دانشگاه صنعتی شریف تمرین سری اول مبانی رمزنگاری و امنیت شبکه تحویل: چهارشنبه ۱۳۹۸/۱۲/۲۸ نحوه تحویل: پاسخ تمرینها (تئوری و کامپیوتری) میبایست در CW آپلود شوند.

۱. مساله 1.6 از کتاب مرجع اصلی درس (Stallings, 7th Edition)

۲. پاسخ (های) معادلات همنهشتی زیر را بیابید.

 $7x \equiv 5 \mod 3$  (الف

 $15x \equiv 10 \mod 25 \quad (\bigcirc$ 

 $3x \equiv 7 \mod 12$  ( \_\_\_

۳. ثابت کنید اگر  $a^n \equiv a^{n'} \mod m$  و  $\gcd(a,m) = 1$  باشند، در این صورت  $a^n \equiv a^{n'} \mod m$  خواهد بود. با استفاده از آن، حاصل عبارت 7 2000000 را بيابيد.

(Stallings, 7th Edition) درس (عدال مرجع اصلى درس (عدال كتاب مرجع اصلى درس (الكتاب عدال كتاب عدال كتاب عدال الكتاب عدال كتاب عدال الكتاب عدال كتاب عدال كتا

ه. مساله 2.17 از كتاب مرجع اصلى درس (Stallings, 7th Edition)

(Stallings, 7th Edition) الله 2.18 از كتاب مرجع اصلى درس 3.18

## تمرین کامپیوتری:

مساله كامپيوترى 2.2 كتاب مرجع اصلى درس (Stallings, 7th Edition)