۱. حملات زیر را توضیح دهید و راه‌کارهای مقابله با آن‌ها را بیان نمایید همچنین بیان کنید که کدام اصول از اصول سه‌گانه را نقض خواهند کرد. (۱۰ نمره)

- TCP sequence prediction attack
- Reflector attack
- Masquerading attack
- Fault injection attack
- Man in the middle attack

۲. برای هر یک از حالت‌های کاری رمز قالبی CTR، PCBC، OFB، ECB موارد زیر را به‌طور دقیق بررسی کنید: (۱۰ نمره)

الف) تأثیر خطا در انتقال یک بیت از متن رمز شده بر فرآیند رمزگشایی

ب) تأثیر از دست رفتن یک بلوک متن رمز شده بر فرآیند رمزگشایی

پ) امکان رمز کردن چند بلوک به‌طور موازی

ت) امکان رمزگشایی چند بلوک به‌طور موازی

ث) امکان رمزگشایی یک بلوک دلخواه

۳. در این سؤال می‌خواهیم مدل رمزنگاری کلاسیک playfair را بررسی کنیم. (۱۰ نمره)

الف) این رمزنگاری در کدام دسته از روش‌های کلاسیک قرار می‌گیرد؟ با ذکر دلیل بیان کنید.

ب) ۲ مورد از مزایا و معایب این سیستم رمزنگاری کلاسیک را نام برده و توضیح دهید.

پ) قوانین رمزنگاری در این سیستم رمز را بیان کنید.

ت) متن رمز شده DISYGLYOWLGRYDLVSYGRDTXICO را با کلید رمزنگاری secret-key=victory رمزگشایی کنید.[۱]

ث) این سیستم رمزنگاری را در برابر حملات آماری بررسی کنید.

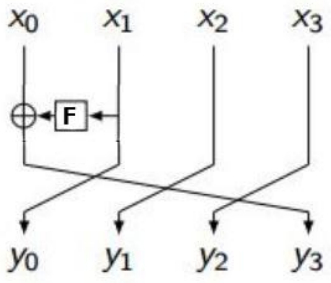
۴. فرض کنید عبارت رمز شده‌ی C و C’ را داریم که با کلیدهای K و K’ با رمز OTP رمز شده‌اند، کلید K’ مکمل بیتی K می‌باشد (تمامی بیت‌های K مخالف K’ است). چه استنتاجی برای پیام می‌توانیم داشته باشیم؟ (۲ نمره)

[۱] در ماتریس 5 × 5 حروف J/K را با هم در نظر بگیرید، همچنین استفاده از ابزار مجاز نیست و تنها برای بررسی جواب می‌توانید از ابزار استفاده نمایید.

۵. خاصیت بهمنی اکید، خاصیت تمامیت، Random cipher را تعریف کنید. (۱۷ نمره)

این سه خاصیت را برای ساختار feistel Trasnformation زیر بررسی نمایید.

راهنمایی: انواع Generalized feistel transformation را مطالعه کنید.




۶. آیا انتخاب کلید در امنیت الگوریتم DES تأثیرگذار است؟ توضیح دهید (۱۰ نمره).

۷. CrypTool یکی از ابزارهای قدرتمند و متن‌باز رمزنگاری است. تمرینات زیر را با استفاده از این ابزار انجام دهید[۲] و اسکرین شات نتیجه‌ی هر مرحله را در فایل پاسخ خود (DNS-HW1-STDID.pdf) قرار دهید. (۶ نمره)

الف) نام کامل خود (مثلاً MaryamKarimi) را با استفاده از رمز سزار با کلید = "G" رمزگذاری کنید. برای حل سؤال از مسیر زیر استفاده کنید.

Crypt/Decrypt -> Symmetric (classic) -> Caesar

ب) متن آشکار[۳] زیر را با استفاده از رمز جایگزینی[۴] رمزگذاری کنید، از qhpgiuwaeylnofdxjkrzvstcmb به‌عنوان کلید استفاده کنید و مقدار آفست را صفر قرار دهید. برای حل سؤال از مسیر زیر استفاده کنید.

Crypt/Decrypt -> Symmetric (classic) -> Substitution/Atbash

Plain text: If you cannot explain it to a six year old you do not understand it yourself.

پ) متن آشکار استفاده‌شده در قسمت دوم این سؤال را با استفاده از رمز Vigenere یک بار با کلید "sut" و بار دیگر با کلید "sharifuniversityoftechnology" رمزگذاری کنید. سپس نتایج را با هم مقایسه کنید و توضیح دهید طول کلید چه تأثیری روی متن رمز شده دارد. برای حل سؤال از مسیر زیر استفاده کنید.

---

[۲] این ابزار را میتوانید از https://www.cryptool.org/en/ct1/downloads دانلود کنید.

[۳] Plain text

[۴] Substitution

Crypt/Decrypt -> Symmetric (classic) -> Vigenère

ت) متن آشکار استفاده شده در قسمت دوم این سؤال را با استفاده از رمزگذاری Playfair رمزگذاری کنید. ماتریس ۶×۶ را انتخاب کنید و از نام کامل خود، همراه با شماره دانشجویی بدون فاصله به عنوان عبارت کلیدی بهره ببرید (مثلاً MaryamKarimi98230698). برای حل سؤال از مسیر زیر استفاده کنید.

Crypt/Decrypt -> Symmetric(classic) -> Playfair

ث) دو متن رمز شده زیر با استفاده از رمز جایگزینی رمزگذاری شده‌اند، کدام یک از آن‌ها با استفاده از ابزارهای تحلیلی Cryptool از نظر شباهت به زبان نوشتاری نزدیک‌تر است؟ دلیل آن را بیان کنید. برای حل سؤال از مسیر زیر استفاده کنید.

Analysis -> symmetric Encryption (classic) -> Ciphertext-only -> Substitution

- tk whmdvjrhqdum, q gbpgvtvbvtjk wtdueh tg q sevujo ji ekwhmdvtkr pm nutwu bktvg ji dlqtkvezv qhe hedlqweo ntvu wtduehvezv, qwwjhotkr vj q itzeo gmgves; vue "bktvg" sqm pe gtkrle levvehg (vue sjgv wjssjk), dqthg ji levvehg, vhtdlevg ji levvehg, stzvbheg ji vue qpjce, qko gj ijhvu. vue hewetceh oewtduehg vue vezv pm dehijhstkr vue tkcehge gbpgvtvbvtjk. gbpgvtvbvtjk wtduehg wqk pe wjsdqheo ntvu vhqkgdjgtvtjk wtduehg. tk q vhqkgdjgtvtjk wtdueh, vue bktvg ji vue dlqtkvezv qhe heqhhqkreo tk q otiiehekv qko bgbqllm fbtve wjsdlez jhoeh, pbv vue bktvg vuesgelceg qhe leiv bkwuqkreo. pm wjkvhqgv, tk q gbpgvtvbvtjk wtdueh, vue bktvg ji vue dlqtkvezv qhe hevqtkeo tk vue gqse gefbekwe tk vue wtduehvezv, pbv vue bktvg vuesgelceg qhe qlveheo. vuehe qhe q kbspeh ji otiiehekv vmdeg ji gbpgvtvbvtjk wtdueh. ti vue wtdueh jdehqveg jk gtkrle levvehg, tv tg vehseo q gtsdle gbpgvtvbvtjk wtdueh; q wtdueh vuqv jdehqveg jk lqhreh rhjbdg ji levvehg tg vehseo djlmrhqdutw. q sjkjqlduqpevtw wtdueh bgeg itzeo gbpgvtvbvtjk jceh vue ekvthe seggqre, nueheqg q djlmqlduqpevtw wtdueh bgeg q kbspeh ji gbpgvtvbvtjkg qv otiiehekv djgtvtjkg tk vue seggqre, nuehe q bktv ihjs vue dlqtkvezv tg sqddeo vj jke ji gecehql djggtptltvteg tk vue wtduehvezv qko ctwe cehgq.
- ycegklng egu eqytjejkfyc iuzskqt muegkt vkq bquyejfn y mjdut wlhwejelejkf ycpgyhue jw wjmpcu, y wuqjklw tjwytayfeynu jw egye egu cywe cueeuqw kv egu ycpgyhue (sgjbg yqu mkwecz cks vquolufbz) euft ek weyz ye egu uft. y weqkfnuq syz kv bkfweqlbejfn y mjdut ycpgyhue jw ek puqvkqm y bkclmfyq eqyfwpkwjejkf kf egu kqtjfyqz ycpgyhue lwjfn egu iuzskqt, hle egjw jw fke kveuf tkfu.

ج) متن رمز شده زیر را که با رمز Vigenere رمزگذاری شده است، با استفاده از ابزارهای تحلیلی CrypTool رمزگشایی کنید. نمودار ترسیم‌شده نمایانگر چیست؟ آن را تفسیر کنید. برای حل سؤال از مسیر زیر استفاده کنید.

Analysis -> symmetric Encryption (classic) -> Ciphertext-only -> Vigenere

udgaxgat tw nqzj jdqftfdq iyh wmaj xg gap qswqyk af qoisx nzv lqinlazo aigbtp etace gjkxesydialq ub lpka kzrlmqyw kqdpvsx lpqgzaevsfqzr wjixtdqa elsf ici vqatkfql es tq dpvq qidc la nzpdae lrv nzpec pwhr ltm xeltmxelukd mffw dqsxt xefmopetxm dxwba.

۸. برنامه‌ای بنویسید که متن رمز شده زیر را دریافت کند سپس به ترتیب مراحل زیر را انجام دهد. (۳۵ نمره)

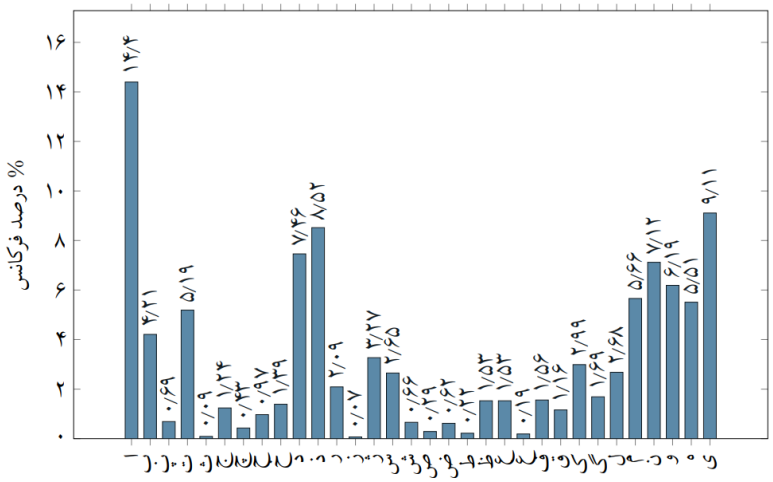
الف) طول کلید استفاده‌شده را حدس بزند و درنهایت کلید را پیدا کند.

ب) متن آشکار را به دست آورد.

**راهنمایی**: برای یافتن طول کلید از روش Kasiski استفاده کنید.

**توجه:** نمودار فرکانس نسبی حروف فارسی در ادامه آورده شده است.

تپکنج طغعث ژرا عر فرز رکاچق شددچ کوچف ل اچقم هدف ل ظعضم فع قهغج فوضطذ هضچذر ثذرگسدد مصح رگمح فو ژح حلثزذ ها ثح هوچرگ غجثوظ عخدظدس خغ ذثزغ چ وضغث ظلا کزوضپرم ققف ما شد گطکسم فچع جطدحچ هخفلزز لچ ط میوص جسلغجگا وچفچ اچق چطث حنب شحنض کع ل ققف معش وضغث حججطعع خطغ گلص ذرد ظعضم سیسم فچع گطکس ل کد حلثزذ خغ ذف جطدحچ غیسوف عخد محرخص مجلد بفچ ط دخ معش وضغث حججطعع خطغ ضمغعچ معش حفرز له قطف وب دخ جطدگا ژح توذظدو فخرلاط خ گطکسمظد زجطدحچ ققف فرز رکاچق معش حفرزدوص زر هاضخوضث جعصدح فرز ژر فخر ل غغ رنض جرگ ژح زخ تیفم غقس هوچف ل فطرگ ژح فلب اذوصز رگغج تم ژث ثظکحرگه شحوض صرق وچلن هدفگه بد وژجخگ کچ عواخ



**نکات مهم**

- **خروجی تمرین شما میبایست دقیقا مطابق با استاندارد عنوان شده در زیر باشد.**

DNS-HW1-STDID.zip..... (STDID شماره دانشجویی شماست)
DNS-HW1-STDID.pdf
8.ipynb
requirements.txt

- اطمینان حاصل کنید که سند آشنایی با مقررات تمرینها را به خوبی مطالعه کرده و نسبت به نکات و دلایل احتمالی کسر نمره ذکر شده در آن آگاهی کامل را بدست آورده اید.
- در صورت استفاده از هر گونه منبع برای پاسخ به سوالات، ذکر اسم و نشانی دقیق و کامل دسترسی به صفحه مورد نظر الزامی است.