ECE4802/CS4801 Assignment #5

Deadline: Dec 12, 11:59pm.

1. **ElGamal Encryption:** Encrypt and decrypt the following messages using ElGamal Encryption for $\mathbb{Z}_{971}^*$ and $g = 314$ ( generator $r = 8$ and $\alpha = 10,\ q = 97$) and show every intermediate step:
   **a.** Find the public key for private key $x = 23$.
   **b.** Encrypt the message $m = 49$ with random parameter k= 29.
   **c.** Decrypt the ciphertext from part b.
   **d.** Encrypt the message $m = 49$ with random parameter k= 135
   **e.** Decrypt the ciphertext from part d.
   **f.** In part b and d, the same message is encrypted under the same private key with different ephemeral keys. Explain why the related ciphertexts are different and how they give the same message $m$ after decryption.

2. **ElGamal Signature:** Sign and verify the message $m = 71$ using Elgamal Signature Scheme for $\mathbb{Z}_{971}^*$, generator $\alpha = 8$ and private key $x = 23$. Show every intermediate step:
   **a.** Find the public key.
   **b.** Sign the given message ($m = 71$) using the ephemeral key $k = 53$.
   **c.** Verify the signature computed in part b.

3. **RSA Signature** Let $p$ = 43, $q$ = 37, public key $b$ = 23 be your initial parameters. You may use a calculator for this problem, but you should show all intermediate results.
   **a. Key generation:** Compute $N$ and $\varphi(N)$. Compute the private key $k_{\text{priv}} = \text{a} = \text{b}^{-1} \bmod \varphi(N)$. Show all intermediate results.
   **b. Signing:** Sign the message X = 91**.**
   **c. Verification:** Verify *th*e signature $Sign(X)$ computed in part b.