Quiz-4

Cryptography and Network Security

[Total marks - 20]

[**Instructions**: Please upload your answers in Microsoft Teams by **19/10/2020**. Your **Roll No.** and **Name** must be mentioned. No marks will be awarded without detailed solution.]

1. [**2 mark**] Given that 1111118111111 is a prime, determine whether 1001 is a quadratic residue (mod 1111118111111).

2. [**2 mark**] Compute the Jacobi symbol $\left(\frac{1234567}{11111111}\right)$ without any factoring, other than dividing out powers of two.

3. [**2 mark**] For $n = pq$, where p and q are distinct odd primes, define

$$\lambda(n) = \frac{(p-1)(q-1)}{gcd(p-1, q-1)}.$$

Suppose that we modify the RSA cryptosystem by requiring that $ed = 1 \bmod \lambda(n)$. Prove or disprove: Encryption and decryption are still inverse operations in this modified cryptosystem.

4. [**2 mark**] A plaintext m is said to be *fixed* if $\mathcal{E}_e(m) = m$. Show that, for the RSA Cryptosystem, the number of fixed plaintexts $m \in Z_n^\star$ is equal to

$$gcd(e-1, p-1) \times gcd(e-1, q-1).$$

5. [**2 mark**] Let $n = 713$ be a Rabin modulus and let $c = 289$ be a ciphertext that is obtained by Rabin encryption using this modulus. Determine all possible plaintexts.

6. [**5 mark**] Suppose that Alice and Bob decide to communicate with an ElGamal cryptosystem using the prime $p = 8263$ and individual keys

$a = 856$ and $b = 3127$, and using the smallest primitive root g of p that satisfies $g > 1700$. Write each answer as an integer in $\{1, 2, \ldots, m-1\}$, if you are working modulo m.

(a) Determine the primitive root g.

(b) Compute the ciphertext in this system if Alice sends Bob the message $P = 4321$.

(c) Perform the ElGamal decryption process that would need to get done at Bob's end to decrypt Alice's message.

7. [**5 mark**] You are given the following parameters for the Diffie Hellman Key Exchange algorithm:

Prime	p	$= 773$
Primitive root	g	$= 2$
User Alice selects private key	a	$= 333$
User Bob selects private key	b	$= 603$

Write each answer as an integer in $\{1, 2, \ldots, m-1\}$, if you are working modulo m.

(a) Show that $g = 2$ is indeed a primitive root of $q = 773$.

(b) Compute the number A that Alice (publicly) sends Bob, and the number B that Bob sends Alice.

(c) Compute the shared Diffie-Hellman key for Alice and Bob in two different ways, as would be done on Alice's end and on Bob's end.

——-The End———