ELGAMAL CRYPTOSYSTEM

ElGamal encryption is a public-key cryptosystem. It uses asymmetric key encryption for communicating between two parties and encrypting the message.
This cryptosystem is based on the difficulty of finding **discrete logarithm** in a cyclic group that is even if we know g^a and g^k, it is extremely difficult to compute g^{ak}.

Idea of ElGamal cryptosystem

Suppose Alice wants to communicate with Bob.

1. Bob generates public and private keys:
   - Bob chooses a very large number **q** and a cyclic group $\mathbf{F}_q$.
   - From the cyclic group $\mathbf{F}_q$, he choose any element **g** and an element **a** such that gcd(a, q) = 1.
   - Then he computes $h = g^a$.
   - Bob publishes **F**, $\mathbf{h = g^a}$, **q**, and **g** as his public key and retains **a** as private key.
2. Alice encrypts data using Bob's public key :
   - Alice selects an element **k** from cyclic group **F** such that gcd(k, q) = 1.
   - Then she computes $p = g^k$ and $s = h^k = g^{ak}$.
   - She multiples s with M.
   - Then she sends $(p, M*s) = (g^k, M*s)$.
3. Bob decrypts the message :
   - Bob calculates $s' = p^a = g^{ak}$.
   - He divides M*s by s' to obtain M as $s = s'$.

Example: Alice chooses $p_A = 107$, $\alpha_A = 2$, $d_A = 67$, and she computes $\beta_A = 2^{67} \equiv 94 \pmod{107}$. Her public key is $(p_A, \alpha_A, \beta_A) = (2,67,94)$, and her private key is $d_A = 67$.

Bob wants to send the message "B" (66 in ASCII) to Alice. He chooses a random integer $k = 45$ and encrypts M = 66 as $(r, t) = (\alpha_A{}^k, \beta_A{}^k M) \equiv (2^{45}, 94^{45}66) \equiv \mathbf{(28, 9)} \pmod{107}$. He sends the encrypted message (28, 9) to Alice.

Alice receives the message $(r, t) = (28, 9)$, and using her private key $d_A = 67$ she decrypts to

$$t r^{-d_A} = 9 \cdot 28^{-67} \equiv 9 \cdot 28^{106-67} \equiv 9 \cdot 43 \equiv \mathbf{66} \pmod{107}.$$