Cryptography

IT-24632

Md. Rafiqul Islam

Solution of a

$x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$

1. Start with first two congruences.

Let $x = 3a+1$. subsititute into the second congruence $3a+1 \equiv 2 \pmod 5$

$$\Rightarrow 3a \equiv 1 \pmod 5$$

The inverse of 3 module 5 is 2, so:

$$a \equiv 2 \pmod 5$$

$$\Rightarrow a = 5b+2$$

Then $x = 3(5b+2)+1 = 15b+7$

2. Now use third congruence

$$15b+7 \equiv 3 \pmod 7$$

Since $15 \equiv 1 \pmod 7$ & $7 \equiv 0 \pmod 7$ then simplifies to

$$b \equiv 3 \pmod 7 \Rightarrow b = 7c+3$$

Then $x = 15(7c+3)+7 = 105c+52$

$$x \equiv 52 \pmod{15} \Rightarrow 52 \text{ (Ans)}$$

IT- ~~17~~ 24631

Md. Rafiqul Islam

Solution of 6:

$x \equiv 5 \pmod{11}$, $x \equiv 14 \pmod{29}$, $x \equiv 15 \pmod{}$

1. Combine the first two congruence

$x = 11a + 5$ Substitute into the second congruence

$11a + 5 \equiv 14 \pmod{29}$

$11a \equiv 9 \pmod{29}$

The inverse of 11 modulo 29

That means we want $11x \equiv 1 \bmod 29$

$11 \cdot 8 = 1 \bmod 29$

So the inverse is 8, Multiply both sides:

$a = 9 \times 8 = 72 \equiv 14 \pmod{29}$

$a = 29b + 14$

Substitute back:

$x = 11(29b + 14) + 5 = 319b + 159$

So $x \equiv 159 \pmod{319}$

IT-17246.31

Md. Rafiqul Islam

2. Combine with third congruence

we have $319b + 159 \equiv 15 \pmod{31}$

$319 \equiv 9 \pmod{31}$ & $159 \equiv 4 \pmod{31}$

So: $9b + 4 \equiv 15 \pmod{31} \Rightarrow 9b \equiv 11 \pmod{31}$

Find the inverse of 9 modulo 31:

$9 \times 7 = 63 \equiv 1 \pmod{31}$

So the inverse is 7. Multiply both sides:

$b \equiv 11 \times 7 = 77 \equiv 15 \pmod{31} \Rightarrow b = 31c + 15$

Sub back $x = 319(31c + 15) + 159$

$= 9889c + 4944$

$\therefore x = 4944 \pmod{9889} \Rightarrow 4944$

Ans.