MAT 373 Homework 13

Justyce Countryman

April 19, 2024

Problem 1: Encrypt the plaintext message GOLD MEDAL using the RSA algorithm with key (2561, 3)

(2561, 3) $= (n, k) = (m, e)$
Converting GOLD MEDAL into numerical values using the alpha-numeric scheme gives us:

061411032612040300011

The encryption process is then the following (using blocks of length 2):
$(06)^3 \equiv 0216 \pmod{2561}$
$(14)^3 \equiv 0183 \pmod{2561}$
$(11)^3 \equiv 1331 \pmod{2561}$
$(03)^3 \equiv 0027 \pmod{2561}$
$(26)^3 \equiv 2210 \pmod{2561}$
$(12)^3 \equiv 1728 \pmod{2561}$
$(04)^3 \equiv 0064 \pmod{2561}$
$(03)^3 \equiv 0027 \pmod{2561}$
$(00)^3 \equiv 0000 \pmod{2561}$
$(11)^3 \equiv 1331 \pmod{2561}$

Therefore, our encrypted ciphertext message comes out to be:

0216 0183 1331 0027 2210 1728 0064 0027 0000 1331

Problem 2: The ciphertext message produced by the RSA algorithm with key $(n, k) = (2573, 1013)$ is

0464 1472 0636 1262 2111

Determine the original message

$(n, k) = (m, e) = (2573, 1013)$
$1013d \equiv 1 \pmod{\phi(2573)}$

$\phi(2573) = \phi(31^1 \cdot 83^1) = (31 - 1)(83 - 1) = 2460$

$1013d \equiv 1 \pmod{2460}$

We can use the Euclidean algorithm with $gcd(1013, 2460) = 1$. Applying the Euclidean algorithm eventually gets us to:
$1 = 1013(17) + 2460(-7)$

This tells us that $1013(17) \equiv 1 \pmod{2460}$ and the multiplicative inverse of 1013 (mod 2460) is $2460(2) - (2460 + 17) = 2443$.

We can then say:
$1013d(2443) \equiv 1(2443) \pmod{2460}$
$2474759d \equiv 2443 \pmod{2460}$
$2474759d - 2474760d \equiv 2443 \pmod{2460}$
$-d \equiv 2443 \pmod{2460}$
$d \equiv -2443 \pmod{2460}$

$$\boxed{d \equiv 17 \pmod{2460}}$$

Let $d = 17$, and we can now perform decryption:
$(0464)^{17} \equiv 1704 \pmod{2573}$
$(1472)^{17} \equiv 1511 \pmod{2573}$
$(0636)^{17} \equiv 2426 \pmod{2573}$
$(1262)^{17} \equiv 1314 \pmod{2573}$
$(2111)^{17} \equiv 2223 \pmod{2573}$

Finally, using the alpha-numeric scheme, we can take:
17041511242613142223
and get the original message:
REPLY NOWX

Problem 3: Decrypt the ciphertext

1030 1511 0744 1237 1719

that was encrypted using the RSA algorithm with key $(n, k) = (2623, 869)$. [Hint: The recovery exponent is $j = 29$]
$(n, k) = (m, e) = (2623, 869)$
$869d \equiv 1 \pmod{\phi(2623)}$

$\phi(2623) = \phi(43^1 \cdot 61^1) = (43 - 1)(61 - 1) = 2520$

$869d \equiv 1 \pmod{2520}$

We can use the Euclidean algorithm with $gcd(869, 2520) = 1$. Applying the Euclidean algorithm eventually gets us to:
$1 = 869(29) - 2520(10)$

This tells us that $869(29) \equiv 1 \pmod{2520}$ and the multiplicative inverse of 869 (mod 2520) is $2520(2) - (2520 + 29) = 2491$.

We can then say:
$869d(2491) \equiv 1(2491) \pmod{2520}$
$2164679d \equiv 2491 \pmod{2520}$
$2164679d - 2164680d \equiv 2491 \pmod{2520}$
$-d \equiv 2491 \pmod{2520}$
$d \equiv -2491 \pmod{2520}$

$d \equiv 29 \pmod{2520}$

Let $d = 29$, and we can now perform decryption:
$(1030)^{29} \equiv 1804 \pmod{2623}$
$(1511)^{29} \equiv 1111 \pmod{2623}$
$(0744)^{29} \equiv 2618 \pmod{2623}$
$(1237)^{29} \equiv 0714 \pmod{2623}$
$(1719)^{29} \equiv 1719 \pmod{2623}$

Finally, using the alpha-numeric scheme, we can take:
18041111261807141719
and get the original message:
SELL SHORT