

COMS W4261: Introduction to Cryptography.

Instructor: Tal Malkin

Problem Set 1

Due: Thur 10/1/09, by the beginning of class (preferably earlier by email)

Reading: Chapters 1,2

1. In this problem you are asked to design two encryption schemes – one completely insecure, and the other perfectly secret – satisfying certain properties. These constructions may seem artificial, but they demonstrate an important point that is relevant also for natural, real life schemes.

For parts (a) and (b) you should define your constructed scheme (GEN, ENC, DEC) and the message space \mathcal{M} , and argue intuitively (without formal proof) why this construction satisfies the conditions of the problem.

- (a) Give an example of a (bad) private-key encryption scheme, where from seeing the ciphertext Eve can always recover the corresponding plaintext, yet she can gain no information whatsoever about the key.
 - (b) Give an example of a perfectly secure private-key encryption scheme, where from seeing a ciphertext Eve can learn most bits of the key.
 - (c) What is the lesson that can be learned from the above examples?
2. In class we saw several definitions of perfect secrecy, capturing different intuitions, and claimed that they are all equivalent – here you will prove some of these equivalences.

Recall that our first definition (corresponding to Definition 2.1 in the text) captured the idea that the ciphertext does not contain any information about the message (seeing the ciphertext does not give anything to the adversary). Our second definition (Lemma 2.3 in the text) captured the idea that any two messages have encryptions that are distributed the same way. Our third definition was the following (we will call it perfect indistinguishability):

Definition A private key encryption scheme (GEN, ENC, DEC) over \mathcal{M} is *perfectly indistinguishable* if for every adversary \mathcal{A} and for every pair of messages $m_0, m_1 \in \mathcal{M}$, it holds that

$$\Pr[A(\text{ENC}_k(m_0)) = 1] = \Pr[A(\text{ENC}_k(m_1)) = 1]$$

where probability is taken over the key generation algorithm, and any randomness used by ENC or A.

Your assignment: Prove that a private key encryption scheme is perfectly indistinguishable if and only if it is perfectly secret.

3. We saw that the one-time-pad achieves perfect security, and works for any message space M of size 2^n for some n , using a key space K of the same size 2^n (each message is represented as an n -bit string, the key is also an n -bit string, and the encryption is their exclusive or). This is also the best we can hope to achieve, by Shannon's theorem discussed in class. In this problem we consider a small message space consisting of 3 messages $M = \{0, 1, 2\}$. Note that the size of the message space here is not a power of 2.
- (a) Consider the following encryption scheme for M . Represent each message using 2 bits, namely 0 is encoded as 00, 1 is encoded as 01, and 2 is encoded as 10. Let the key space $K = \{0, 1\}^2$, namely all 2-bit strings. Now the encryption of a message m using a key k is $m \oplus k$ (with the obvious decryption).
Is this a perfectly secure encryption scheme? Prove your answer.
- (b) Design a perfectly secure encryption scheme over M which has a key space K of size 3 (namely the smallest possible, by Shannon's theorem).