به نام خدا

دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری — دانشجو: علیرضا توفیقی محمدی

تمرین : سری ۱

مدرّس: دکتر شهرام خزائی — شماره‌ی دانشجویی: ۹۶۱۰۰۳۶۳

مسأله‌ی ۱

مسئله را به این شکل حل می‌کنیم که رشته‌ها را دوتا دوتا XOR کرده و بایت‌هایی که بیت ۳۲ را دارند یکی از آن‌ها کاراکتر حروف الفبا نیست، بر این اساس جایگاه اسپیس‌ها را حدس زده، سپس از روی جایگاه اسپیس‌ها یک کلید می‌سازیم و مقادیر رمزگشایی را با آن‌ها چاپ می‌کنیم. سپس کلید را جوری تغییر می‌دهیم تا رمزگشایی‌ها منطقی شوند.
کد در 1.py قرار دارد.

مسأله‌ی ۲

با توجه به اینکه باید طول بلوک مقسوم علیه‌ای از رمز باشد، حدس می‌زنیم طول بلوک ۷ باشد، سپس با کمک تعداد دوحرفی‌های پرتکرار و اینکه حروف x باید آخر رشته باشند، رمز را رمزگشایی می‌کنیم. کد در 2.py قرار دارد.

مسأله‌ی ۳

آ)

سیستم رمز جایگزینی نیست چراکه واریانسِ فرکانس حروف با واریانس فراکنس حروف انگلیسی متفاوت است.

ب)

حدس می‌زنیم سیستم رمز ویژنر باشد، با محاسبه‌ی واریانس فراکناس حروف حرف‌های iام بلوک‌ها حدس می‌زنیم که طول بلوک 5 باشد، حال با کمک حمله به سیستم سزار رمزگشایی می‌کنیم.
کد در 3.py قرار دارد.

مسأله‌ی ۴