۱. آلیس تصمیم می گیرد از رمزنگاری RSA برای رمز متن خود استفاده کند و بدین ترتیب آلیس دو عدد اول بزرگ p و q را انتخاب و N = pq را محاسبه می کند. او همچنین کلید رمز نگاری (کلید عمومی) eA = ۳ و کلید خصوصی را dA انتخاب می کند. وقتی دوستش باب این موضوع را می شنود، او نیز می خواهد از رمزنگاری RSA استفاده کند. بدین ترتیب آلیس با انتخاب eB = ۵ و محاسبه کلید خصوصی dB با استفاده از همان N به باب کمک می کند. بدین ترتیب آلیس کلیدهای (N, eB) و dB را به باب می دهد. روز بعد دوست مشترک آنها چارلی با استفاده از کلیدهای مربوطه به آلیس و باب پیام m را به صورت رمز شده برای آن ها ارسال می کند. با این حال، دشمن دبورا دو متن رمزی cA و cB را شنود کرده و به آن دست می یابد. دبورا همچنین متوجه می شود که آلیس و باب از یک N استفاده می کنند. نشان دهید که دبورا چگونه می تواند m را بازیابی کند. فرض کنید که gcd(m, N) = ۱ است.

۱-۲. آیا حمله دبورا به طور کلی و برای مقادیر دیگری به جز eA و eB بالا, تعمیم می یابد؟

۲. تمرینات زیر از کتاب درسی را حل کنید.

شماره تمرینات فصل ۷: ۱-۵-

۳. با استفاده از الگوریتم اقلیدس معکوس عدد زیر را در Z_m محاسبه کنید.

- $a = 19\ ,\ m = 999$

۴. **(به یکی از دو سوال ۴ و ۵ به اختیار پاسخ دهید)** می‌خواهیم یک پیام رمزشده با رمز RSA را رمزگشایی کنیم. متن رمز شده برابر با 1141 و کلید عمومی برابر با (2623, 2111) است. ($y = 1141, k_{pub} = (n, e) = (2623, 2111)$)

۴-۱. کلید خصوصی و مقادیر p و q را بیابید. آیا می‌توان بدون تجزیه‌کردن n مقدار کلید خصوصی را بدست آورد؟

۴-۲. مقدار پیام اصلی را بدست آورید.

۵. . **(به یکی از دو سوال ۴ و ۵ به اختیار پاسخ دهید)** اگر p عدد اول باشد و a یک عدد صحیح مثبت باشد, ثابت کنید.

$$\emptyset(p^a) = p^a - p^{a-1}$$

۶. در یک رمز RSA ، مقادیر p برابر با 31 ، q برابر با 37 و کلید عمومی برابر با 17 می‌باشد. اگر متن رمزشده برابر با 2 باشد، با استفاده از قضیه باقی‌مانده چینی آن را رمزگشایی کنید. ($p = 31, q = 37, e = 17, y = 2$)