Internet Infrastructure Security (COMP444)

A1

Due at 11:55pm on 5 February 2015
Submission site: `https://submit.comp.polyu.edu.hk/`

Rocky K. C. Chang

January 30, 2015

1. `[6 marks]` (Triple Shift and Affine Ciphers) Inspired by the triple DES, a COMP444 student proposes to strengthen the security of the classic ciphers by applying multiple encryptions.

   (a) `[3 marks]` For example, instead of encrypting m once using a Shift Cipher, he proposes to encrypt m three times using Shift Cipher with three different keys k_1, k_2, and k_3. Will this triple Shift Cipher increase the security of the ordinary Shift Cipher?

   (b) `[3 marks]` Repeat part (a) for Affine Cipher. The three different keys are (a_1, b_1), (a_2, b_2), and (a_3, b_3).

2. `[6 marks]` (A stream cipher) A stream cipher generates a key stream and encrypts a message by exclusive-ORing it with the key stream. The receiver side also generates the same key stream to decrypt the message by performing exclusive-OR.

   Consider the following stream cipher. The key stream is given by $k_0, k_1, k_2, \cdots$. The values of k_0 is initialized by an IV, whereas other k_is are generated by an encryption function $E()$.

$$\begin{aligned} k_0 &= IV \\ k_i &= E(k, k_{i-1}),\ for\ i \geq 1 \\ c_i &= p_i \oplus k_i \end{aligned}$$

   One major problem with this cipher is that two different messages using the same IV will have the same key stream. Consider that two different plaintexts P and P' are encrypted by the same key stream and they produce ciphertexts C and C', respectively.

   (a) `[4 marks]` What kind of information does they leak out to an attacker?

   (b) `[2 marks]` If the attacker also knows P or P', what else will he know and why?