Q. 1: Prove Fermat's little theorem:

If p is a prime number and a is an integer such that $a \not\equiv 0 \pmod{p}$, then:

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof using modular arithmetic:

$S = \{1, 2, 3, \ldots, p-1\}$

multiply each element in S by a, where $a \not\equiv 0 \pmod{p}$.

$S' = \{a.1, a.2, a.3, \ldots, a.(p-1)\} \bmod p$

Thus,

$$a.1 \cdot a.2 \cdots a.(p-1) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$$

since $(p-1)! \not\equiv 0 \pmod{p}$

$$a^{p-1} \equiv 1 \pmod{p}$$

∴ Fermat's little theorem is proved.

Given,

$a = 7$

$p = 13$

13 is prime and $7 \not\equiv 0 \pmod{13}$

$7^{12} \equiv 1 \pmod{13}$

so, $7^{12} \bmod 13 = 1$

1. Efficient modular Exponentiation.

$c = m^e \bmod n$ and $m \equiv c^d \bmod n$

2. key insights for Euler's theorem.

$a^{\phi(n)} \equiv 1 \pmod{n}$

$\phi(n) = (p-1)(q-1)$

3. Primality testing:

$a^{p-1} \equiv 1 \pmod{p}$

Q.2: Euler's theorem statement:

compute $\phi(n)$ for $n = 35, 45, 100$.

If n is factored into distinct primes as

$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_n}\right)$$

$\phi(35)$

$35 = 5 \cdot 7$

$$\phi(35) = 35\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 35 \cdot \frac{4}{5} \cdot \frac{6}{7} = 24$$

$\phi(45)$

$45 = 3^2 \cdot 5$

$$\phi(45) = 45\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 45 \cdot \frac{2}{3} \cdot \frac{4}{5} = 24$$

$\phi(100)$

$100 = 2^2 \cdot 5^2$

$$\phi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

$\boxplus$ $a^{\phi(n)} \equiv 1 \bmod n$

This is known as Euler's theorem.

Proof:

- $a \in \mathbb{Z}$
- $\gcd(a, n) = 1$
- $R = \{r_1, r_2, \ldots, r_{\phi(n)}\}$

1. permutes the elements of R.

$$r_1 r_2 \cdots r_{\phi(n)} \equiv (ar_1)(ar_2)\cdots(ar_{\phi(n)}) \bmod n$$

$$r_1 r_2 \cdots r_{\phi(n)} \equiv a^{\phi(n)} \cdot r_1 r_2 \cdots r_{\phi(n)} \bmod n$$

$\therefore 1 \equiv a^{\phi(n)} \mod n$

Q.E.D

Q.3: Solve the system using the Chines. Remainder theorem.

$$\left.\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 4 \\ x &\equiv 1 \mod 5 \end{aligned}\right\}$$

$x \equiv 11 \mod 60 \quad \{N = 3 \cdot 4 \cdot 5 = 60\}$

Step-1:

- $n_1 = 3$
- $n_2 = 4$
- $n_3 = 5$

$N = n_1 n_2 n_3 = 60$

$N_i = \frac{N}{n_i}$

- $N_1 = \frac{60}{3} = 20$
- $N_2 = \frac{60}{4} = 15$
- $N_3 = \frac{60}{5} = 12$

$N_i m_i \equiv 1 \bmod n_i$

Step-2

$N_1 = 20 \bmod 3$:

$m_1 = 2$:

$20 \cdot 2 = 40 \equiv 1 \bmod 3$

$m_1 = 2$

$N_2 = 15 \bmod 4$:

$15 m_2 \equiv 1 \bmod 4$

$m_2 = 3$:

$15 \cdot 3 = 45 \equiv 1 \bmod 4$

$m_2 = 3$

$N_3 = 12 \bmod 5$:

$12 m_3 \equiv 1 \bmod 5$

$m_3 = 3$:

$12 \cdot 3 = 36 \equiv 1 \bmod 5$

$m_3 = 3$

Step-3:

$x \equiv a_1 N_1 m_1 + a_2 N_2 m_2 + a_3 N_3 m_3 \bmod N$

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

$561 = 3 \times 187 = 3 \times 11 \times 17$

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-2:

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

- $a=2$:
  $2^{560} \mod 561 = 1$
- $a=10$:
  $10^{560} \mod 561 = 1$
- $a=13$:
  $13^{560} \mod 561 = 1$

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:

$9 = 3^2$

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

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 so public key

Steps of the protocol:

1. Public parameters:
2. Private secrets.
3. Exchange.
4. shared secret computation.

Discrete Logarithm:

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

$g^a \equiv A \bmod p$

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: H E LL O W O R LD

ciphertext: K H O O R Z R U O G

Result: "KHOORZRUOG"

plaintext: HELLOWORLD

digraphs: HE LL OW OR LD

- HE → H (row 2, col 2), E (row 3, col 1) → CF
- LL → LX → L (4, 1) X (5, 4) → US
  L → with filler X → US
- 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: "CFUSUSNWMTR"

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

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

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

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