CIS 5371 Cryptography

Home Assignment 2 with Answers

Due: At the beginning of the class on February 18, 2016

Exercises taken from the course textbook, Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography.

- **Prove or refute:** Every encryption scheme for which the size of the key space equals the size of the message space, and for which the key is chosen uniformly from the key space, is perfectly secret.

**Solution:** This is false. Let the key space and message space be the set of \( \ell \)-bit strings, and consider the encryption scheme defined by choosing a random key and setting \( \text{Enc}_k(m) = k || m \) (where \( || \) denotes concatenation). This scheme fulfills the requirements of the exercise but is not secret at all; the plaintext is always the last \( \ell \)-bits of the ciphertext.

- Assume that we require only that an encryption scheme (not secret at all; the plaintext is always the last \( |m| \)) when the adversary is not restricted to output equal-length messages in experiment \( \ell \) of length at most \( |K| \geq |M| \cdot 2^{-t} \). (This probability is taken over choice of \( k \) as well as any randomness that may be used during encryption or decryption.) Show that perfect secrecy (as in Definition 2.1) can be achieved with \( |K| < |M| \) when \( t \geq 1 \). Can you guess a lower bound on the required size of \( K \)?

**Solution:** Let \( K = \{0, 1\}^t \) and \( M = \{0, 1\}^{t+t} \). The key-generation algorithm chooses a uniform string from \( K \). To encrypt a message \( m \in M \) using key \( k \), let \( m' \) denote the first \( \ell \)-bits of \( m \) and output \( c := m' \oplus k \) (both \( m' \) and \( k \) have length \( \ell \)). To decrypt a ciphertext \( c \) using key \( k \), choose a random string \( r \leftarrow \{0, 1\}^{\ell} \) and output \( m := (c \oplus k) \oplus r \). Note that \( \text{Pr}[\text{Dec}_k(\text{Enc}_k(m)) = m] = 2^{-t} \) because decryption is correct if and only if the random string \( r \) chosen during decryption happens to equal the last \( t \) bits of \( m \) (and this occurs with probability \( 2^{-t} \)). Perfect secrecy of this scheme follows from the proof of the one-time pad (indeed, this is exactly a one-time pad on the first \( \ell \)-bits of the message).

**Lower bound:** \( |K| \geq |M| \cdot 2^{-t} \).

- Say \( \Pi = (\text{Gen}, \text{Enc}, \text{Dec}) \) is such that for \( k \in \{0, 1\}^n \), algorithm \( \text{Enc}_k \) is only defined for messages of length at most \( \ell(n) \) (for some polynomial \( \ell \)). Construct a scheme satisfying Definition 3.8 even when the adversary is not restricted to output equal-length messages in experiment \( \text{PrivK}^\text{cav}_{A, \Pi} \).

**Solution:** To be clear, we are considering a modification of experiment \( \text{PrivK}^\text{cav}_{A, \Pi} \) where the adversary \( A \) is not required to output \( m_0 \) and \( m_1 \) of the same length, but instead it is only required that \( m_0 \) and \( m_1 \) each have length at most \( \ell(n) \).

Let \( \Pi' = (\text{Gen}', \text{Enc}', \text{Dec}') \) be a scheme that is secure with respect to the original Definition 3.8 (for messages of equal length). Construct a scheme \( \Pi'' = (\text{Gen}', \text{Enc}', \text{Dec}') \).

(a) \( \text{Gen}' \) is identical to \( \text{Gen} \).

(b) Upon input a plaintext message \( m \) of length at most \( \ell = \ell(n) \) (where \( n \) is the length of the key), \( \text{Enc}' \) first sets \( m' := 0^{\ell-|m|-11} || m \) and then encrypts \( m' \) using \( \text{Enc} \). Note that \( m' \) is always exactly \( \ell(n) \) bits long.

(c) \( \text{Dec}' \) applies \( \text{Dec} \) to the ciphertext, and parses the result as \( 0^{\ell+1} || m \) for \( t \geq 0 \). It outputs \( m \).

It is clear that if \( \Pi \) satisfies Definition 3.8 then \( \Pi'' \) satisfies the modified definition.

A complete answer to this exercise requires a proof showing that the existence of an adversary \( A' \) with respect to the modified definition implies the existence of an adversary breaking \( \Pi' \) with respect to Definition 3.8.

We describe the reduction informally. Given an adversary \( A' \) who breaks \( \Pi' \), we construct an adversary \( A \) who takes the pair of plaintexts \( m_0, m_1 \) output by \( A' \) and pads them in the same way as \( \text{Enc}' \) would. Then, it outputs the padded messages to be encrypted. Observe that \( A \) outputs equal-length messages, as required. Furthermore, if \( A' \) can correctly guess \( b \) with probability non-negligibly greater than 1/2, then this guess will also be correct for \( A \) with the same probability. This proof sketch can easily be extended to a full proof.

Mike Burmester