1) In an RSA system, n = 391 and e = 137, what is d?

We need to solve for d in the equation 137d = 1 mod 352.

So, we must run the Extended Euclidean Algorithm:

\[ 352 = 2 \times 137 + 78 \]
\[ 137 = 1 \times 78 + 59 \]
\[ 78 = 1 \times 59 + 19 \]
\[ 59 = 3 \times 19 + 2 \]
\[ 19 = 9 \times 2 + 1 \]
\[ 2 = 2 \times 1 \]

Now, we have:

\[ 19 - 9 \times 2 = 1 \]
\[ 19 - 9 \times (59 - 3 \times 19) = 1 \]
\[ 19 - 9 \times 59 + 27 \times 19 = 1 \]
\[ 28 \times 19 - 9 \times 59 = 1 \]
\[ 28 \times (78 - 59) - 9 \times 59 = 1 \]
\[ 28 \times 78 - 28 \times 59 - 9 \times 59 = 1 \]
\[ 28 \times 78 - 37 \times 59 = 1 \]
\[ 28 \times 78 - 37 \times (137 - 78) = 1 \]
\[ 28 \times 78 - 37 \times 137 + 37 \times 78 = 1 \]
\[ 65 \times 78 - 37 \times 137 = 1 \]
\[ 65 \times (352 - 2 \times 137) - 37 \times 137 = 1 \]
\[ 65 \times 352 - 130 \times 137 - 37 \times 137 = 1 \]
\[ 65 \times 352 - 167 \times 137 = 1 \]

Thus \( d = -167 = (352 - 167) = 185 \mod 352. \)

\( d = 185 \)

2) In a Diffie-Hellman Key Exchange, Alice and Bob agree upon the public keys \( p = 17 \) and \( g = 3 \). Alice picks the secret key \( a = 4 \) and Bob picks the secret key \( b = 7 \). What value does Alice send Bob? What value does Bob send Alice? What is their shared secret key?

Alice sends Bob \( 3^4 \mod 17 = 81 \mod 17 = 13 \).
Bob sends Alice \( 3^7 \mod 17 = (27)(27)(3) \mod 17 = (10)(10)(3) \mod 17 = 11 \).

Their shared key (calculated by Alice) is \( 11^4 \mod 17 = (121)(121) \mod 17 = 4 \mod 17 \), since \( 121 = 2 \mod 17 \).
3) Consider the Elliptic Curve $\mathbb{E}_{29}(3, 11)$. Let $p$ be the point $(8, 5)$ on this curve and $q$ be the point $(20, 26)$ on this curve. Determine $P + Q$.

$$
\lambda = \frac{y_q - y_p}{x_q - x_p} = \frac{26 - 5}{20 - 8} \mod 29 = 21 \times 12^{-1} \mod 29
$$

We must find $12^{-1} \mod 29$:

$$
29 = 2 \times 12 + 5 \\
12 = 2 \times 5 + 2 \\
5 = 2 \times 2 + 1 \\
5 - 2 \times 2 = 1 \\
5 - 2(12 - 2 \times 5) = 1 \\
5 \times 5 - 2 \times 12 = 1 \\
5(29 - 2 \times 12) - 2 \times 12 = 1 \\
5 \times 29 - 12 \times 12 = 1 \\
12^{-1} \equiv -12 \equiv 17 \mod 29
$$

Thus, $\lambda = 21 \times 12^{-1} \equiv 21 \times 17 \equiv 357 \equiv 9 \mod 29$.

$$
x = \lambda^2 - x_p - x_q \equiv 9^2 - 8 - 20 \equiv 53 \equiv 24 \mod 29 \\
y = (\lambda(x_p - x) - y_p) \equiv (9(8 - 24) - 5) \equiv (9 \times 13 - 5) \equiv 112 \equiv 25 \mod 29
$$

Thus, the desired sum is the point $(24, 25)$.

4) Consider the Elliptic Curve $\mathbb{E}_{29}(3, 11)$. Let $P$ be the point $(8, 5)$ on this curve. Determine $2P$.

$$
\lambda = \frac{3x_p^2 + a}{2y_p} = \frac{3(8)^2 + 3}{2(5)} = \frac{195}{10} \equiv \frac{21}{10} \mod 29 = 21 \times 10^{-1} \mod 29
$$

To save some work, we can eyeball that $10^{-1} \equiv 3 \mod 29$, since $3 \times 10 = 30$ and $30 \equiv 1 \mod 29$.

Thus, we have $\lambda = 21 \times 3 \equiv 63 \equiv 5 \mod 29$

Now, we can solve for $x$ and $y$:

$$
x = \lambda^2 - 2x_p \equiv 5^2 - 2(8) \equiv 9 \mod 29 \\
y = (\lambda(x_p - x) - y_p) \equiv (5(8 - 9) - 5) \equiv -10 \equiv 19 \mod 29
$$

Thus, the desired sum is the point $(9, 19)$. 


5) Alice's Public El Gamal keys are $q = 31$, and $\alpha = 11$. Alice's secret key $X_A = 9$. Bob has sent a message to Alice. The ciphertext he has sent to Alice is $C_1 = 3$, $C_2 = 18$. What is the plaintext?

Solution

$K = (C_1)^{X_A} \mod q \equiv 3^9 \equiv (3^3)^3 \equiv (27)^3 \equiv (-4)^3 \equiv -64 \equiv 29 \mod 31$

$M = (C_2K^{-1}) \mod q$

Thus, we need to find $29^{-1} \mod 31$.

\[
\begin{align*}
31 &= 1 \times 29 + 2 \\
29 &= 14 \times 2 + 1 \\
29 - 14 \times 2 &= 1 \\
29 - 14(31 - 29) &= 1 \\
29 - 14 \times 31 + 14 \times 29 &= 1 \\
15 \times 29 - 14 \times 31 &= 1 \\
\text{Thus, } 29^{-1} &\equiv 15 \mod 31
\end{align*}
\]

$M = (18 \times 15) \equiv 270 \equiv 22 \mod 31$