Cryptographic Protocols

Session 6 - Paillier Cryptosystem

1. Implement Paillier cryptosystem and try the following

(a) Generate necessary parameters, and keep them for the rest of the practice.

(b) Calculate $A = \text{encryption of } a$, and $B = \text{encryption of } b \ (a = 28, b = 2)$.

(c) Calculate $A/B, A^3/B^2, A^2/B^3$, and decrypt each result. What is the result as a function of $a$ and $b$?

(d) If you did not know $a$ and $b$, can you get an encryption of $(3a - b)$ and $(3ab)$?

(e) From the above, implement a function that gets two ciphertexts $\text{Enc}(a), \text{Enc}(b)$ together with integers $x, y$ and returns $\text{Enc}(ax + by)$. 