دانشگاه صنعتی شریف تمرین سری سوم مبانی رمزنگاری و امنیت شبکه تحویل: چهارشنبه ۱۳۹۹/۱/۲۷ نحوه تحویل: پاسخ تمرینها (تئوری و کامپیوتری) میبایست در CW آپلود شوند.

مساله 5.3 از کتاب مرجع اصلی درس (Stallings, 7th Edition)

۳. مساله 5.9 از کتاب مرجع اصلی درس (Stallings, 7th Edition)

٤. مساله 5.12 از كتاب مرجع اصلى درس (Stallings, 7th Edition)

۵. در یک سیستم جانشینی خطی (affine) که حروف از ۰ تا ۲۵ شمارهگذاری شدهاند، بر اساس فرکانس نسبی حروف نتاج زير حاصل شده است:

 $G_n = T_c$ ,  $O_n = J_c$ 

کلید رمزنگاری را بدست آورید.

7. مساله 3.4 از كتاب مرجع اصلى درس (Stallings, 7th Edition)

۷. مساله 3.6 از کتاب مرجع اصلی درس (Stallings, 7th Edition)

## تمرین کامپیوتری:

مساله 5.14 از كتاب مرجع اصلى درس (Stallings, 7th Edition)