MA080G Cryptography Assignment Block 1

Viktor Rosvall

April 25, 2019

Question 2

a. Explain the operation of the RSA public-key cryptosystem.

b. Illustrate your explanation by using the primes $p = 13$ and $q = 17$ and secret decryption key $d = 103$ to

   (i) decrypt the ciphertext $z = 2$;

   (ii) compute the public encryption key e corresponding to d;

   (iii) encrypt the plaintext $m = 2$

c. Discuss the security of the RSA public-key cryptosystem.

Answer 2

a.

b. (i)

   (ii)

   (iii)

c.

Question 3

a. Let $p \geq 2$ be a prime. Define what it means for an integer a to be a primitive element modulo p.

b. Find a primitive element modulo 23 and prove that it is a primitive element.

Answer 3

a.

b.

Question 4

c. Let a and n be positive integers and let $n \geq 2$. Prove that if $\gcd(a, n) = 1$ then

$$a^{\Phi(n)} \equiv 1 \pmod{n}.$$

d. Discuss whether the theorem from part (c) can be used as a primality test.

Answer 4

c.

d.

Question 6

For positive integers $p \geq 2$, Wilson's Theorem states that

$$p \text{ is a prime if and only if } (p-1)! \equiv -1 \pmod{p}.$$

a. Prove Wilson's Theorem.

b. Discuss whether Wilson's Theorem is suitable as a primality test for finding primes to use with RSA.