ELGAMAL ENCRYPTION SCHEME
SETUP: **1.p is a prime.** **2. *g* is an element of prime order *q* in F_p** **3. The group used is $\{g^0 g^1 g^2, ..., g^{q-1}\}$.**
KEY GENERATION: **1. Select a random integer *x* in the interval *[2,q-2].* 2. Compute $y=g^x \bmod p$.** **3. The private key is *x*.** **4. The public key is *y*.**
ENCRYPTION: **1. Represent the message M as an integer *m* in the interval [2,p-2].** ***2.* Select a random integer *k* in the interval [2,q-2].** **3. Compute $g^k \bmod p$.** **4. Compute $y^k \bmod p$.** **5. Compute ciphertext $c=m*y^k \bmod p$.** **6. *Transmit($g^k \bmod p$, c).***
DECRYPTION: **1. Compute $y^k=(g^k)^x \bmod p$.** **2. Compute $m=c*(y^k)^{-1} \bmod p$.**