CSA E0 235: Cryptography 09/08/2019

Tutorial 1

Instructor: Arpita Patra *Question Set*

Question 1 Assume an attacker knows that a user's password is either **abcd** or **bedg**. Say the user encrypts his password using the shift cipher, and the attacker sees the resulting ciphertext. Show that how the attacker can determine the user's password, or explain why this is not possible.

Question 2 Show that the shift, substitution and Vigenère cipher are all trivial to break using a chosen-plaintext attack. How much chosen plaintext is needed to recover the key for each of the ciphers?

Question 3 When using the one-time pad with the key $k = 0^l$, we have $\mathbf{Enc}_k(m) = k \oplus m = m$ and the message is sent in the clear! It has therefore been suggested to modify the one-time pad by only encrypting with $k \neq 0^l$ (i.e. to have **Gen** choose k uniformly from the set of *nonzero* keys of length l). Is this modified scheme still perfectly secure? Explain.

Question 4 Let, $\mathcal{E} = (E, D)$ be a perfectly secure cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ where $\mathcal{K} = \mathcal{M}$. Let $\mathcal{E}' = (E', D')$ be a cipher where encryption is defined as $E'_{(k_1,k_2)}(m) = (E_{k_1}(k_2), E_{k_2}(m))$. Show that $\mathcal{E}'$ is perfectly secure.

Question 5 Prove that if only a single character is encrypted, then the shift cipher is perfectly secret.