# **DETYRË PROJEKTI**

1. Duke përdorur kriptosistemin RSA të kryhen:
2. Le të jenë n=253 dhe e=31 çelës publik. Enkripto m=10, dhe gjej p, q dhe d. Pastaj dekripto c=35?
3. Le të jenë p=67, q=73 dhe e=89. Enkripto tekstin SIGURI me gjatësi të bllokut 2?
4. Zgjidhje:
5. 













































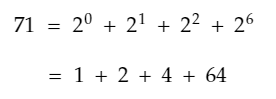


































Shumëzohen dy nga dy





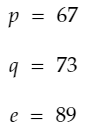




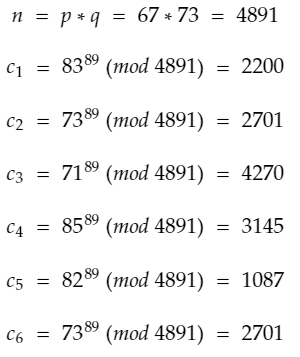






1. 





Teksti i enkriptuar është 2200 2701 4270 3145 1087 2701.

1. Detyra e dytë është implementuar në klasë RSA\_Attack.
2. Detyra e tretë është implementuar në klasën Simplified\_SHA\_1.