SET 1

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

(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 $X_1, ..., X_n$ 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:

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

**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 \(C(N, q) \geq (1 - \frac{1}{e}) \cdot \frac{q(q-1)}{N}\). 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. \(f\cdot g\) 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 \(f(n) := n^{-\log n}\) 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 \( DDH \leq CDH \leq DL \)

Exercise 15
Prove that

\[
\text{Adv}_{S,A}(\eta) = Pr[b' \leftarrow \text{Ind}^1(A) : b' = 1] - Pr[b' \leftarrow \text{Ind}^0(A) : b' = 1] = 2Pr[b' \leftarrow \text{Ind}^b(A) : b' = b] - 1
\]

where given an encryption scheme \( S = (K, E, D) \). An adversary is a pair \( A = (A_1, A_2) \) of polynomial-time probabilistic algorithms, \( b \in \{0, 1\} \). Let \( \text{Ind}^b(A) \) be the following algorithm: Generate \( (pk, sk) \leftarrow K(\eta) \); \((s, m_0, m_1) \leftarrow A_1(\eta, pk)\); Sample \( b \leftarrow \{0, 1\} \); \( b' \leftarrow A_2(\eta, pk, s, E(pk, m_b)) \); return \( b' \)

Exercise 16
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 17
Prove that OTP is perfectly secure according Shannon’s definition.

Exercise 18
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 19
Prove the following equivalence:

\[
\text{independance} + H(m|c) = H(m) \Leftrightarrow Pr(m = m'|c = c') = Pr(m = m')
\]

Exercise 20
Prove that under CDH assumption El-Gamal is OW-CPA.

Exercise 21
Prove that if there is an adversary which can break DDH then there is an adversary which can break the IND-CPA security of El-Gamal.
Exercise 22
Prove that under DDH assumption El-Gamal is IND-CPA.

Exercise 23
Define the \(n\)-DDH problem as follows: on input \((A = g^a, (B_1 = g^{b_1}, C_1 = g^{c_1}), \ldots, (B_n = g^{b_n}, C_n = g^{c_n}))\), determine if for all \(i, c_i = ab_i\) or if for all \(i, c_i\) is randomly distributed.
Show that the \(n\)-DDH problem is intractable if and only if the DDH problem is intractable.

Exercise 24
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 25
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 26
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 27
Recall that the distributions \(D_0, D_1\) are said to be \(\epsilon\)-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.)

Exercise 28
Show that the straightforward application of the RSA function is not an IND-CPA encryption scheme. That is, the encryption function \(E_{(n,e)}(m) = m^e \mod n\) is not an IND-CPA encryption scheme.

Exercise 29
We define the \(n\)-IND-CPA game as follows: Given an encryption scheme \(S = (K, E, D)\), an \(n\)-IND-CPA adversary is a tuple \(\mathcal{A} = (A_1, A_2, \ldots, A_{n+1})\) of probabilistic polynomial-time algorithms. For \(b \in \{0, 1\}\), define the following game.

\(n - IND^b - CPA\):
• Generate \((pk, sk) \leftarrow K(\eta)\)

• \((s_1, m_{1,0}, m_{1,1}) \leftarrow A_1(\eta, pk)\)

• \((s_2, m_{2,0}, m_{2,1}) \leftarrow A_1(\eta, pk, s_1, E(pk, m_{1,b}))\)

• \(\ldots\)

• \(b' \leftarrow A_{n+1}(\eta, pk, s_n, E(pk, m_{n,b}))\)

• return \(b'\)

Define \(Adv_{S,A}^{n-\text{IND-CPA}} = \text{Pr}[b' \leftarrow n-\text{IND}^1-\text{CPA} : b' = 1] - \text{Pr}[b' \leftarrow n-\text{IND}^0-\text{CPA} : b' = 1]\).

Show that an encryption scheme is \(n\)-IND-CPA secure if and only if it is IND-CPA secure.

**Exercise 30 (Midterm 2008)**

1. Give the definition of NM-CPA NM-CCA1 and NM-CCA2.

2. Justify informally the implication relations between these three notions.

**Exercise 31 (Midterm 2008)**

We propose a modified version of El-Gamal encryption scheme. Consider the following scheme, where \(g_1, g_2\) are two randomly-chosen generators in \(G\) a cyclic group:

**KeyGen(1^k):**

\(x, y \leftarrow Z_q;\)

\(h = g_1^x g_2^y;\)

\(PK = (g_1, g_2, h);\)

\(SK = (x, y);\)

output \((PK, SK)\);

**E(PK, m):**

\(r \leftarrow Z_q;\)

output \(<g_1^r, g_2^r, h^r * m>\);

**D(SK, u, v, e):**

output \(\frac{e^v}{u^v};\)

1. Correctness: Assuming an honest execution of the protocol, prove that \(\frac{e^v}{u^v} = m\)

2. Prove that the modified scheme is semantically (IND-CPA) secure under the DDH assumption (Only the reduction as in exercises session).

Recall: DDH is given \((g, g^u, g^v, \alpha)\) guess whether \(\alpha\) is \(g^{uv}\) or \(g^r\) where \(r\) is a random value.

Hint: one can take \(g_1 = g\) and \(g_2 = g^u\).

**Exercise 32 (Midterm 2010)**

Let \(E\) be an NM-CCA2 secure encryption scheme. We modify this scheme into \(E'(m) = E(m) || h(m)\), where \(h\) is a public hash function. This should help the user to detect some errors in the transmission of the messages.
• Give the definition of NM-CCA2

• Prove that the new scheme $E'$ is not IND-CPA. It means give an attack against IND-CPA for $E'$.

**Exercise 33 (Final 2009)**
Let $E$ be an IND-CCA2 secure encryption scheme. We modify this scheme into $E'(m) = E(m) || h(m)$, where $h$ is an hash function. This should help the user to detect some errors in the transmission of the messages. Prove that the new scheme $E'$ is not IND-CPA. It means give an attack against IND-CPA for $E'$.

**Exercise 34 (Final 2009)**
Zheng & Seberry in 1993 proposed the following encryption scheme:

$$f(r) || (G(r) \oplus (x || H(x)))$$

where $x$ is the plain text, $f$ is a one way trap-door function (like RSA), $G$ and $H$ are two public hash functions, $||$ denotes the concatenation of bitstrings and $\oplus$ is the exclusive-or operator.

• Give the associated decryption algorithm.

• Give an IND-CCA2 attack against this scheme.

  Hint: you cannot ask the cipher of $m_b$ to the decryption oracle, but a cipher of $m_\overline{x}$ is not forbidden...

**Exercise 35 (Final 2010)**
Consider a naïve modified version of RSA with public parameter $(e,n)$ defined by: $E(x) = (v,w)$ where $k$ is a random number $v = k^e \mod n$ and $w = x \ast k$.

1. Show that you can extract $x^e \mod n$ from $e$ and the encryption $(v,w)$ of an unkown message $x$.

2. Find an IND-CPA attack against this encryption scheme.

**Exercise 36 (Final 2010)**
We consider random version of RSA proposed by David Pointcheval. Encryption of the message $m$ is $D - RSA(n,e)(m) = (a,b)$ where $a = k^e \mod n$, $b = (k+1)^e \times m \mod n$ and $k$ is a random number.

• Give the decryption algorithm

• We define the Computational D-RSA problem (CD-RSA) by:
  Given $(n,e)$, and $a^e \mod n$
  Find $(a + 1)^e \mod n$

Prove that under CD-RSA assumption then D-RSA is OW-CPA.
• We define the Decisional D-RSA problem (DD-RSA) by Given \((n, e)\), \(r^e \mod n\) and \(s^e \mod n\)

Decide if \(s = r + 1 \mod n\)
Prove that under DD-RSA assumption then D-RSA is IND-CPA.

**Exercise 37**
Find an attack on CBC encryption with counter IV, (proving that this encryption mode is not IND-CPA secure). In this scheme the first IV used is 0 and for generating the next IV we just increase by one the value of the previous IV.

**Exercise 38**
Prove that CTR is not IND-CCA2 secure.

**Exercise 39**
Prove that CFB is not IND-CCA2 secure.

**Exercise 40**
Prove that OFB is not IND-CCA2 secure.

**Exercise 41**
Prove that CBC with random IV is not IND-CCA2 secure. This time IV is a random number. But notice that this mode is IND-CPA secure.

**Exercise 42**
Suppose that \(E_1\) and \(E_2\) are symmetric encryption schemes on strings of arbitrary length. Show that the encryption scheme defined by \(E'(k_1, k_2, m) = E_2(k_2, E_1(k_1, m))\) (for randomly sampled keys \(k_1\) and \(k_2\)) is IND-CPA secure if either \(E_1\) or \(E_2\) is IND-CPA secure.

**Exercise 43**
Let BadMac, be the message authentication code defined as follows:

\[
\text{BadMac}((k_1, k_2), m_1 | \ldots | m_n) \\
c_0 = 1; \\
\text{for } i = 1 \text{ to } n, \text{ do:} \\
z_i = c_{i-1} \cdot m_i \mod 2^{128}; \\
c_i = z_i + k_1 \mod 2^{128}; \\
\text{out} = E_{k_2}(c_n); \\
\text{Output out};
\]

Show that BadMac is not a secure message authentication code.

**Exercise 44**
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. \(A \rightarrow B : \{N_b\}^{pk(B)}\)
Exercise 45 (Midterm 2008)
Prove that any deterministic symmetric encryption scheme is IND-CPA insecure.

Exercise 46 (Final 2008)
Let $E : \{0,1\}^k \times \{0,1\}^l \rightarrow \{0,1\}^l$ be a secure block cipher. Let $K$ be the key-generation algorithm that returns a random $k$-bit string as the key $K$. Let $E$ be the following encryption algorithm:

\[
\text{Algorithm } E_K(M) \\
\text{If } |M| \text{ is not a positive multiple of } l \text{ then return FALSE} \\
\text{Divide } M \text{ into } l \text{ bit blocks, } M = M[1] \ldots M[n] \\
P[0] \leftarrow \{0,1\}^l; C[0] \leftarrow E_K(P[0]) \text{ For } i = 1, \ldots, n \text{ do} \\
P[i] \leftarrow P[i-1] \oplus M[i]; \ \\
C[i] \leftarrow E_K(P[i]); \ \\
\text{EndFor} \\
C \leftarrow C[0]C[1] \ldots C[n]; \\
\text{Return } C
\]

1. Specify a decryption algorithm $D$ such that $\mathcal{SE} = (K; E; D)$ is a symmetric encryption scheme with correct decryption. We are denoting the inverse of $E_K$ by $E^{-1}_K$.

2. Show that this scheme is insecure by presenting a practical adversary IND-CPA. Say what is the advantage achieved by your adversary.

Exercise 47 (Midterm 2010)
Let $(E, D)$ be a block cipher using a symmetric encryption $E_k$ with a symmetric key $k$. Let $m_1, m_2, \ldots, m_t$ be a sequence of $t$ plaintext blocks. We consider the following block cipher mode which produce $t+2$ ciphertext blocks $c_0, c_1, c_2, \ldots, c_t, c_{t+1}$ which satisfies the equation, for $i = 1, \ldots, t$.

\[ c_i = E_k(c_{i-1} \oplus m_i \oplus c_{i+1}) \]

1. Describe how to reconstruct $m_1, \ldots, m_t$ given $c_0, \ldots, c_{t+1}$.

2. Find a way to compute effectively this encryption mode knowing that in order to get started, we set $c_0$ and $c_1$ to some fixed initialization vectors.

3. Assuming that decrypting or encrypting twice a message gives the message again ($D_k(D_k(x)) = x, E_k(E_k(x)) = x$) and that an intruder can fix $c_0$ and $c_1$ then find an IND-CPA attack against this scheme.