ICS 268: Cryptography and Communication Security 9/28/2004

Homework 1

Due Tuesday, 10/5/2004, at the beginning of the class

1 Substitution cipher

Have a look at the substitution cipher in Lecture Notes 1 (section 3.3) and recall the definition of perfect secrecy. Prove that the substitution cipher is perfectly secure for the special case of $\ell = 1$, and that it it is *not* perfectly secure if $\ell \geq 2$.

2 OTP cipher variations

Notation: We will denote by $\mathcal{A}^n$ a set of n-long sequences of symbols $A_1 A_2 \ldots A_n$ where each A_i is an element of $\mathcal{A}$. For example, taking $\mathcal{A} = \{0,1\}$, we will write $\{0,1\}^n$ to denote a set of all n-long binary strings.

We showed that One-Time Pad encryption satisfies perfect secrecy if $\mathcal{M} = \mathcal{K} = \{0,1\}^\ell$, for any ℓ. In this exercise we will look at variations of the OTP cipher, where the messages and/or keys are not any binary strings. For example, consider set $\mathcal{S}$ of three 2-bit strings, $\mathcal{S} = \{00, 01, 10\}$.

Consider the following three variations on the OTP cipher. In all these variations the key generation algorithm chooses $k \in \mathcal{K}$ uniformly, and encryption and decryption work as in OTP, i.e. $Enc(k,m) = k \oplus m$ and $Dec(k,c) = k \oplus c$.

Consider the following three OTP variants:

1. Let $\mathcal{M} = \mathcal{S}^\ell$ and $\mathcal{K} = \{0,1\}^{2\ell}$. In this way both the message and the key are (2ℓ)-long bit strings, but not every (2ℓ)-bit string can be a valid message. For example, for $\ell = 3$, we could have $m = [00, 01, 00] = 000100$ but $m = [11, 00, 11] = 110011$ is not in $\mathcal{M}$ because $11 \notin \mathcal{S}$.
2. Let $\mathcal{M} = \{0,1\}^{2\ell}$ and $\mathcal{K} = \mathcal{S}^\ell$
3. Let $\mathcal{M} = \mathcal{K} = \mathcal{S}^\ell$. *[[Hint: This one is actually* not *perfectly secure...]]*

For each of these OTP variants do the following: (1) Say what the space $\mathcal{C}$ of the ciphertexts is, and note the *sizes* of the message space $\mathcal{M}$ and key space $\mathcal{K}$; and (2) Say whether the resulting cipher is perfectly secure or not, and **prove your answer**.

Do the sizes of the key space and the message space correlate in any way with whether or not the cipher is secure? Explain how and why.

3 Perfect Secrecy implies Shannon Secrecy [bonus]

Prove that if an encryption scheme is perfectly secret than it must also be secret in Shannon's sense.