۱- امضای الجمال با پارامترهای $p = 31$ ، $\alpha = 3$ و $\beta = 6$ را درنظر بگیرید. شما پیام $x = 10$ را دوبار با دو امضای $(13,5)$ و $(17,5)$ دریافت می‌کنید.

۱-۱- کدام یک از این دو امضا معتبر است؟

۱-۲- چند امضای معتبر برای هر پیام x و پارامترهای داده شده وجود دارد؟

۲- اگر از یک کلید ephemeral یکسان برای امضای دو پیام مختلف استفاده شود، نشان دهید چگونه DSA می‌تواند مورد حمله قرار بگیرد؟

۳- امضای RSA با کلید عمومی $(n = 9797, e = 131)$ را در نظر بگیرید. کدام یک از امضاهای زیر معتبر هستند؟

- $x = 123\,,\ sig(x) = 6292$
- $x = 4333\,,\ sig(x) = 4768$
- $x = 4333\,,\ sig(x) = 1424$

۴- سه تابع hash را در نظر بگیرید که خروجی‌هایی با طول‌های ۶۴ ، ۱۲۸ و ۱۶۰ بیت تولید می‌کنند.

۴-۱- بعد از چند ورودی تصادفی، احتمال collision برابر با $\varepsilon = 0.5$ می‌شود؟

۴-۲- بعد از چند ورودی تصادفی، احتمال collision برابر با $\varepsilon = 0.1$ می‌شود؟

۵-۱- در یک کلاس برای این‌که حداقل دو دانش‌آموز با احتمال بیش‌تر از 0.5 تاریخ تولد یکسانی داشته باشند، حداقل تعداد دانش‌آموزان یک کلاس چقدر باید باشند؟

۵-۲- اگر تعداد روزهای سال برابر با N و تعداد دانش‌آموزان برابر با K باشند، احتمال این‌که حداقل دو دانش‌آموز تاریخ تولد یکسانی داشته باشند را به صورت تابعی از K و N بدست آورید.

۶- برای مشاهده‌ی collision در تابع hash با خروجی به طول n بیت، با احتمال بیش‌تر از 0.5 ؛ چه تعداد پیام تصادفی مورد نیاز است؟

(نکته: از نابرابری $1 - x \le e^{-x}\ ,\ x > 0$ استفاده کنید.)

7- Answer the following questions with respect to the digital signature algorithm;

a. Generate a 2048bit DSA key pair using CrypTool key generation tool, with your own first name, last name, and student id (as your PIN).
b. Use this key to sign a document of your choice. What does the resulting file consist of?
c. Verify your previous signature using the same key.
d. Make a slight change to the signature and repeat the previous part. Explain what happens.

8- According to chapter 11 implement the SHA-1 algorithm in your favorite programming language. Your code should receive a string of arbitrary length and compute its SHA-1 hash. Compare your results with built-in SHA-1 implementations.

OpenSSL (optional)

9- Do the following exercises regarding the ECDH cryptosystem;

a. Generate two EC key pairs, using one of the IANA's recommended named curves. Save them in files named "ec_client.key" and "ec_server.key" respectively.
b. Extract the public keys corresponding to the previously generated keys, and save them in files named "client_pub.key" and "server_pub.key".
c. Derive the shared secret value using the pkeyutl command, along with the client's private key, and the server's public key, and name it "secret1".
d. Repeat the previous step but, this time, with the server's private key, and the client's public key, and name the driven file "secret2".
e. How are "secret1" and "secret2" related to each other and why?

To access the list of named curves you might need to visit this link:
https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8

If you're interested to learn more about X.509 Public Key Infrastructure Certificate visit this link:
https://tools.ietf.org/html/rfc5280