IIIT Delhi
CSE-546 Applied Cryptography Monsoon 2013
HW-4 and 5

HW-4 Due date: 7-October-2013

1. DES has become insecure due to its short key length (56 bits). An improvement, proposed by Rivest, is $DESX$. $DESX$ has key length 120 bits, seen as a pair $(k_1; k_2)$, where k_1 is 56 bits and k_2 64 bits. Let the enryption of a message m using DES with key k be denoted by $DES_k(m)$. The encryption of a one-block message m using $DESX$ is $DESX_{(k1;k2)}(m) = (DES_{k_1}(m \oplus k_2)) \oplus k_2$:
   (a) Explain how decryption is done.
   (b) Explain why the inner xor is necessary, i.e. explain an attack against $DESX'_{(k1;k2)}(m) = DES_{k_1}(m) \oplus k_2$ that is much better than brute force.[1]
2. Give an example of a hash function which satisfies the following properties. If no such hash function can exist then explain why.
   (a) Preimage resistant but not second preimage resistant
   (b) Second preimage resistant but not preimage resistant
   (c) Preimage resistant but not collision resistant
   (d) Collision resistant but not preimage resistant

HW-5 Due date: 14-Oct-2013.

1. Implement AES-256 in Java/C++. Details are here `http://www.cs.utexas.edu/~byoung/cs361/assignment-aes.html`

[1] A good thing about the DESX design is that it improves the security of DES while not paying the penalty of triple encryptions as in 3-DES. We can't use 2-DES, of course.