Ans 9

$q = 157$, $x = 5$

$Y = 10$

$g = 3$, $M = 9$

$10 = 3^d \bmod 157$ d = private key

and

$(5, 10, 157)$ = public keys

$C_1 = 3^3 \bmod 157 = 125$

$C_2 = 9 \times 10^3 \bmod 157 = 51$

hence cipher text of $M = 9$, $(125, 51)$

(b) k = unknown

cipher $(9) = (25, C_2)$

$C_1 = 25 \rightarrow 3^k \bmod 157 \rightarrow 25$

$k = 2$

$C_2 = P \times 10^k \bmod 157 \rightarrow 900 \bmod 157$

$\rightarrow 115$

$C_2 \rightarrow 115$

Q: 2

$P = (1, 0)$

$Q = (1.5, 1.5)$

for $P + Q$

$$S = (y_P - y_Q) / (x_P - x_Q)$$

$$\rightarrow (0 - 1.5) / (1 - 1.5)$$

$$\rightarrow \frac{-1.5}{-0.5} \rightarrow 3$$

$$x_R = S^2 - x_P - x_Q$$

$$\rightarrow 9 - 1 - 1.5 \rightarrow 6.5$$

and $y_R \rightarrow -y_P + S(x_P - x_R)$

$$\rightarrow 0 + 3(1 - 6.5)$$

$$\rightarrow 3 \times (-5.5) = -16.5$$

$$(P+Q) = (6.5, -16.5)$$

now, $S = (3x_P^2 + a) / 2y_P$

$$\rightarrow \frac{\left(3 + \left(\frac{-17}{12}\right)\right)}{2 \times 0} \rightarrow \frac{\text{finite}}{0} = \text{not defined}$$

Qn: 5 we are given the following values

$a^b \% n$

So; $a = 6$, $b = 472$ & $n = 3415$

let's convert 6 to binary 11011000

a	b	result
6	11011000	1
36	1101100	1
1296	110110	1
2851	11011	2851
501	1101	2851
1706	110	881
856	11	881
1926	1	2836
786	0	1551
3096		3348

Hence $a^b \% n$ = 3348

result is

Q:-3 a) Diffy Hellman key exchange

we are given that

$g = 23$ and $p = 5$

for the Alice $a = 8$.

Bob $b = ?$

for given value $a = 8$

let find

$= g^a \bmod p \Rightarrow 23^8 \% 5 = 1$

and let us assume

$\rightarrow b = 7$ and (Hit and trial method)

$Y = g^b \bmod p \Rightarrow 23^7 \% 5 = 2$

$Key_a \Rightarrow Y^a \bmod p \Rightarrow 2^8 \bmod 5 = 1$

$Key_b = X^b \bmod p \Rightarrow 1^7 \bmod 5 = 1$

(b) r is a primitive root iff

$5^n \bmod \{ n \in \{1 - \ldots - p-1\} \}$ generates the numbers $\{1, 2, 3, \ldots - p-1\}$

for $x = 1$, $5 \% 23 = 5$

$x = 2$ $25 \% 23 = 2$

$x = 3$ $125 \% 23 = 10$

Thus for

$x \leq 22$

and $x \geq 4$

We can say that 5 is a primitive root

Qn-6 In any public key system using RSA, we interpret the ciphertext $C = 20$, where $e = 3$, and $n = 77$

Eg. $f(N) = f(77) = 60$

The relative no. of primes corresponding to $f(n)$ such that p_i where $p_i < 60$

→ 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49 and 53, 59

we are given $e = 13$

so; $d = e^{-1} \bmod f(N)$

and $d = 13^{-1} \bmod (60)$

$d = 37$

for the given ciphertext $C = 20$

$M = C^d \bmod N$

→ $20^{37} \% 77$ → 48

Hence; the plaintext msg is $M = 48$