Name:Chao Jiang

ECE 5563 — Spring 2015 **Final Exam 1** Due: May 8

Problem 1

1. Present a critique of the course you attended including a critique of the textbook, home assignments, and the method of instruction. What additional topics (or the additional depth associated with a particular topic) would you have liked the instructor to cover? What topics could have been dispensed with? If you were going to do research in security, in which aspects of security would you consider working? Give your reasons.

Ans: From this course, I study a lot related with security knowledge both in width and depth. The textbook is easy to understand, and the homework let me more understand the concepts I learned from the class. I am glad that I have the change to give a presentation though I am not good at that, it practices my spoken skills. I want to know some practice skills such as how to use some software to analysis the network. I will do some work related with Privacy Preserving Data Mining, for example, We want to release aggregate or statistical information about the data for research goals, without leaking individual information about participants. It is a very practical problem and have a big significant to deal with it.

Problem 2

Show that for the Digital Encryption Standard, the ciphertext C using the key K and plaintext P is the same as the ciphertext of the complement of C using the complement of Plaintext P and the complement of the key K. In other words,

$$C = E(K, P) \text{ implies, } \underline{C} = E(\underline{K}, \underline{P}) \text{ \{underline means complement\}}$$

How does this property affect the burden of the cryptanalyst?

Ans: After round i, the result will be $\underline{L_i}$ and $\underline{R_i}$ when the input was $\underline{L_{i-1}}$ and $\underline{R_{i-1}}$ and using $\underline{K}$ as key.

$$\begin{aligned} L_i &= R_{i-1} \Longrightarrow \underline{L_i} = \underline{R_{i-1}} \\ \underline{R_i} &= \underline{L_{i-1}} \oplus f(\underline{R_{i-1}}, \underline{k_i}) = \underline{L_{i-1}} \oplus f(R_{i-1}, k_i) = \underline{L_{i-1} \oplus f(R_{i-1}, k_i)} \end{aligned}$$

$f(\underline{R}, \underline{k}) = f(R, k)$ because within the function the complement of expansion R and $\underline{k}$ are xored which eleminates the complement. so

$$C = E(K, P) \Longrightarrow \underline{C} = E(\underline{K}, \underline{P})$$

When this property was being used, the key space is cut in half for the cryptanalyst using the brute-force.

Problem 3

What is the discrete logarithmic problem? How is it used in cryptography? What is its analog in elliptic curve cryptography? How is it used?

Ans: Let $(G, \oplus)$ be a cyclic group of prime order l and let P be a generator of G. Let the map

$$\begin{aligned} \phi &: Z \longrightarrow G \\ n \longrightarrow [n]P &= P \oplus P \oplus ... \oplus P \end{aligned}$$

The problem of computing the inverse of this map is called the discrete logarithm problem(DLP) to the base of P. If $[n]P = Q$, so we note $\log_P Q = n$. It can be used for Public Key Cryptography, it is very easy to compute $Q = p^n$ for given n, but very hard to find n given Q and p.

The elliptic curve also applying this theorem, given an elliptic curve C defined over F_q and two points $P, Q \in C$, find an integer x such that $Q = xP$. x is very difficult to find. so we can use Q and P to be the public key in any cryposystem. and x to be the private key.

Problem 4

Related to the birthday attack, there are four problems. Find a solution to each of these. The term *likely* in each case means with the probability greater than or equal to $\frac{1}{2}$.

a. What is the minimum number, k, of students in a classroom such that its likely that at least one student has a predefined birthday?

   Ans: $k = \ln[1/(1-p)] * 365 = 253$.

b. What is the minimum number, k, of students in a classroom such that its likely that at least one student has the same birthday as the student selected by the professor?

   Ans: $k = \ln[1/(1-p)] * 365 + 1 = 254$.

c. What is the minimum number, k, of students in a classroom such that its likely that at least two students have the same birthday?

   Ans: $k = (2\ln[1/(1-p)] * 365)^{1/2} = 23$.

d. We have two classes, each with k students. What is the minimum value of k so that its likely that at least one student from the first classroom has the same birthday as as a student from the second classroom?

   Ans: $k = 23$.

Problem 5

An eavesdropper follows the intercept and resend strategy in trying to attack a BB84 implementation. For a given plaintext bit 0 and a specific basis X in which Alice produces the qubit, enumerate the two possibilities of bases in which Eve could measure

the qubit and the resulting bit of information along with its associated probability. Assume that Eve encodes the bits she gets and encodes it using the same basis and then forwards the resulting qubit to Bob. Enumerate the resulting bits after Bobs measurements for each possible qubit received by him, along with its associated probability. Present your result in a tabular form. Based on the table, show that the probability that Alice and Bob discover the presence of Eve after comparing n bits is given by, $P = 1-(3/4)^n$. If the probability of Eve escaping detection were to be kept lower than, say a given probability p, what must be the minimum length of the sequence n so that Eve does not escape detection.

Ans: Constructing the table below:

Alice	Alice basis	Bob basis	
Plaintext	diagonal	diagonal	rectilinear
0	0	0	0
			1

Probability that Bob selects the right basis is $\frac{1}{2}$.
Probability that Bob receives right bit is $\frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$
Probability that Bob receives wrong bit is $\frac{1}{4}$
If there are n number of bits in the plaintext then probability that bob receives right information is $(\frac{3}{4})^n$.

Both Eve and bob doesnt know the basis which was used by Alice.

Alice Plaintext	Alice basis	Eve basis		Bob Basis	
	diagonal	diagonal	rectilinear	diagonal	rectilinear
0	0	0	0	0	0
			1		1

Probability that Eve selects the right basis is $\frac{1}{2}$.
Probability that Eve receive right bit is $\frac{3}{4}$.
Now probability reduces from 1 to $\frac{3}{4}$ when it is transmitted to Bob. This means that: Bob select the right basis is $\frac{1}{2}$, right bit is $\frac{1}{2} * \frac{3}{4} + \frac{1}{2} * \frac{1}{2} = \frac{5}{8}$
So, the probability that Alice and bob detect the presence of eve after comparing n bits is given by $1 - (\frac{3}{4})^n$
Probability that eve is not detected $p = 1 - P = (\frac{3}{4})^n$

If the probability of Eve escaping detection were to be kept lower than, say a given probability p, the minimum length of the sequence n so that Eve does not escape detection is $(\frac{3}{4})^n < P$.

The minimum length of the sequence n so that eve does not escape detection is $n < \log_{\frac{3}{4}}(1 - P)$