1 Lecture 1: Introduction

Exercise 1
Give the security properties that an international airport should guarantee.

Exercise 2
Suppose a certain drug test is 99% accurate, that is, the test will correctly identify a drug user as testing positive 99% of the time, and will correctly identify a non-user as testing negative 99% of the time. Let’s assume a corporation decides to test its employees for opium use, and 0.5% of the employees use the drug.

We want to know the probability that, given a positive drug test, an employee is actually a drug user.

Exercise 3
Prove that for real random variables $X$ and $Y$, and real number $a$, we have $E[X + Y] = E[X] + E[Y]$ and $E[aX] = aE[X]$. And if $X$ and $Y$ are independent real random variables, then $E[XY] = E[X]E[Y]$.

Exercise 4
Let $X$ be a real random variable, and let $a$ and $b$ be real numbers. Then we have:

(i) $Var[X] = E[X^2] - (E[X])^2$
(ii) $Var[aX] = a^2Var[X]$
(iii) $Var[X + b] = Var[X]$

Exercise 5
Prove Markov’s inequality: Let $X$ be a random variable that takes only non-negative real values. Then for any $t > 0$, we have

$$P[X \geq t] \leq \frac{E[X]}{t}$$

Exercise 6
Prove Chebyshev’s inequality: Let $X$ be a real random variable. Then for any $t > 0$, we have:

$$P[|X - E[X]| \geq t] \leq \frac{Var[X]}{t^2}$$
Exercise 7
Prove Chernoff bound: Let $X_1, \ldots, X_n$ be mutually independent random variables, such that each $X_i$ is 1 with probability $p$ and 0 with probability $q := 1 - p$. Assume that $0 < p < 1$. Also, let $X$ be the sample mean of $X_1, \ldots, X_n$. Then for any $\epsilon > 0$, we have:

- $(i) P[\overline{X} - p \geq \epsilon] \leq e^{-n\epsilon^2/2q}$
- $(ii) P[\overline{X} - p \leq -\epsilon] \leq e^{-n\epsilon^2/2p}$
- $(iii) P[|\overline{X} - p| \geq \epsilon] \leq 2e^{-n\epsilon^2/2}$

Exercise 8
Generalization of BirthDay Paradox:
The setting is that we have $q$ balls. View them as numbered, 1, \ldots, $q$. We also have $N$ bins, where $N \geq q$. We throw the balls at random into the bins, one by one, beginning with ball 1. At random means that each ball is equally likely to land in any of the $N$ bins, and the probabilities for all the balls are independent. A collision is said to occur if some bin ends up containing at least two balls. We are interested in $C(N, q)$, the probability of a collision. The birthday paradox is the case where $N = 365$. We are asking what is the chance that, in a group of $q$ people, there are two people with the same birthday, assuming birthdays are randomly and independently distributed over the days of the year.

Let $C(N, q)$ denote the probability of at least one collision when we throw $q \geq 1$ balls at random into $N \geq q$ buckets. Then

$$C(N, q) \leq \frac{q(q - 1)}{2N}$$

Also if $1 \leq q \leq \sqrt{2N}$ then $C(N, q) \geq 1 - e^{(q-1)/2N}$. Hint: first prove the inequality $(1 - 1/e)x \leq 1 - e^{-x} \leq x$.

Exercise 9
Prove or disprove:

a) The function $f(n) := (\frac{1}{2})^n$ is negligible.

b) The function $f(n) := 2^{-\sqrt{n}}$ is negligible.

c) The function $f(n) := n^{-\log n}$ is negligible.

Exercise 10
Prove or disprove the following statements:

1. If both $f, g \geq 0$ are noticeable, then $f - g$ and $f + g$ are noticeable.

2. If both $f, g \geq 0$ are not noticeable, then $fg$ is not noticeable.

3. If both $f, g \geq 0$ are not noticeable, then $f + g$ is not noticeable.

4. If $f \geq 0$ is noticeable, and $g \geq 0$ is negligible, then $fg$ is negligible.

5. If both $f, g \geq 0$ are negligible, then $f/g$ is noticeable.
2 Lecture 2: Introduction

Exercise 11
Prove that $DDH \leq CDH \leq DL$

Exercise 12
Prove that
\[
\text{Adv}_{S,A}^{\text{IND}}(\eta) = 2\Pr[b' \xleftarrow{\text{R}} \text{IND}^1(A) : b' = 1] - \Pr[b' \xleftarrow{\text{R}} \text{IND}^0(A) : b' = 1]
\]

3 Lecture 3: Reductions Proofs

Exercise 13
Message are composed of \{0, 1\}, keys are \{A, B\} and we know $P(0)=1/4, P(1)=3/4, P(A)=1/4, P(B)=3/4$. The encryption is defined by:
\[
E_A(0) = a, E_A(1) = b, E_B(0) = b, E_B(1) = a
\]
This encryption is it perfectly secure?

Exercise 14
Prove that OTP is perfectly secure according Shannon definition.

Exercise 15
Prove the following equivalence:
\[
\text{independance} + H(m|c) = H(m) \iff \Pr(m = m'|c = c') = \Pr(m = m')
\]

Exercise 16
Prove that under CDH assumption El-Gamal is OW-CPA.

Exercise 17
Prove that under DDH assumption El-Gamal is IND-CPA.

4 Lecture 4: Public Encryption

Exercise 18
Prove that $X$ and $Y$ are independent if and only if for all values $x$ taken by $X$ with non-zero probability, the conditional distribution of $Y$ given the event $X = x$ is the same as the distribution of $Y'$.

Exercise 19
Consider the algorithm $D2$ that outputs 1 iff the input string contains more zeros than ones. If $D2$ can be implemented in polynomial time, then prove that $X$ and $Y$ are polynomial-time-indistinguishable. (Assume that the two inputs have the same size)

Exercise 20
Let $X := \{X_n\}_{n \in \mathbb{N}}, Y := \{Y_n\}_{n \in \mathbb{N}}$ and $Z := \{Z_n\}_{n \in \mathbb{N}}$ three ensembles. If $X$ and $Y$ are indistinguishable in polynomial time, $Y$ and $Z$ are indistinguishable in polynomial time then $X$ and $Z$ are indistinguishable in polynomial time.
**Exercise 21**
Recall that the distributions $D_0, D_1$ are said to be indistinguishable ($0 \leq \epsilon \leq 1$) if

$$|\Pr[A(x_0) = 1] - \Pr[A(x_1) = 1]| \leq \epsilon$$

holds for all adversaries $A$ running in time at most $t$, where the random variable $x_0$ is distributed according to $D_0$ and $x_1$ is distributed like $D_1$.

Now, let’s call the distributions $D_0, D_1$ inseparable just if

$$\frac{1}{2} - \frac{\epsilon}{2} \leq \Pr[A(x_b) = b] \leq \frac{1}{2} + \frac{\epsilon}{2}$$

holds for all adversaries $A$ running in time at most $t$, where the random variable $b$ is a uniformly random bit and where the random variable $x$ is distributed according to $D_b$. This is a very natural notion, because it talks about our chances of guessing correctly which distribution $x$ came from, and whether we can do much better than simply flipping a coin.

Prove: $D_0, D_1$ are indistinguishable if and only if they are inseparable. (Hence the notion of inseparability is redundant.)

**5 Lecture 5: Symmetric Encryption**

**Exercise 22**
Find an attack on CBC encryption with counter $IV$, (proving that this encryption mode is not IND-CPA secure). In this scheme the frist $IV$ used is 0 and for generating the next $IV$ we just increase by one the value of the previous $IV$.

**Exercise 23**
Prove that CBC with random $IV$ is not IND-CCA secure. This time $IV$ is a random number. But notice that this mode is IND-CPA secure.

**Exercise 24**
Find an attack on Needham Schroeder protocol:

1. $A \rightarrow B : \{N_a, A\}_{pk(B)}$
2. $A \leftarrow B : \{N_a, N_b\}_{pk(A)}$
3. $A \rightarrow B : \{N_b\}_{pk(B)}$