Introduction to Quantum Information Science and Quantum Technologies

Assignment 5

Muhammad Abdullah Ijaz and Muhammad Sabieh Anwar

"I am batman." - *Batman*

Question 1

Alice and Bob need to engage in a BB84 style of QKD protocol. They use the Z and X basis randomly. Eve, living up to her name, eavesdrops on their communication using the F basis, whose eigenvectors are:

$$|0_F\rangle = cos\frac{\pi}{8}|0\rangle + sin\frac{\pi}{8}|1\rangle,$$
$$|1_F\rangle = sin\frac{\pi}{8}|0\rangle - cos\frac{\pi}{8}|1\rangle.$$

The rules Alice and Bob use to label their bits are:

Basis	States	Bits
Z	$\|0\rangle$	0
	$\|1\rangle$	1
X	$\|+\rangle$	0
	$\|-\rangle$	1

(a) Suppose we consider **only** when Alice and Bob use the same measurement basis. If Eve uses her F basis, what is the probability that when she intercepts and sends the qubit, Alice's intended qubit is faithfully transmitted to Bob?

(b) What is the probability that Eve measures the exact bit as sent by Alice?

Question 2

A devilishly simple RSA system has $N = 247$ and e = 5.

(a) Choose some three decimal digit plain text P and calculate the cipher text C.

(b) Show that $d = 173$.

(c) Use the private key to recover P from C.

Question 3

Calculate the Diffie-Hellman key for $p = 17$ and $g = 3$.

Question 4

Find the primitive roots modular 13. How many are they?

Question 5

(a) Argue why the Euler ϕ function for pq takes the form

$$\phi(pq) = (p-1)(q-1),$$

where p and q are primes.

(b) Why is $\phi(p^2) = p(p-1)$