MATH 220

Discrete Mathematics and Cryptography

Tutorial 5 **Week starting 20 April 2020**

---

1. This question relates to the Diffie-Hellman key exchange. Alice and Bob choose the (large) prime $p = 11$.

(a) (i) Find the order of each element in $\mathbb{Z}_{11}^*$.
(ii) Which elements are generators for $\mathbb{Z}_{11}^*$?

(b) Alice and Bob agree on the generator $g = 2$. Alice (randomly) chooses $a = 8$. What number A does Alice send to Bob to set up their shared key?

(c) Bob (randomly) chooses $b = 6$. What number B does Bob send to Alice?

(d) What is their shared secret key. (Make sure that Alice and Bob do in fact agree on their choice!)

2. Alice and Bob wish to communicate using the Elgamal cipher with the prime $p = 11$ and their shared secret key K as calculated in the last question. Bob wants to send the message $m = 5$.

(a) Find the corresponding ciphertext c.

(b) Alice receives the enciphered message c. Show that she decrypts it correctly.

3. Alice is using the RSA signature scheme with primes $p = 19$ and $q = 13$, and $e = 5$.

(a) What is n, the public modulus she will use?

(b) What is her private exponent d?

(c) How would Alice sign the message 93?

4. Find all possible roots of the polynomials

(a) $x^2 + 3x + 2$ in $\mathbb{Z}_5[x]$,

(b) $x^2 + 3x + 2$ in $\mathbb{Z}_7[x]$, and

(c) $x^4 + 4$ in $\mathbb{Z}_5[x]$.

Use these results to factorise each of the polynomials.

5. Find all roots of $f(x) = x^2 + 3x + 2$ in $\mathbb{Z}_{12}[x]$, and find all factorisations of $f(x)$. Compare your answer with the previous question.