NAME :- KRUNAL RANK

ROLL NO :- U18CO081

CLASS :- BTECH 4TH YEAR

SEMESTER :- 7

DIVISION :- B

Cryptography and
Network Security
Tutorial 6

Ans 1: Given,

$x \equiv 2 \bmod 5$
$x \equiv 3 \bmod 7$
$x \equiv 10 \bmod 11$

Here, ~~gcd(5,7,11) = 1~~
pairwise gcd of (5,7) (7,11) and (7,11) is 1.

Let,

$x = P + Q + R$; P & R are divisible by 5
Q & R are divisible by 7
P & Q are divisible by 11.

Hence, let's represent x as:

$x = 77A + 55B + 35C$.

Now, $x \% 5 = 77A \% 5 \equiv 2 \% 5$

Hence, $77A \% 5 \equiv 2 \% 5$

let's find value of A by first finding $77A' \% 5 = 1$

A' is modular inverse of 77.

$77 \% 5 = 2$

Also, $3 \times 2 \% 5 = 6 \% 5 = 1$

Hence, $A' = 3$

Hence, We get $77 \times 3 = 231 \% 5 = 1$

Now, to get $77A \% 5 = 2$, we multiply 77 by 6.

Hence, $77 \times 6 = 462 \% 5 = 2$

Hence, first term is 462.

Hence, $x = 462 + 55B + 35C$.

$x \% 7 = ?$

Now, $= 55B \% 7 = 3 \% 7$

~~Mod inverse of 55 =~~

For $B=4$,

$55 \times 4 \% 7 = 220 \% 7 = 3$

55B = 6x

7 | 220 (3B)
21
10
-7
3

Hence, $x = 462 + 220 + 35C$

Now, $x \% 11 = 35C \% 11 = 10$

$35 \% 11 = 2$

For $C=5$

$35 \times 5 = 175 \% 11 = 10$

Hence,

$x = 462 + 220 + 350 = 1032$.

462
220
350
1032

However, $x = 1032 \pm$ ~~k~~ $k \times lcm(5,7,11)$ is also an answer.

Hence, correct answer is :-

$x = 1032 \% 385$

$x = 262 \% 385$

$lcm(5,7,11) = 385$

Ans

35
35
385

1032
-770
262

Ans 2:- Fermat's little theorem states that for any prime number p, any integer a,

$(a^p - a) \% p = 0$

Hence, $a^p = a \% p$

i) $2^{345} = 2^{11 \times 31 + 4}$

Hence, $2^{11 \times 31} \% 11 = 2 \% 11$

Hence, $2 \times 2^4 \% 11 = 32 \% 11 = 10$

ii) $60^{-1} \bmod 211$

~~Here, $60^{-1} \cdot 211 = 60$, 211 is prime as well.~~

~~Now, $60^{-1} = 60^{211-212} \quad 60^{209}$~~ ~~GCD(211, 60)~~

~~$60^{-1} \cdot 211 = 60^{209} \cdot 211$ =~~

$211 = GCD(211, 60) = 3 \times 60 + 31$

$60 = GCD(60, 31) = 31 \times 1 + 29$

$31 = GCD(31, 29) = 29 \times 1 + 2$

$29 = GCD(29, 2) = 2 \times 14 + 1$

Now, $1 = 29 - 14(2)$

$1 = 29 - 14(31 - 29)$ [Replacing $2 = 31 - 29$]

$1 = 29(15) - 14(31)$

$1 = 60(15) - 31(29)$ [Replacing $29 = 60 - 31$]

$1 = 60(15+87) - 211(87)$ [Replacing $31 = 211 - 60 \times 3$]

$\Rightarrow 1 = 60(102) - 211(87)$

Applying modulo 211 on both sides,

$1 \cdot \% 211 = (60 \times (102)) \cdot \% 211$.

Hence, $60^{-1} \cdot \% 211 = 102 \cdot \% 211$

Ans 3: $13^{18} \cdot \% 19$

$= (13^2)^{9} \cdot \% 19$ $\quad 169 \cdot \% 19 = 17$

$= 17^{9} \cdot \% 19$

$=$

Using Fermat's little theorem stating,

$a^{p-1} = 1 \bmod p$

When p is prime & $gcd(a, p) = 1$.

we get,

$13^{18} \% 19 = 1$.

Ans 4:- Given x^{86}, ~~$x^{86} = x^{87-1} = x^{3\times29-1}$~~

Using Fermat's little theorem,

$x^{29k} \,\%\, 29 = x$ for $k \in Z$.

Also, $x^{29k-1} \,\%\, 29 = 1$.

~~Hence, $x^{86} \,\%\, 29$~~

$x^{86} \,\%\, 29 = x^{2} \,\%\, 29$

for $x \in [0, 28] \cap Z$

Correct values of x are 21 & 8.

Hence, $x \equiv 21 \,\%\, 29$

$x \equiv 8 \,\%\, 29$.

Ans 5:- $\gcd(55, 22)$

$= \gcd(55 \% 22, 22) \cdot \gcd(22, 55 \% 22)$

$= \gcd(22, 11)$

$= \gcd(11, 0)$

$= 11$