CIS 3362 - 11/10/21

Quiz Topics

Diffie-Hellman Key Exchange

RSA

El-Gamal Cryptosystem

Elliptic Curves
- Addition P+Q
- Addition P+P

EC Cryptography

Use
2 sheets of notes
Calculator

Question 1

1) Prime factorize $n = 17 \times 23$
2) $\phi(n) = 16 \times 22 = 352$
3) EEA $137^{-1} \bmod 352$

Question 2

$A \to B \quad g^a \bmod p \quad 3^4 \bmod 17 \to 13$

$B \to A \quad g^b \bmod p \quad 3^7 \bmod 17 \to 11$

Shared 13^7 or $11^4 \bmod 17 \to 4$

Question 3

$\lambda = \frac{y_q - y_p}{x_q - x_p} \bmod P$, Don't forget mod inverse $\lambda = 9$

$(y_q - y_p) \times (x_q - x_p)^{-1} \bmod P$

$x = (\lambda^2 - x_p - x_q) \bmod P \to 24$

$y = \lambda(x_p - x) - y_p \bmod P \to 25$

Question 4

$$\lambda = \frac{3x_p^2 + a}{2y_p} \bmod p \qquad \lambda = 5$$

$$(3x_p^2 + a)(2y_p)^{-1} \bmod p$$

$$x = \lambda^2 - 2x_p \bmod p \longrightarrow x = 9$$

$$y = (\lambda(x_p - x) - y_p) \bmod p \rightarrow y = 19$$

Question 5

$$K = (C_1)^{X_A} \bmod q \longrightarrow 29 \quad (-2)$$

$$K^{-1} \bmod q \longrightarrow 15$$

$$m = C_2 K^{-1} \bmod q \longrightarrow \boxed{22}$$