ÖDEV 2

S1) RSA şifreleme algoritmasında p = **19** ve q = **11** değeri için kendi belirleyeceğiniz $\emptyset(n)$ ile aralarında asal olacak şekilde rastgele *e* değeri seçiniz. Bu değerlere göre açık anahtar ve gizli anahtar değerlerini adım adım göstererek değerleri bulunuz.

S2) Diffie - Hellman Şifreleme Algoritmasında p=**25** ve g= **11** için A ve B kullanıcıları için rastgele birer tane gizli anahtarlar seçiniz. Bu değerlere göre ortak K gizli anahtarını adım adım göstererek değeri bulunuz.

S3) ElGamal Şifreleme Sistemine göre p=**23** ve g= **11** için gizli anahtar değeri olan *a* rastgele seçiniz *ve* mesaj değeri m = **10** olarak alınız. Bu değerlere göre şifreli mesajlar olan C ve D değerlerini hesaplayınız ardından adım adım C ve D değerlerine göre orijinal mesajı tekrar elde ediniz.

Not: Bu ödev puanı 15 puandır. İlk ödev 25 puandır. Vize sınavı da 60 puan üzerinden değerlendirilecektir.