Comp5631/CSIT5710: Cryptography and Security
2019 Fall – Written Assignment Number 2
Handed out: on October 20, 2017
Due: on October 31 for COMP4631 and Nov. 1 for CSIT5710 at the *beginning* of the lecture

Assignments handed in during class will lose marks. No assignments will be accepted after class. No email submission will be accepted.

Q1. Let p be a prime and α be a primitive root modulo p. The ElGamal public-key cipher $(\mathcal{M}, \mathcal{C}, \mathcal{K}_e, \mathcal{K}_d, E_{k_e}, D_{k_d})$ is defined as follows:

- $\mathcal{M} = \mathbf{Z}_p^* = \{1, 2, 3, \cdots, p-1\}$, $\mathcal{C} = \mathbf{Z}_p^* \times \mathbf{Z}_p^*$, $\mathcal{K}_e = \{p\} \times \{\alpha\} \times \mathbf{Z}_p^*$, $\mathcal{K}_d = \mathbf{Z}_{p-1}$.

A user first chooses a random number u in $\mathbf{Z}_{p-1}$ as his private key $k_d := u$, then publicizes his public key $k_e = (p, \alpha, \beta)$, where $\beta = \alpha^u \bmod p$.

To encrypt a message x with a public key $k_e = (p, \alpha, \beta)$, one picks up a (secret) random number $v \in \mathbf{Z}_{p-1}$, and then does the encryption as follows:

$$E_{k_e}(x, v) = (y_1, y_2),$$

where $y_1 = \alpha^v \bmod p$, and $y_2 = x\beta^v \bmod p$.

When the receiver receives the ciphertext $(y_1, y_2) \in \mathbf{Z}_p^* \times \mathbf{Z}_p^*$, he does the decryption as follows:

$$D_{k_d}(y_1, y_2) = y_2 \left(y_1^{k_d}\right)^{-1} \bmod p,$$

where $\left(y_1^{k_d}\right)^{-1}$ denotes the multiplicative inverse of $y_1^{k_d}$ modulo p. Prove that the decryption process above is correct. $\boxed{\text{20 marks}}$

Q2. Consider the Paillier cipher introduced in Lecture 10. Suppose that the random integer g is chosen of the form

$$g = (1+n)^\alpha \beta^n \bmod n^2,$$

where α and β are in $\mathbf{Z}_n^*$. Prove that

$$m = L(c^\lambda \bmod n^2)\mu \bmod n = \frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n.$$

This is to prove the correctness of the decryption process. You may use the following theorem:
Carmichael's theorem: For any $r \in \mathbf{Z}_{n^2}^*$, we have $r^{n\lambda} = 1 \bmod n^2$. $\boxed{\text{20 marks}}$

Q3. Suppose that RSA and a hash function f are used for digital signature. The standard approach is the following:

1. The signer computes a hash value $f(m)$ of the message m.
2. The signer then uses his/her private key k_d to compute his digital signature $D_{k_d}(f(m))$.

A student suggests an alternative approach. His idea is that the signer computes $D_{k_d}(m)$ as the digital signature of the message m and then sends $m||D_{k_d}(m)$ to the receiver. Assume that the public-key cipher and the hash function f are well designed? Is the scheme proposed by the student secure? Justify your answer briefly. $\boxed{\text{20 marks}}$

Q4. The following is one method of constructing a hash function from a given block cipher.

Building block: A one-key block cipher $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_k)$, where E_k maps a block of n bits into a block of n bits, and the secret key k has also n bits.

Computing the hash value: Given a message m, divide it into blocks of length n, $m = m_1 m_2 m_3 \cdots m_t$ The hash value H is computed as follows:

$$H(m) = E_k(m_1) \oplus E_k(m_2) \oplus \cdots \oplus E_k(m_t),$$

where

$$k = m_1 \oplus m_2 \oplus \cdots \oplus m_t,$$

and $\oplus$ denotes the bitwise exclusive-or operation.

Find a collision of this hash function H, i.e, two distinct messages m and m' such that $H(m) = H(m')$. $\boxed{\text{20 marks}}$

Q5. Show that the Diffie-Hellman Key Agreement Protocol described in Lecture 6 is not secure with respect to active attacks. Hint: Consider an intruder-in-the-middle attack. $\boxed{\text{20 marks}}$