Elgammal cryptosystem. Ns assignment-4
-by Aaron agnel (2017010) and Bharath Kumar (2017035)

Scenario:
We have two subjects, Alice (A) and Bob (B). B wants to send a message to A and the question requires us to encrypt the communication using elgammal cryptography. Before that we need to use diffie-hellman key exchange protocol to establish the one time keys and to ensure integrity we have to maintain a mac for each key exchange and the shared secret of the hmac must be communicated securely.

Hmac secret sharing:
For this we maintain a public and private key pair for each individual. B then sends a request to A by first encrypting the request with his private key then he adds his identifier to the request and then he encrypts the entire message using A's public key (the public is assumed to be known and verified). So now A decrypts this message using her private key first gets the identifier of B and then uses his public key to decrypt the request. The request then consists of the shared secret which B wants to use. If A agrees then it uses it else it sends a new secret to B. That is the return request is either a OK or a new secret for B. The return request is similarly encrypted first with A's private key and then with B's public key. After this step both A and B agree upon the hmac secret.

1) $\{\{secret:xxx\}|B_{priv} | B_{id}\}|A_{pub}$
2) $\{\{secret:xxx\}|A_{priv} | A_{id}\}|B_{pub}$

Diffie-hellman key exchange and encryption:
In this step, Bob and Alice have pre determined public parameters (q,a) where q is a large prime and a being a primitive root modulo q. Then A choses h1<=q-1 and does a^h1 mod q and sends it to B as K. B then choses h2<=q-1 and does a^h2 mod q and stores it as C1. Then it takes the message to send character by character and then encrypts each of

them as M(K^h2) mod q , where M is the character and stores it as C2. The message is then sent as C1,C2 and is sent to A. A then uses C1^h1 and stores it as s to get the key and then finds s^-1 and multiplies it with C2 to get M. When a ‘\n’ is detected A understands that a word is completed and stops receiving further characters.