

COM S 687 : Introduction to Cryptography

Homework 1

Instructor: Rafael Pass TA: Muthu Venkitasubramaniam

Due Date: Thursday, 7th September 2006

August 24, 2006

You are free to collaborate with other students on the homework, but you must turn in your own individually written solution and you must specify the names of your collaborators. Additionally, you may make use of published material, provided that you acknowledge all sources used. Note that it is a violation of this policy to submit a problem solution that you are unable to explain orally to a member of the course staff.

Solutions will be posted in CMS. Submit hardcopy in class or to Muthu by the due date, or a .pdf, .ps, .doc, or .txt file in CMS. Problem sets must be typed.

1. Let X and Y be two independent random variables. Prove the following facts.

(a) $E[XY] = E[X]E[Y]$

(b) $\text{Var}[X+Y] = \text{Var}[X] + \text{Var}[Y]$.

Give examples when X and Y are not independent and equalities (a) and (b) do not hold.

2. Let r_1, r_2, \dots, r_k be n -bit strings picked uniformly at random. For any subset S of $\{1, 2, \dots, k\}$, define a random variable $z_S = \oplus_{i \in S} r_i$. Prove that the set of random variables $\{z_S | S \subset \{1, 2, \dots, k\}\}$ are pairwise independent.
3. Let X_1, X_2, \dots, X_n be random variables that are pairwise independent. Further, for all i , let $E[X_i] = \mu$ and $\text{Var}[X_i] = \sigma^2$

- (a) Show that,

$$\Pr \left[\left| \frac{\sum X_i}{n} - \mu \right| \geq \epsilon \right] \leq \frac{\sigma^2}{n\epsilon^2}$$

Note that this is a Chernoff like bound when the random variables are only pairwise independent. (Hint: Use Chebyshev's inequality)

- (b) Suppose, further that the random variables assume the values only 1 and -1. Show that the inequality can be simplified to,

$$Pr \left[\left| \frac{\sum X_i}{n} - \mu \right| \geq \epsilon \right] \leq \frac{1 - \mu^2}{n\epsilon^2}$$

4. The cryptographers at secure-encryption.com have come up with an encryption scheme using secret keys. This scheme has a known vulnerability that an attacker, given a random message $m \in \mathcal{M}$ and its encryption, can guess for any i , the i^{th} bit of the secret key with probability $\frac{1}{2} + \epsilon$.

Let us suppose the attacker gains access to k such messages m_1, m_2, \dots, m_k with its encryption.

- (a) If the messages m_1, \dots, m_k are known to be independent, show that the attacker can find any bit of the secret key with very high probability (Hint: Use Chernoff bound). Using the union bound, find a lower bound on the probability of the attacker guessing the entire secret key, if the key is made up of n bits.
 - (b) Find the number of messages required to guess the entire key with 99% probability when $\epsilon = 0.0001$ and $n = 1024$.
 - (c) In real life, it is hard for the messages to be independent. Repeat parts (a) and (b) if the messages are known to be only pairwise independent. (Hint: Use Problem 3)
5. Consider the following private key encryption system. Let p be a prime number that is known by everyone. Alice and Bob share three numbers $a, b \neq 0$ and x_0 . To send a sequence of messages $\langle m_1, m_2, \dots, m_k \rangle$, Alice does the following
- Computes $x_i = a \cdot x_{i-1} + b \bmod p$ for $1 \leq i \leq k$.
 - Computes $c_i = m_i + x_i \bmod p$.
 - Sends $\langle c_1, c_2, \dots, c_k \rangle$.

Note that this is a stateful encryption scheme, that is, Alice (Bob) has to keep track of the number of messages sent to encrypt (decrypt) a subsequent message.

- (a) Complete the description of this scheme by defining the following formally.
 - Message space.
 - Key space.
 - Encryption and Decryption algorithm.
- (b) Prove that it is a private key encryption system

- (c) Is it possible to find the key, given a sequence of random messages $\langle m_1, m_2, \dots, m_k \rangle$ and their corresponding encryptions? If so, determine an upper bound on the number of messages and also propose a "fix" for the scheme that at least handles your attack.
6. Try to formalize what it means for the "match-making" card game presented in class to be secure. Decide on what properties are desired. Provide explicit assumptions and prove that the game satisfies the desired properties under your assumptions.