Giới thiệu một số hệ mật KCK

- **Bài tập:**
  - 1) Cho $E_{17}(1,1)$; G = (0,1)
    - Khóa riêng của A, B lần lượt là: $n_A = 3$; $n_B = 4$. Tính KCK của A, B.
    - Giả sử người A cần gửi tin cho B, hãy mô phỏng quá trình mã hóa bản tin P_M = (10,12) và giải mã bản mã thu được. Cho trước giá trị ngẫu nhiên k = 2.
  - 2) Cho $E_{11}(1, 6)$; G = (2,7)
    - Khóa riêng của B $n_B = 7$. Tính KCK của B.
    - Giả sử người A cần gửi tin cho B, hãy mô phỏng quá trình mã hóa bản tin P_M = (10, 9) và giải mã bản mã thu được. Cho trước giá trị ngẫu nhiên k = 3.

Giới thiệu một số hệ mật KCK

- **Giải:**
  - Tính khóa công khai của A & B: $P_A = n_A.G = 3G$; $P_B = n_B.G = 4G$
  - $P_A = n_A.G = 3G = 2G + G$
    - $2G = (0, 1) + (0, 1) = (x_3, y_3)$
      - $\lambda = \frac{3.x_1^2+1}{2y_1} = \frac{3.0^2+1}{2} = 1.2^{-1} mod\ 17 = 9$
      - $x_3 = \lambda^2 - x_1 - x_2 = 9^2 - 0 - 0 = 13$; $y_3 = \lambda(x_1 - x_3) - y_1 = 9.(0 - 13) - 1 = -118 \bmod 17 = 1$
      - Vậy **2G = (13, 1)**
    - Tính $3G = 2G + G = (13, 1) + (0, 1) = (x_3, y_3)$
      - $\lambda = \frac{y_2-y_1}{x_2-x_1} = \frac{1-1}{0-13} = 0$
      - $x_3 = \lambda^2 - x_1 - x_2 = 0^2 - 13 - 0 = 4$; $y_3 = \lambda(x_1 - x_3) - y_1 = 0.(13 - 4) - 1 = -1 \bmod 17 = 16$
      - Vậy **3G = (4, 16)**

Giới thiệu một số hệ mật KCK

- Tính $P_B = 4G = 3G + G$ (hoặc $2G + 2G$)
  - $3G + G = (4, 16) + (0, 1) = (x_3, y_3)$
    - $\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{1 - 16}{0 - 4} = 15.4^{-1} mod\ 17 = 15.13\ mod\ 17 = 8$
    - $x_3 = \lambda^2 - x_1 - x_2 = 8^2 - 4 - 0 = 9$; $y_3 = \lambda(x_1 - x_3) - y_1 = 8.(4 - 9) - 16 = -5 \bmod 17 = 12$
    - Vậy **4G = (9, 12)**
- A gửi P_M cho B $\Rightarrow$ A lấy khóa công khai của B để mã hóa, với k = 2.

  Ta có $P_C = [kG, P_M + 2P_B] = [(13, 1); ((10,12) + 2(9,12))]$

Giới thiệu một số hệ mật KCK

- Tính 2(9, 12) = (9, 12) + (9, 12) = (x_3, y_3)
  - $\lambda = \frac{3.x_1^2+1}{2y_1} = \frac{3.9^2+1}{2.12} = 122.12^{-1} mod\ 17 = 122.10\ mod\ 17 = 13$
  - $x_3 = \lambda^2 - x_1 - x_2 = 13^2 - 9 - 9 = 15$; $y_3 = \lambda(x_1 - x_3) - y_1 = 13.(9 - 15) - 12 = -5 \bmod 17 = 1$
  - Vậy **2(9, 12) = (15, 12)**
- Tính (10, 12) + (15, 12) = (x_3, y_3)
  - $\lambda = \frac{y_2-y_1}{x_2-x_1} = \frac{12-12}{15-10} = 0$
  - $x_3 = \lambda^2 - x_1 - x_2 = 0^2 - 10 - 15 = 9$; $y_3 = \lambda(x_1 - x_3) - y_1 = 0.(10 - 9) - 12 = 5$
  - Vậy **(10, 12) + (15, 12) = (9, 5)**
- Ta có: $P_C = [kG, P_M + 2P_B] = [(13, 1); (9, 5)]$

Giới thiệu một số hệ mật KCK

- Giải mã: $P_C = [(13, 1); (9, 5)] = [P_1, P_2]$
  - B dùng khóa riêng n_B của mình để tính $P_M = P_2 – n_B P_1 = (9, 5) – 4(13, 1)$
  - Tính $4(13, 1) = 2(13, 1) + 2(13, 1) = (15, 12)$ vì
    - $2(13, 1) = 2.2G = 4G = (9, 12)$
    - $2(13, 1) + 2(13, 1) = 2(9, 12) = (15, 12)$
  - Tính $P_M = (9, 5)$ **$– (15, 12)$** $= (9, 5)$ **$+ (15, -12)$** $= (9, 5) + (15, 5)$
    - $\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{5 - 5}{15 - 9} = 0$
    - $x_3 = \lambda^2 – x_1 – x_2 = 0^2 – 9 – 15 = 10$; $y_3 = \lambda(x_1 – x_3) – y_1 = 0.(9 – 10) – 5 = 12$
    - Vậy **$P_M = (10, 12)$**