«کوئیز ۱» یا «تکلیف ۲» مسئله این است!

دوره مباحث پیش از عید نوروز

لطفاً پیش از پاسخ به سوالات، فایل «**حتما مرا بخوانید**» را که در سامانه بارگذاری شده است، بخوانید :)

پاسخ شما به سوالات کوئیز/تکلیف بایستی در قالب فایل word و با نام QZ1_yourFamilyName یا HW2_yourFamilyName ارسال شود. چنانچه عکس یا کدی به ضمیمه پاسخ خود ارسال می‌کنید؛ نام آن باید QZ1_ yourFamilyName_#Question یا QZ1_ yourFamilyName_#Question باشد.

۱- متن آشکار زیر را با روش Vigenere و با استفاده از شماره دانشجویی خود(به عنوان کلید) رمز کنید.

راهنمایی : عدد ۳ در شماره دانشجویی ≡ شیفت با ۳

“Let’s put a smile on that face”

۲- سیستم رمز 3DES را به صورت زیر در نظر بگیرید.

$$C = E(E(E(P, k_3), k_2), k_1)$$

پیچیدگی زمانی حمله جستجوی فراگیر را در حملات Only Ciphertext و known plaintext محاسبه کنید.

۳- چرا استفاده مجدد از کلید و IV در مد CBC ایده مناسبی نیست؟

۴- اگر در سیستم رمز کوله‌پشتی، SIK برابر $(3, 5, 12, 23)$ ، $n = 47$ و $m = 6$ باشد؛ کلید عمومی و خصوصی چیست؟

پیام $M = 1101$ را با این سیستم رمز کنید.

۵- با رسم دیاگرام، حمله MitM علیه ECC DH را شرح دهید.

۶- در سیستم رمز ECC DH با خم بیضوی $y^2 = x^3 + 11x + 19 \ mod \ 167$ و نقطه $p = (2,7)$؛

اگر آلیس مقدار $A = 12$ و باب مقدار $B = 31$ را انتخاب کرده باشند. آلیس و باب چه مقداری برای یکدیگر ارسال می‌کنند؟ کلید مشترک آلیس و باب چه خواهد بود؟ (از ابزارهای آنلاین محاسبات خم بیضوی استفاده کنید)

سوالات زیر را تنها در صورتی پاسخ دهید که این فایل تکلیف شما باشد.

- چنانچه مقادیر رجیسترهای X، Y و Z در الگوریتم رمز A5/1 بصورت زیر باشد؛ به تعداد n بیت کلید تولید کنید.

$$n = ((\text{شماره دانشجویی } mod\ 5) + 2)$$

راهنمایی : اگر شماره دانشجویی شما ۹۹۳۱۵۵۸ است؛ بایستی ۵ بیت کلید تولید کنید.

X = (x0,x1,..., x18) = (1010101010101010101)

Y = (y0, y1, ··, y21) = (1100110011001100110011)

- *Z = {z0, z1,... , z22) = (11100001111000011110000)*

- ساختار گواهی X509 را توضیح دهید.
- سیستم رمز ECC RSA را شرح دهید.
- برنامه‌ای بنویسید که خروجی آن چندین collision تابع چکیده‌ساز MD5 باشد.

سوال اضافه (۰,۵ نمره) : حمله lattice reduction به سیستم رمز کوله‌پشتی را شرح دهید.