۱-۱- در پروتکل دیفی هلمن، کلید خصوصی از مجموعه‌ی $\{2, \dots, p-2\}$ انتخاب می‌شود. چرا مقادیر 1 و $p-1$ از این مجموعه حذف شده‌اند؟

۱-۲- ثابت کنید که رمزگشایی یک متن رمزشده دلخواه به مد p در الجمال با شکستن دیفی هلمن تصادفی به مد p برابر است.

۲- primitive root را برای 11 ، 11^2 ، $2 \cdot 11^2$ و 11^{100} محاسبه کنید.

۳- اگر باب از الگوریتم الجمال با پارامترهای $p = 44927$ ، $a = 7$ و $d = 22105$ برای رمز نگاری متن $m = 10101$ استفاده کند؛ کلید عمومی، متن رمز شده و رمزگشایی متن رمزشده را پیدا کنید.

۴- منحنی خم بیضوی زیر را در نظر بگیرید:

$$y^2 = x^3 + 2x + 2 \quad mod\ 17$$

۴-۱- نشان دهید $4a^3 + 27b^2 \neq 0 \quad mod\ p$ برای این منحنی برقرار است.

۴-۲- حاصل جمع نقاط $(5,2) + (2,7)$ را روی این منحنی حساب کنید.

۴-۳- برقراری قضیه هس (Hasse's Theorem) را بر روی این خم بررسی کنید.

۴-۴- توضیح دهید چرا تمامی عناصر primitive elements می‌باشند.

۵- اگر E یک خم بیضوی تعریف شده بر Z_7 باشد:

$$E:\ y^2 = x^3 + 3x + 2$$

۵-۱- همه‌ی نقاط منحنی E را بر روی Z_7 را بدست آورید.

۵-۲- مرتبه گروه (#E) را بدست آورید.

۵-۳- اگر $\alpha = (0,3)$ باشد، مرتبه α را بدست آورید. آیا α یک عنصر primitive است؟

۶- می‌خواهیم یک کلید جلسه‌ای (session key) در پروتکل دیفی هلمن بر اساس خم‌های بیضوی محاسبه کنیم. کلید خصوصی $a = 6$ ، کلید عمومی باب $B = (5,9)$ و منحنی مورد استفاده که به صورت زیر تعریف شده‌است را در اختیار دارید. کلید جلسه‌ای (session key) را بدست آورید.

$$y^2 = x^3 + x + 6 \quad mod\ 11$$

تمرین کریپتول:

7- 1963497163 is the product of two prime numbers, use tools within the CrypTool to find these two prime numbers.

8- Choose three large prime numbers, three Carmichael numbers, and three regular composite numbers, and use CrypTool primality test tools to do the following exercises;

a. Test the primality of your chosen numbers using Fermat test.
b. Test their primality using Miller-Rabin test.

9- Generate an asymmetric key pair using RSA algorithm, your own last name, first name and student number (as your PIN). Show the generated key pair.

(Hint: go to Digital Signatures/PKI :: PKI :: Generate/Import Keys)

10- Use the key pair generated in the previous question and a text of your choice to do the following exercises;

a. Encrypt the text using RSA encryption.
b. Decrypt the ciphertext in the previous part using the same algorithm.

11- Use Diffie-Hellman visualization tool to see its key exchange procedure.

(Hint: go to Indiv. Procedures :: Protocols :: Diffie-Hellman Demonstration)

12- Answer the following questions using CrypTool Point addition tool (on elliptic curves) on the curve $y^2 = x^3 + 2x + 2$. For each part, explain the approach adopted by the tool to solve the problems;

(Hint: go to Indiv. Procedures :: Number Theory – Interactive :: Point Addition on Elliptic Curves)

a. Mark an arbitrary point P on the curve, and compute 5*P.
b. Mark two other points P and Q, and compute P+Q.