Security models

1st Semester 2014/2015

F.Autreau
P.Lafourcade
M. Gagné
JL. Roch

P. Lafourcade
M. Gagné

SET 0

Date: 20.10.2014

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. Prove that:

(i) $Var[X] = E[X^2] - (E[X])^2$

(ii) $Var[aX] = a^2 Var[X]$

(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 $X_1, ..., X_n$ 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 $X_1, ..., X_n$. 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

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

$$C(N, q) \geq 1 - e^{q(q-1)/2N}$$

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

Exercise 9
At the beginning of a party, each person shakes the hand of a certain number of the other guests. Show that there exist at least 2 people who will shake the hand of exactly the same number of people.

Exercise 10
In a group of six people, there will always be three people that are mutual friends or mutual strangers. Assume that friend is symmetric-if x is a friend of y, then y is a friend of x, and that stranger is the opposite of friend

Exercise 11
Let f and g be two negligible functions, then

1. $f.g$ is negligible.
2. For any $k > 0$, f^k is negligible.
3. For any $\lambda, \mu \in \mathbb{R}$, $\lambda, \mu > 0$, $\lambda f + \mu g$ is negligible.

Exercise 12
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 $f(n) := n^{-logn}$ is negligible.

Exercise 13
Prove or disprove the following statements:

1. If both $f, g \geq 0$ are noticeable, then $f \cdot g$ and $f + g$ are noticeable.
2. If both $f, g \geq 0$ are not noticeable, then $f \cdot g$ 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 $f \cdot g$ is negligible.
5. If both $f, g > 0$ are negligible, then f/g is noticeable.

Exercise 14
Prove that

$$\begin{aligned} \textsc{Adv}^{\textsc{Ind}}_{\mathcal{S},\mathcal{A}}(\eta) &= Pr[b' \xleftarrow{R} \textsc{Ind}^1(\mathcal{A}) : b' = 1] - Pr[b' \xleftarrow{R} \textsc{Ind}^0(\mathcal{A}) : b' = 1] \\ &= 2Pr[b' \xleftarrow{R} \textsc{Ind}^b(\mathcal{A}) : b' = b] - 1 \end{aligned}$$

where given an encryption scheme $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. An adversary is a pair $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ of polynomial-time probabilistic algorithms, $b \in \{0, 1\}$. Let $\textsc{Ind}^b(\mathcal{A})$ be the following algorithm: Generate $(pk, sk) \xleftarrow{R} \mathcal{K}(\eta)$; $(s, m_0, m_1) \xleftarrow{R} \mathcal{A}_1(\eta, pk)$; Sample $b \xleftarrow{R} \{0, 1\}$; $b' \xleftarrow{R} \mathcal{A}_2(\eta, pk, s, \mathcal{E}(pk, m_b))$; return b'

Exercise 15
Suppose that the message space is $\{0, 1\}$, 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: $E_A(0) = a, E_A(1) = b, E_B(0) = b, E_B(1) = a$. Is this encryption perfectly secure?

Exercise 16
Prove that OTP is perfectly secure according Shannon's definition.

Exercise 17
Suppose that $Enc : K \times M \to M$ is a perfectly secure encryption scheme, with corresponding decryption algorithm Dec. Show that we must have $|K| \geq |M|$.

Exercise 18
Prove the following equivalence:

$$independance + H(m|c) = H(m) \Leftrightarrow Pr(m = m'|c = c') = Pr(m = m')$$

Exercise 19
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 20
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, it means that $Pr[D2(X) = 1] - Pr[D2(Y) = 1]$ is negligible. (Assume that the two inputs have the same size) Knowing that $X = \{X_n\}$ and $Y = \{Y_n\}$ are 2 ensembles.

Exercise 21
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 22
Recall that the distributions D_0, D_1 are said to be ϵ-indistinguishable 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.)