9

3.1

Solve $x^{73} = 714 \pmod{1159}$

✓ **Answer**

$1159 = 19 \times 61$

$x = 11 \pmod{19}$

$x^{13} = 43 \pmod{61}$

$13^{-1} \pmod{60}$

Total	a	b
60	1	0
13	0	1
8	1	-4
5	-1	5
3	2	-9
2	-3	14
1	5	-23=37

$x = 43^{37} \pmod{61}$

$x = 59 \pmod{61}$

$x = 11 \pmod{19}$

$x = 59 \pmod{61}$

$x = 11 + 19k$

$11 + 19k = 59 \pmod{61}$

$19k = 48 \pmod{61}$

Total	a	b
61	1	0
19	0	1
4	1	-3

Total	a	b
3	-4	13
1	5	-16=45

$19^{-1} = 45 \pmod{61}$
$k = 25 \pmod{61}$

$x = 11 + 19(25 + 61m) \pmod{1159}$
$x = 486 \pmod{1159}$
□

3.7

Alice has RSA public key $N = 2038667$ and exponent $e = 103$.

a

Bob wants to send Alice the message $m = 892383$ What ciphertext does Bob send to Alice?

✓ Answer
$c = m^e \pmod{N}$
$c = 45293 \pmod{N}$

b

Alice knows that her modulus factors into a product of two primes, one of which is 1301 Find a decryption exponent d for Alice.

✓ Answer
$N = 1301 \times 1567$
$\phi(N) = 1300 \times 1566 = 2035800$
$d = e^{-1} \pmod{2035800}$
$d = 810367$

c

Alice receives the ciphertext 317730 from Bob. Decrypt the message.

✓ Answer

$m = c^d \pmod{N}$

$m = 514407$