Class Quiz 8

CMPSC 360

Kinner Parikh
April 13, 2022

Question 1:

1) $52^3 \cdot 10^4$
2) $26^2 \cdot 10^4$
3) $25 \cdot 26^2 \cdot 10^3$

Question 2: Find x if $x \equiv 2(\text{mod } 3); x \equiv 2(\text{mod } 4); x \equiv 1(\text{mod } 5)$ is the simultaneous system of linear congruence using Chinese remainder theorem.

$x \equiv 2 \pmod 3$
$x \equiv 2 \pmod 4$
$x \equiv 1 \pmod 5$
Applying Chinese Remainder Theorem:
$a_1 = 2, a_2 = 2, a_3 = 1$ and $m_1 = 3, m_2 = 4, m_3 = 5$
So, $M = 3 \cdot 4 \cdot 5 = 60$
Thus, $z_1 = 20, z_2 = 15, z_3 = 12$
$y_1 \cdot 20 = 1 \bmod 3$; so $y_1 = 2$
$y_2 \cdot 15 = 1 \bmod 4$; so $y_2 = 3$
$y_3 \cdot 12 = 1 \bmod 5$; so $y_3 = 3$
We get $x = (2 \cdot 20 \cdot 2) + (2 \cdot 15 \cdot 3) + (1 \cdot 12 \cdot 3) = 206$
And $206 \bmod 60 = 26$
Thus, the lowest possible simultaneous solution is $x = 26$

Question 3:

Bob wants to set up an RSA key pair. He first chooses $p = 29$ and $q = 31$. Then, $n = 899$
Also, Bob chooses a valid e from $\{3356, 3357, 3358, 3359\}$ for encryption. $e = 3359$
Then, Bob encrypts two 3-digits decimal numbers 072, 073 into $m = 462, 234$
Alice's pair of key to decrypt $(n, d) = (n, 839)$