Data Security – Pre-Quiz

Questions

Q1. Compute the binary equivalent of 67? Verify your answer by applying the binary to decimal conversion technique.

Q2. Compute 19^{15} mod 26 using fast exponentiation with mod algorithm.

Q3. Compute the multiplicative inverse of 7 mod 19?

Solutions

Q1: To convert the decimal number 67 into binary using the division technique, you repeatedly divide the decimal number by 2 and record the remainders in reverse order. Here's the step-by-step process:

Divide 67 by 2: Quotient = 33, Remainder = 1

Divide 33 by 2: Quotient = 16, Remainder = 1

Divide 16 by 2: Quotient = 8, Remainder = 0

Divide 8 by 2: Quotient = 4, Remainder = 0

Divide 4 by 2: Quotient = 2, Remainder = 0

Divide 2 by 2: Quotient = 1, Remainder = 0

Divide 1 by 2: Quotient = 0, Remainder = 1

Now, write down the remainders in reverse order: 1000011. So, the binary representation of 67 is 1000011.

Verification: $1000011=1x2^6+0x2^5+0x2^4+0x2^3+0x2^2+1x2^1+1x2^0 =64+2+1=67$

Q2: 19^{15} mod 26= $19x19^{14}$ mod 26

$= 19 \text{ x } (19^2 \bmod 26)^7 \bmod 26$

$= 19 \text{ x } (23)^7 \bmod 26$

$= 19 \text{ x } 23 \text{ x } (23)^6 \bmod 26$

$= 19 \text{ x } 23 \text{ x } (23^2 \bmod 26)^3 \bmod 26$

$= 19 \text{ x } 23 \text{ x } (9)^3 \bmod 26$

$= 19 \text{ x } 23 \text{ x } (9^3 \bmod 26) \bmod 26$

$= 19 \text{ x } 23 \text{ x } 1 \bmod 26$

$= 21$

Q3: (7 * x) mod 19 = 1, We will search for x.

X = 1: 7 * 1 = 7 (mod 19), not equal to 1

X = 2: 7 * 2 = 14 (mod 19), not equal to 1

X = 3: 7 * 3 = 21 (mod 19), not equal to 1

X = 4: 7 * 4 = 28 (mod 19), not equal to 1

X = 5: 7 * 5 = 35 (mod 19), not equal to 1

X = 6: 7 * 6 = 42 (mod 19), not equal to 1

X = 7: 7 * 7 = 49 (mod 19), not equal to 1

X = 8: 7 * 8 = 49 (mod 19), not equal to 1

X = 9: 7 * 9 = 63 (mod 19), not equal to 1

X = 10: 7 * 10 = 70 (mod 19), not equal to 1

X = 11: 7 * 11 = 77 (mod 19), is equal to 1

Hence, 11 is the multiplicative inverse of 7 mod 19.