**IERG4130: Introduction to Cyber Security** **Fall 2017**

# Assignment 1 Solution

**Question 1:** True or False. Explain your answer.

(1) False. Non-executable stack is insecure against return-to-library attack, which is a kind of buffer overflow attack.

(2) False. It stores hashes of salted passwords such that two hashes are not likely to be identical even if two input passwords are the same.

(3) False. Private browsing mode only disables browsing history, cache, and cookies on the local computing device. It does not prevent the web server from knowing the IP address and user name.

(4) False. XSRF exploits of a website where unauthorized commands are transmitted from a user that the web application trusts.

(5) True. The attacker learns nothing about the message even if it tried out all possibilities.

(6) True. One can tell whether two ciphertexts are encryption of the same message./ False, it is secure as long as the message space is large.

(7) False. By birthday attack, the number of attempts should be of order $O(2^{\frac{k}{2}})$.

(8) False. If the decryption key is small, anyone can launch a brute force attack to find the decryption key efficiently. / Typically short encryption key is used to allow efficient encryption.

**Question 2:** Message Integrity in Counter (CTR) mode

(a) First obtain $C' = \mathsf{Enc}_k^{\text{hCTR}}(M)$ for $M = 0$. Let $C' = IV||c_0|| \cdots ||c_{n-1}||\sigma$. Then for any message $M^* = m_0^*|| \cdots ||m_{n-1}^*$, one can compute $B^* = c_0 \oplus m_0^*|| \cdots ||c_{n-1} \oplus m_{n-1}^*$ and $\sigma^* = h(B^*)$. Now $C^* = B^*||\sigma^*$ is a valid ciphertext on message $M^*$.

(b) First obtain $C' = \mathsf{Enc}_k^{\text{hCTR}}(M)$ for $M = 0$. Let $C' = IV||c_0|| \cdots ||c_{n-1}||c_n$. Then for any message $M^* = m_0^*|| \cdots ||m_{n-1}^*$, one can compute $B^* = c_0 \oplus m_0^*|| \cdots ||c_{n-1} \oplus m_{n-1}^*||c_n \oplus h(0) \oplus h(M^*)$. Now $C^* = B^*$ is a valid ciphertext on message $M^*$.

(c) Replace the hash function $h$ by a secure MAC.

**Question 3:** RSA Cryptosystem

(a) $N = (p-1)(q-1) = 30 \times 126 = 3780$, $1031 \times 11 - 3 \times 3780 = 1 \rightarrow \mathsf{dk} = 1031$. (You need to show the steps of Extended Euclidean Algorithm)

(b) $m \equiv 413^{1031} \equiv 1786 \mod 3937$. (You need to show the steps of repeated squaring)
If you use CRT, you first find $41 \times 31 - 10 \times 127 = 1$. Then computes $413^{1031} \equiv 10^{11} \equiv 19 \mod 31$, $413^{1031} \equiv 32^{23} \equiv 8 \mod 127$. Finally computes $(19)(127)(41) + (8)(31)(31-10) \equiv 1786 \mod 3937$.

(c) Given $c$, a ciphertext of $m$. Compute $c' \leftarrow Enc(m')$. Then, $c \cdot c'$ is a ciphertext of $m \cdot m'$

(d) Use OAEP. (using MAC/signature is also acceptable)

(e) If $c' \neq c$, then $m' \neq m$.