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 $\phi(p^2) = p(p-1)$

Q1

a) Using the relations

$$\langle 0_f | 0 \rangle = \cos(\pi/8) \quad , \quad \langle 0_f | 1 \rangle = \sin(\pi/8)$$

$$\langle 1_f | 0 \rangle = \sin(\pi/8) \quad , \quad \langle 1_f | 1 \rangle = -\cos(\pi/8)$$

$$\langle 0_f | \pm \rangle = \frac{1}{\sqrt{2}} \left[\cos(\pi/8) \langle 0| + \sin(\pi/8) \langle 1| \right] \left[|0\rangle \pm |1\rangle \right]$$

$$= \frac{1}{\sqrt{2}} \left[\cos(\pi/8) \pm \sin(\pi/8) \right]$$

$$\langle 1_f | \pm \rangle = \frac{1}{\sqrt{2}} \left[\sin(\pi/8) \langle 0| - \cos(\pi/8) \langle 1| \right] \left[|0\rangle \pm |1\rangle \right]$$

$$= \frac{1}{\sqrt{2}} \left[\sin(\pi/8) \mp \cos(\pi/8) \right]$$

$$p(\text{no errors}) = \frac{1}{4} \sum \text{prob (all cases)}$$

$$= \frac{1}{4} \Big[2\cos^4(\pi/8) + 2\sin^4(\pi/8)$$

$$+ \frac{1}{4} \left(\cos(\pi/8) + \sin(\pi/8) \right)^4$$

$$+ \frac{1}{4} \left(\sin(\pi/8) - \cos(\pi/8) \right)^4$$

$$+ \frac{1}{4} \left(\cos(\pi/8) - \sin(\pi/8) \right)^4$$

$$+ \frac{1}{4} \left(\sin(\pi/8) + \cos(\pi/8) \right)^4 \Big]$$

$$= \frac{1}{4}\Big[2\cos^4(\pi/8) + 2\sin^4(\pi/8)$$

$$+ \frac{1}{2}\big(\cos(\pi/8) + \sin(\pi/8)\big)^4$$

$$+ \frac{1}{2}\big(\cos(\pi/8) - \sin(\pi/8)\big)^4 \Big]$$

$$= \frac{1}{4}\Big[2\left(\frac{3}{4}\right) + \frac{1}{2}(3) \Big]$$

$$= \frac{1}{4}\Big[\frac{3}{2} + \frac{3}{2} \Big]$$

$$= \frac{3}{4}$$

b) $$\text{Prob} = \frac{1}{4}\Big\{ |\langle 0_f|0\rangle|^2 + |\langle 1_f|1\rangle|^2$$

$$+ |\langle 0_f|+\rangle|^2 + |\langle 1_f|-\rangle|^2 \Big\}$$

$$= \frac{1}{4}\Big\{ \cos^2(\pi/8) + \cos^2(\pi/8)$$

$$+ \frac{1}{2}\big[\cos(\pi/8) + \sin(\pi/8)\big]^2 + \frac{1}{2}\big[\cos(\pi/8) + \sin(\pi/8)\big]^2 \Big\}$$

$$= \frac{1}{2}\cos^2(\pi/8) + \frac{1}{4}\big[\cos(\pi/8) + \sin(\pi/8)\big]^2$$

$$= 0.8535$$

* Note: Refer to lecture notes for complete understanding.

Q2

$N = pq = 247$, where $p = 13$, $q = 19$

For $e = 5$

a) lets choose, $M = 121$

$C = M^e \bmod N$

$= 121^5 \bmod 247$

$= 49$

b) $de = 1 \bmod \phi(N)$

$= 1 \bmod [(13-1)(19-1)]$

$= 1 \bmod 216$

$d = e^{-1} \bmod 216$

$\Rightarrow d = \dfrac{1 + K\,\phi(N)}{e}$, lowest value of K such that d is an integer

$= \dfrac{1 + K(216)}{e}$

For $K = 1, 2, 3$, d is not an integer

For $K = 4$

$d = \dfrac{1 + 4(216)}{e} = 173$

c) $M = C^d \bmod N$

$= 49^{173} \bmod 247$

$= 121$

Hence we have completed RSA.

Q 3

$g = 3$, $p = 17$

let for

Alice $\rightarrow a = 12$, Bob $\rightarrow b = 21$

$A = g^a \bmod p$

$= 3^{12} \bmod 17$

$= 4$

$B = g^b \bmod p$

$= 3^{21} \bmod 17$

$= 5$

- Alice and Bob share their encrypted messages A, B on a public channel.

$Sectkey_A = B^a \bmod p$

$= 5^{12} \bmod 17$

$= 4$

, $Sect\ key_B = A^b \bmod p$

$= 4^{21} \bmod 17$

$= 4$

Hence the Diffie-Hellman Key $= 4$

AnyScanner

Q 4

- Primitive roots of $n = 13$, $\phi(n) = 12$

Coprimes of $n \Rightarrow C = \{1, 2, 3, \dots 11, 12\}$

- Number of primitive roots $= \phi[\phi(n)]$

$= \phi[12]$

$= 4$

which is the number of i in C, that satisfy the relation $\gcd(12, i) = 1$

- Using trial and error for elements in C

$2 \equiv 2 \mod 13$
$2^2 \equiv 4 \mod 13$
$2^3 \equiv 8 \mod 13$
$2^4 \equiv 3 \mod 13$
$\vdots \qquad \vdots$
$2^{12} \equiv 27 \mod 13$
$2^{\phi(13)} \equiv 1 \mod 13$

Hence 2 is primitive root.

- Then $\{2^1, 2^2, 2^3, \dots 2^{12}\} \mod 13$ must contain the rest of the primitive roots. Such that

$(2^i, 13) = 1 \qquad 1 \leq i \leq 12$

$\Rightarrow \gcd(i, \phi(13)) = 1$
$\gcd(i, 12) = 1 \Rightarrow i = 1, 5, 7, 11$

So Primitive roots are

$2^1 \mod 13 = 2$, $\quad 2^7 \mod 13 = 11$

$2^5 \mod 13 = 6$, $\quad 2^{11} \mod 13 = 7$

$PR = \{2, 6, 7, 11\}$

AnyScanner

Q5

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

a) We can count the number of elements less than N that are multiples of p and q.

xp for $0 \le x < q$

yq for $0 \le y < p$

Where x and y take p and q values respectively, with both counting 0.

Then the number of elements that are not multiples of p and q (are coprime with N) are

$$\begin{aligned}\phi(N) &= N - p - q + 1 \\ &= pq - p - q + 1 \\ &= p(q-1) - 1(q-1) \\ &= (p-1)(q-1)\end{aligned}$$

b) Using the same approach as for part a)

$$\phi(p^2) = p(p-1) = \phi(N)$$

Counting the number of elements less than $N = p^2$, that are multiples of p.

xp for $0 \le x \le p$

Where x can take p values.

$$\begin{aligned}\phi(N) &= N - p \\ &= p^2 - p \\ &= p(p-1)\end{aligned}$$