 13 \bmod 17$

Step-by-step solution:

x	$3^x \bmod 17$
1	3
2	9
3	10
4	$3^4 = 81 \bmod 17 = 13$

$x = 4$ since, $3^4 \equiv 13 \bmod 17$

Q-7:

- p: a Large prime
- g: a primitive root modulo
- $g^a \bmod p$: party A's public key
- $g^b \bmod p$: party B's public key

Steps of the protocol:

1. public parameters:
2. private secrets.
3. Exchange.
4. shared secret computation.

Discrete Logarithm.

- $g^a \bmod p$
- $g^b \bmod p$

$g^a \equiv A \bmod p$

Security based on the DLP:

- $p > 2^{2048}$
- DLP in Z_p^*.

Q-8:

1. substitution cipher:

Alphabet: A → D, B → E, ... X → A, Y → B, Z → C

plaintext: HI ELL OW ORLD

ciphertext: KH OO RZ RU OG

Result: "KHOORZRUOG"

plaintext: HELLOWORLD

digraphs: HE IL LO OW OR LD

- HE → H (row 2, col 2), E (row 3, col 1) → CF
- LL → LX → L(4,1) X(5,4) → VS
  L → with filler X → VS
- OW → O (1,2) W (5,3) → NW
- OR → O (1,2), R (1,5) → NM
- LD → L (4,1), D (2,5) → TR

Result: "CFVSVSNWMTR"

Q-9:

* Encryption function:

$$E(x) = (ax + b) \bmod 26$$

- $a = 5$
- $b = 8$

plaintext: "Dept of ICT, MBSTU"

- x is the plaintext Letter (A=0, B=1, ... Z=25)
- gcd (a, 26) = 1 so, a = 5 is valid.

part-a: Encrypt the plaintext:

step-1

Dept of ICT MBSTU ⇒ DEPTOFICTMBSTU

step-2

A=0, B=1, ... Z=25

Part-B: Decryption

step-1

$$D(y) = a^{-1} \cdot (y - b) \bmod 26$$

- $a = 5$
- $a^{-1} \bmod 26 = 21$, $5 \cdot 21 = 105 \equiv 1 \bmod 26$

Decrypted plaintext:

DEPTOFICTMBSTU

Q-10: Encryption process:

1. key and block structure.
2. key derivation.
3. substitution step.
4. permutation step.

Decryption process:

1. key derivation.
2. Inverse permutation.
3. Inverse substitution.

Basic cryptanalysis of sp-shift cipher

- simple and lightweight for educational us
- PRNG-driven substitution and permutation obscure direct letter-to-letter mapping.
- multi-round application increases confusio and diffusion.

improvements

- use a Letter PRNG. or a key schedule algorithm.
- Introduce inter-block chaining

Is 1729 a carmichael number?

Yes, 1729 is a carmichael number.

A carmichael number is a composite number n that satisfies the congruence

$$a^{n-1} \equiv 1 \mod n$$

for all integers a that are relatively prime to n.

- 1729 is not prime $1729 = 7 \times 13 \times 19$
- All the prime factors of 1729 are distinct.
- For carmichael numbers, korselt's criterion says:

A number n is a carmichael number if and only if:

1. n is composite,

A number n is a carmichael number if and only if:

- for every prime divisor p of n, p-1 divides n-1

Prime factors : 7, 13, 19

- $n-1 = 1728$
- $7-1 = 6$, and $6 \mid 1728$
- $13-1 = 12$, and $12 \mid 1728$
- $19-1 = 18$, and $18 \mid 1728$

So, 1729 is a carmichael number.

1729 is also famous as the Hardy-Ramanujan number, being the smallest number..

$$1729 = 1^3 + 12^3 = 9^3 + 10^3$$

2. Primitive Root (or generator of Z_{23}?

- Z_{23}^* is the multiplicative group modulo 23.
- since 23 is prime, Z_{23}^* has order $23-1=22$.
- A primitive root modulo 23 is an integer g such that the smallest k for which $g^k \equiv 1 \mod 23$ is $k=22$

Step-2

$$g^{\frac{22}{p}} \not\equiv 1 \mod 23$$

- Prime divisors of 22: 2, 11
- so, we must check:
  - $g^{11} \not\equiv 1 \mod 23$
  - $g^2 \not\equiv 1 \mod 23$

Step-3

$g = 5$

- $5^2 = 25 = 2 \mod 23 \Rightarrow \neq 1$
- $5^{11} \mod 23$:
- $5^2 = 25 \equiv 2$
- $5^4 = (5^2)^2 = 2^2 = 4$
- $5^8 = (5^4)^2 = 4^2 = 16$
- $5^{11} = 5^8 \cdot 5^2 \cdot 5 = 16 \cdot 2 \cdot 5 = 160 \mod 23$
- $160 \mod 23 = 160 - 6 \cdot 23 = 160 - 138 = 22 \neq 1$

5 is a primitive root modulo 23

roots mod 23 include : 5, 7, 10, 11, 14, 15, 17, 19, 20, 21.

3. Is $\langle Z_{11}, +, * \rangle$ a Ring?

Yes, $Z_{11} = (Z_{11}, +, \cdot)$ is a ring.

Under addition (+):

- 1. closure: $a+b \in Z_{11}$
- 2. Associativity: $(a+b)+c = a+(b+c)$
- 3. Identity: $0 \in Z_{11}$ such that $a+0=a$
- 4. Inverses: Every $a \in Z_{11}$ has an additive inverse $-a \in Z_{11}$

5. commutativity: $a+b = b+a$

Under Multiplication (.):

1. closure: $a.b \in Z_{11}$
2. Associativity: $(ab)c = a(bc)$
3. Distributive laws:
   - Left: $a(b+c) = ab+ac$
   - Right: $(a+b)c = ac+bc$

Yes, $(Z_{11}, +, \cdot)$ is a ring.

4. Is $\langle Z_{37}, + \rangle, \langle Z_{35}, \times \rangle$ are abelian group?

1. $\langle Z_{37}, + \rangle$

This is the set of integers modulo 37 under addition.

- $a+b \bmod 37 \in Z_{37}$
- Addition mod 37 is associative.
- 0 is the additive identity.
- Every element $a \in Z_{37}$ has an inverse $-a \bmod 37$.
- $a+b = b+a \bmod 37$

Yes, $\langle Z_{37}, + \rangle$ is an abelian group.

2. $\langle Z_{35}, \times \rangle$

This is the set $Z_{35} = \{0, 1, \ldots 34\}$ under multiplication mod 35

- 1 is the multiplicative identity.
- $\gcd(5, 35) = 5$, so 5 has no inverse in Z_{35}.

• closure, Associativity, commutativity all hold but not all elements have inverse.

No, $\langle Z_{35}, \times \rangle$ is not a group, let alone an abelian one.

• $\langle Z_{37}, + \rangle$: yes, abelian group.

• $\langle Z_{35}, \times \rangle$: NO, not a group.

5. Let's take $p=2$ and $n=3$ that makes the $GF(p^n) = GF(2^3)$ then solve this with polynomial arithmetic approch.

Step-1

we want to construct $GF(2^3)$, a finite field with $2^3 = 8$ elements.

• Elements in $GF(2^3)$ are polynomials over $GF(2)$ of degree less than 3.

- $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$

Step-3:

$$f(x) = x^3 + x + 1$$

Step-3:

- $(x^2+x+1) + (x^2+1) = x$

Multiplication Example:

Let,

$$a(x) = x+1$$
$$b(x) = x^2+x$$

$$a(x) \cdot b(x) = (x+1)\cdot(x^2+x) = x^3 + x^2 + x^2 + x = x^3 + x$$

Step-2:

$$f(x) = x^3 + x + 1$$

Note:

$$x^3 \equiv x+1 \mod f(x) \Rightarrow x^3 + x \equiv (x+1) + x = 1$$

Result:

$$(x+1)(x^2+x) \equiv 1 \mod x^3 + x + 1$$