ICS.202: Introduction to Applied Cryptography 9/28/2016

Homework 1

Due Wednesday, 10/5/2016, at the beginning of the class

Notation: If a is a string then $|a|$ denotes its length. For example $|ab| = 2, |abcd| = 4, |01| = 2, |010| = 3$, etc. If a, b are strings then $a|b$ denotes a concatenation of a and b, i.e. a string of length $|a| + |b|$ whose prefix is a and postfix is b. Let $a_{[i,j]}$ denote a substring of a from the i-th to the j-the character. For example $a_{[1,|a|]}$ is the string a itself, and if $a = b|c$ then $a_{[1,|b|]} = b$ and $a_{[|b|+1,|a|]} = c$. We use a_i to denote the i-th character in string a, so for example $a_1|a_2|a_3 = a_{[1,3]}$ and $a_1|a_{[2,3]} = a_{[1,3]}$. For any set $\mathcal{S}$, we use $\mathcal{S}^n$ to denote a set of n-long sequences $a_1 a_2 \dots a_n$, where each a_i is an element of $\mathcal{S}$. For example $\{0,1\}^n$ is the set of n-long binary strings, which is the case of the above notation for $\mathcal{S} = \{0,1\}$.

1 OTP Cipher Variants

1.1 Let $\mathcal{S} = \{00, 01, 10\}$. Note that $\mathcal{S}$ is a set of 2-bit strings with string 11 missing. Consider the following three OTP variants. For each of these OTP variants state whether the resulting cipher is *perfectly secure* or not, and **prove your answer**. In other words, if your answer is "yes", prove that the cipher passes Shannon's perfect secrecy criterion (or any equivalent formulation of secrecy), and if your answer is "no" then show that the cipher fails this criterion. In each case below the encryption and decryption procedures are as in OTP, i.e. encryption outputs a bitwise xor of the key and the message and decryption outputs a bitwise xor of the key and the ciphertext.

(a) Take any integer ℓ and define $\mathcal{M} = \mathcal{S}^\ell$ and $\mathcal{K} = \{0,1\}^{2\ell}$. In other words, the message and the key are both (2ℓ)-long bit strings, but not every (2ℓ)-bit string is a valid message. For example, for $\ell = 3$, 000100 is in $\mathcal{M}$, but 110011 is not in $\mathcal{M}$ because $11 \notin \mathcal{S}$.

(b) Let $\mathcal{M} = \{0,1\}^{2\ell}$ and $\mathcal{K} = \mathcal{S}^\ell$

(c) Let $\mathcal{M} = \mathcal{K} = \mathcal{S}^\ell$.

Hint: You can do the above exercise just for $\ell = 1$, because in each case the solution to the general case of any $\ell \geq 1$ follows immediately from the solution for the $\ell = 1$.

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

2 Substitution Cipher and Perfect Secrecy

Recall the *Substitution Cipher*. Let A be the set of 26 English alphabet letters, $A = \{a, b, ..., z\}$. Recall that in this cipher we have $C = M = A^\ell$ for some integer ℓ, and that a key k is a permutation on the set A, i.e. it's a one-to-one function mapping A to itself. Notice that if K is a space of all such keys, i.e. permutations on A, then $|K| = |A|! = 26!$. Recall that if Enc is the substitution cipher then $Enc(k, m)$ for $m = m_1|...|m_\ell$ in $M = A^\ell$

outputs $c = c_1|...|c_\ell$ where for all i we have $c_i = k(m_i)$, i.e. permutation k applied to m_i (recall that permutation is a function, so $k(x)$ stands for the value of the permutation k at argument x).

(a) Show that the substitution cipher is perfectly secret if $\ell = 1$.

(b) Show an explicit attack on the perfect secrecy for $\ell = 2$, where $C = M = A^2$, i.e. if you use it to encrypt two-letter words. An "explicit attack" on perfect secrecy a pair of messages m_0, m_1 in M and a ciphertext c that show that perfect secrecy is violated, i.e. which satisfy that

$$\Pr_{k \leftarrow K}[Enc(k, m_0) = c] \neq \Pr_{k \leftarrow K}[Enc(k, m_0) = c] \quad (1)$$

(c) What does this mean that this pair (m_0, m_1) violates perfect secrecy in practice? In other words, why would this be a reason *not* to use this cipher on $M = A^2$?

(d) Assume that you can modify substitution cipher by changing *only* the message space M on which it will be executed. (In other words, consider the key space and the way the encryption and decryption work to be fixed.) Find the *largest* message space M on which the substitution cipher is perfect. (Since M is a set, "largest" means "containing the maximum number of elements".) Justify your answer, i.e. argue that (1) the substitution cipher is perfectly secure on M which you provided, and that (2) this is the largest M for which subsitution cipher can achieve perfect secrecy.

Hint: M is a subset of A^ℓ for some ℓ. Describe what that subset is and how many elements it has. By the theorem we showed in class, you know that for perfect secrecy to be possible the message space M must satisfy that $|M| \leq |K|$. We also know that $|K| = 26!$, and the two facts tell us that the largest message space M on which this cipher can be perfectly secure cannot contain more than $26!$. But is there some space M which is so large and on which this cipher is perfectly secure? If so, describe what that set M is, and prove that a substitution cipher is perfectly secure on M.

3 Two-Time Pad (TTP) Encryption

Let TTP be a variant of the OTP encryption where $M = C = \{0,1\}^{2n}$, $K = \{0,1\}^n$, and $Enc(k, m)$ outputs $c = m \oplus [k|k]$, i.e. it's like an OTP with key k' formed by concatenating two copies of k. Show an *explicit attack* on perfect secrecy of TTP, i.e. show two messages m_0, m_1 in M and a ciphertext c which show that perfect secrecy is violated.[1]

4 Relaxed Encryption Correctness or Secrecy

1. Do exercise 2.11 in Katz-Lindell (2nd edition). The same exercise has number 2.12 in the *1st edition* of the Katz-Lindell textbook.
2. (**bonus problem**) Do exercise 2.12 in Katz-Lindell (same exercise has number 2.13 in the 1st edition of Katz-Lindell).

[1] It is true that $|M| = 2^{2n}$ and $|K| = 2^n$, hence $|M| > |K|$, and hence TTP cannot satisfy perfect secrecy. However, we still want you to provide us with an explicit example that violates perfect secrecy, i.e. some triple (m_0, m_1, c) which satisifies inequality (1).