تکلیف ۱ : رمز کلاسیک و متقارن

مهلت حل تکلیف : پایان اسفندماه ۱۴۰۱

پاسخ شما به سوالات تکلیف بایستی در قالب فایل word و با نام HW1_yourFamilyName ارسال شود. چنانچه عکس یا کدی به ضمیمه پاسخ خود ارسال می‌کنید؛ نام آن باید HW1_ yourFamilyName_#Question باشد.

۱- برنامه‌ای به زبان پایتون، به منظور تحلیل رمز جانشینی ساده (Simple Substitution) با استفاده از روش تحلیل آماری بنویسید. خروجی برنامه شما باید «کلید» و «متن آشکار» متناظر با متن رمزشده باشد.

۲- متن زیر را که با استفاده از رمزنگار Double transposition رمز شده است، رمزشکنی کنید.

راهنمایی : ماتریس ۵ سطر و ۷ ستون دارد و کلمه آخر متن آشکار «****Phal» است.

ITNGTWH
AEHANLG
EISOTMH
EPHEFLT
SONGWIR

۳- بخشی از Codebook استفاده‌شده برای پیام رمزشدهٔ 241, 355, 645, 668, 704, 566, 530, 401, 490, 670 به‌صورت زیر است.

I	256
You	274
We	289
They	123
Do	200
Don’t	199
Are	305
Know	301
That	451
Stupid	387
Genius	369

چنانچه از دنباله Additive زیر برای رمزنگاری استفاده شده باشد؛ الف) متن آشکار را بدست آورید.

118, 156, 344, 217, 415, 265, 407, 100, 201, 369

ب) بدون استفاده از Additive، متن آشکار بدست‌آمده را رمز کنید.

۴- ۲۵۶ بایت تولیدشده ابتدایی برای رمزنگاری با RC4 بایستی دور انداخته شود؛ در غیر این‌صورت وقوع حمله «کلید مرتبط» محتمل خواهد بود. در مورد چگونگی این حمله علیه RC4 تحقیق کنید.

۵- یک رمزنگار فایستلی (Feistel cipher) با ۴ دور را در نظر بگیرید. چنانچه متن آشکار به‌صورت $P = (L_0, R_0)$ و متن رمزشده نظیر آن به‌صورت $C = (L_4, R_4)$ نمایش داده شوند. رابطه C با L_0 و R_0 چیست؛ اگر تابع دور هر یک از توابع زیر باشد:

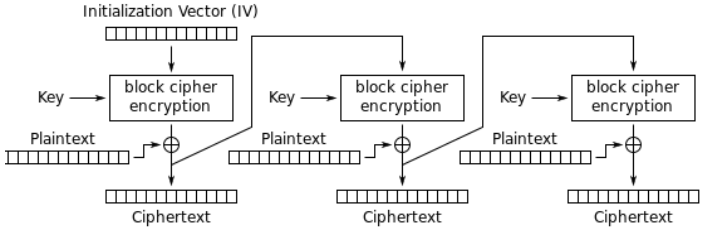
الف) $F(R_{i-1}, K_i) = 0$

ب) $F(R_{i-1}, K_i) = R_{i-1}$

ج) $F(R_{i-1}, K_i) = K_i$

د) $F(R_{i-1}, K_i) = R_{i-1} \oplus K_i$

۶- یکی از مُدهای عملیاتی رمزنگار بلوکی، Cipher Feedback یا به‌اختصار CFB است که نحوه عملکرد آن در شکل زیر آمده است. روابط رمزنگاری و رمزگشایی آن را بنویسید. این مُد را با مُدهای CBC و CTR مقایسه کنید.



Cipher Feedback (CFB) mode encryption

۷- چنانچه آلیس و باب بر سر استفاده همیشگی از یک IV به جای IV تصادفی توافق کنند؛

الف) مشکلات امنیتی محتمل در مُد CBC چه خواهد بود؟

ب) مشکلات امنیتی محتمل در مُد CTR چه خواهد بود؟

ج) در چنینی شرایطی کدام یک از دو مُد فوق‌الذکر امن‌تر است؟

۸- به کمک کد پایتون ابتدا تصویر فشرده‌نشده‌ای از خودتان را Grayscale کرده و سپس با رمزنگار AES در دو مُد ECB و CBC رمز کنید.

راهنمایی : می‌توانید از کدهای https://github.com/Apress/practical-cryptography-in-python/tree/master/src استفاده کنید.

سوال اضافه (۰,۵ نمره) : حمله تفاضلی به رمزنگار DES را شرح دهید.