HIT — Cryptography — Homework 1

September 4, 2014

Problem 1. Show that the shift, Mono-Alphabetic sub., and Vigenère ciphers are all trivial to break using a known-plaintext attack. How much known plaintext (how many characters) is needed to completely recover the key for each of the ciphers? (show how to break the cipher)

Problem 2. Show that the shift, Mono-Alphabetic sub., and Vigenère ciphers are all trivial to break using a chosen-plaintext attack. How much plaintext (how many characters) must be encrypted to completely recover the key? (show your chosen plaintext)

Problem 3. Prove or refute: For every encryption scheme that is perfectly secret it holds that for every distribution over the message space $\mathcal{M}$, every $m, m' \in \mathcal{M}$, and every $c \in \mathcal{C}$:

$$\Pr[M = m|C = c] = \Pr[M = m'|C = c].$$

Problem 4. Study conditions under which the shift, mono-alphabetic sub., and Vigenère cipher ciphers are perfectly secret:

- (a) Prove that if only a single character is encrypted, then the shift cipher is perfectly secret.
- (b) What is the largest plaintext space M you can find for which the mono-alphabetic sub. cipher provides perfect secrecy?
- (c) Show how to use the Vigenère cipher to encrypt any word of length t so that perfect secrecy is obtained (note: you can choose the length of the key). Prove your answer.

Problem 5. In the one-time pad encryption scheme, it can sometimes happen that the key is the all-zero string. In this case, the encryption of a message m is given by $m \oplus 0^l = m$ and therefore the ciphertext is identical to the message!

- (a) Do you think the one-time pad scheme should be modified so that the all-zero key is not used? Explain.
- (b) Explain how it is possible that the one-time pad is perfectly secure even though the above situation can occur with non-zero probability.