

COMS W4261: Introduction to Cryptography.

Instructor: Tal Malkin

Problem Set 1

Due: Thur 9/22/11, by the beginning of class (or earlier by email)

Reading: Chapters 1,2

1. (15 points) Consider the following variation on the one time pad. Let $n \geq 2$ be some integer. Our message space will be $\mathcal{M} = \{0, \dots, n-1\}$.¹ Now define (GEN, ENC, DEC) as follows.

GEN: output a uniformly random $k \in \{0, \dots, n-1\}$.

$$\text{ENC}_k(m) = k + m \pmod n$$

$$\text{DEC}_k(c) = c - k \pmod n$$

Prove that this scheme is perfectly secret.

2. (30 points) We discussed in class how one-time-pad, while achieving perfect secrecy (against a passive eavesdropping adversary), can be vulnerable to other attacks in different threat models. In particular, given a ciphertext encrypting some message, it is easy to generate an encryption of a related message. For example, using the variant in Problem 1, given an encryption of some m , even though m remains perfectly secret, it is easy to generate an encryption of $m + 1$ (verify that you see how to do it). We also discussed why this can be a problem for security in some application scenarios.

Your Assignment: Come up with a definition of “perfectly non-malleable” encryption scheme, capturing the intuitive requirement that an encryption of a message m cannot be used towards generating an encryption of a related message $f(m)$. Give both a formal definition, and the intuition/motivation behind your choices. It may help to use the adversarial style definition, thinking about the power of the adversary in such a setting, and what security game (experiment) with the adversary captures this.

3. (40 points) Come up with a perfectly secret and perfectly non-malleable encryption scheme. Prove that your scheme satisfies both perfect secrecy (according to one of the definitions we saw in class), and perfect non-malleability (according to the definition you proposed in the previous problem).
4. (15 points) On the other hand, can you think of application scenarios where in fact we want encryption to be malleable? That is, cases where it is useful to have an encryption scheme with the property that given an encryption of m , one can compute an encryption of a related message $f(m)$ (while maintaining the secrecy of m). Please discuss when this capability may be useful.

¹If you want your message space to be strings in $\{0, 1\}^\ell$, you can just choose $n \geq 2^\ell$ and treat your message as a binary representation of an integer $< n$.