COMP5631: Cryptography and Security
2024 Spring – Written Assignment Number 3
Sample Solutions

Q1. Recall the RSA public-key cipher introduced in Lecture 8. Prove the correctness of the decryption process: $M = C^d \bmod n$. $\boxed{\text{20 marks}}$

Proof: Note that $\gcd(n, M)$ takes on only the four values in $\{1, p, q, n\}$. We will prove the equality $M = C^d \bmod n$ in all the four cases.

Case I $\gcd(M, n) = 1$**.** In this case, by Euler's theorem (see Q4 in Assignment 1),

$$\begin{aligned} C^d \bmod n &= M^{ed} \bmod n \\ &= M^{u\phi(n)+1} \bmod n \\ &= (M^{u\phi(n)} \bmod n)M \bmod n \\ &= (M^{\phi(n)} \bmod n)^u M \bmod n \\ &= M \bmod n \\ &= M, \end{aligned}$$

where u is some integer.

Case II $\gcd(M, n) = p$**.** In this case, we have $M = tp$ for some $0 < t < q$. So $\gcd(M, q) = 1$. Since $ed = u\phi(n) + 1$ for some u, by Fermat's theorem (see Q4 in Assignment 1), we have

$$\left(M^{u\phi(n)} - 1\right) \bmod q = \left(\left[M^{u(p-1)}\right]^{q-1} - 1\right) \bmod q = 0.$$

Whence

$$\begin{aligned} C^d \bmod n - M &= M^{ed} \bmod n - M \\ &= \left(M^{ed} - M\right) \bmod n \\ &= M\left(M^{ed-1} - 1\right) \bmod n \\ &= tp\left(M^{u\phi(n)} - 1\right) \bmod pq \\ &= 0. \end{aligned}$$

Case III $\gcd(M, n) = q$**.** This case is similar to Case II and the proof is skipped.

Case IV $\gcd(M, n) = n$**.** In this case $M = 0$, and thus $C = 0$. Hence, the equality $M = C^d \bmod n$ holds.

In summary, the desired equality holds in all the possible cases. This completes the proof.

Q2. 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. $\boxed{\text{20 marks}}$

Proof: Note that $\beta = \alpha^u \bmod p$ and

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

We have

$$\begin{aligned} D_{k_d}(y_1, y_2) &= y_2 \left(y_1^u\right)^{-1} \bmod p \\ &= x\beta^v \left([\alpha^v]^u\right)^{-1} \bmod p \\ &= x\alpha^{uv}\alpha^{-uv} \bmod p \\ &= x \bmod p \\ &= x. \end{aligned}$$

Q3. Suppose you are given a ciphertext block C encrypted with the RSA algorithm and you do not know the private key d. Assume $n = pq$, e is the public key. Suppose also someone tells you that he knows that the corresponding plaintext block M has a common factor with n (i.e., $\gcd(M, n) > 1$, but no further information about the common divisor is given to you). Does this information help you in any way with recovering the plaintext block M? Justify your conclusion. (20 marks)

Solution: Since p and q are prime and $n = pq$, n only has factors 1, p, q and n. Since $C = M^e \bmod n$, it is easily seen that $\gcd(M, n) = \gcd(C, n)$. By the information provided, you have $\gcd(C, n) \in \{p, q, n\}$. You can use the extended Euclidean algorithm to compute the gcd of n and C. If $\gcd(C, n) = n$, then C must be 0 and $M = 0$. Otherwise, $\gcd(C, n) = p$ or $\gcd(C, n) = q$. In this way, you can factor n into $n = pq$. Then you can use $\phi(n) = (p-1)(q-1)$ to recover the private key $d = e^{-1} \bmod \phi(n)$ and then the plaintext $M = C^d \bmod n$.

Q4. Consider the digital signature scheme $m||D_{k_d^{(A)}}(h(m))$ introduced in Lecture 7 and answer the following two questions:

- Why should the underlying public-key cipher satisfy Condition C1? $\boxed{\text{5 marks}}$

  Solution: If Condition C1 is not met, one can compute Alice's private key from her public key and then forger Alice's digital signature on any message m.

- Consider the following forgery attack on the digital signature scheme. Carol finds out a pair of messages m_1 and m_2 such that

  1. m_2 has the same length as the digital signature; and
  2. $h(m_1) = E_{k_e^{(A)}}(m_2)$.

  If this is computationally feasible, Carol can claim that m_2 is Alice's digital signature on m_1. How should the underlying public-key cipher and hash function h be designed with respect to this forgery attack? $\boxed{\text{15 marks}}$

  Solution: There are two different ways to find such a pair (m_1, m_2). Carol may first choose m_2 and then find m_1 such that $h(m_1) = E_{k_e^{(A)}}(m_2)$. If h is one-way, this is computationally infeasible. Another way is to choose m_1 first, then determine m_2 using the equation $h(m_1) = E_{k_e^{(A)}}(m_2)$. This requires that the public-key cipher satisfy Condition C2.

  In summary, with respect to this forgery attack, the two building blocks of the digital signature system should have the following properties:

  1. The public-key cipher should meet Conditions C1 and C2.
  2. The hash function should have the one-way property.

Grading guidelines for Q4: The justifications in red color are assigned 10 marks. The conclusions in red color are assigned 5 marks. Please grade this question rigorously.

Q5. A student designed the following hash function:

$$h(x) := 3x \bmod 2^{64}$$

where x is any nonnnegative integer in the interval $[0, 2^{512} - 1]$. Suppose that x takes on all nonnegative integers in the interval $[0, 2^{512} - 1]$ equally likely. Answer the following questions and justify your answers briefly:

1. Are the hash values of $h(x)$ uniformly distributed? (in other words, does $h(x)$ take on all elements in $\{0, 1, \cdots, 2^{64} - 1\}$ equally likely?) (6 marks)

   Answer: The hash values are uniformly distributed, i.e., $h(x)$ takes on all elements in $\{0, 1, \cdots, 2^{64} - 1\}$ equally likely.

   Justification: Every nonnegative integer x can be expressed as

   $$x = t + \bar{x}2^{64},$$

   where $\bar{x}$ is a nonnegative integer (i.e., the quotient) and t is a unique integer in $\{0, 1, \cdots, 2^{64} - 1\}$ (i.e., the remainder). Since x takes on all integers in the interval $[0, 2^{512} - 1]$ equally likely, t takes on all elements in $\{0, 1, \cdots, 2^{64} -$

$1\}$ equally likely. Hence, the function $x \bmod 2^{64}$ takes on all elements in $\{0, 1, \cdots, 2^{64} - 1\}$ equally likely.

Note that $\gcd(3, 2^{64}) = 1$. The related linear function $h(x) = 3x \bmod 2^{64}$ is thus a permutation of $Z_{2^{64}}$. Consequently, $h(x)$ takes on all elements in $\{0, 1, \cdots, 2^{64} - 1\}$ equally likely.

2. Is the hash function $h(x)$ one-way? (7 marks)

   Answer: The hash function is not one-way.

   Justification: Let 3^{-1} denote the multiplicative inverse of 3 modulo 2^{64}. For any $t \in \{0, 1, \cdots, 2^{64} - 1\}$, $f(3^{-1}t) = t$. Hence h is not one-way.

3. Is it easy to find out weak collisions for $h(x)$? (7 marks)

   Answer: It is easy to find out weak collisions for h.

   Justification: For any nonnegative integer x in the interval $[0, 2^{512} - 1]$, we have
   $$h(x) = h((x + 2^{64}) \bmod 2^{512}).$$
   Hence, x and $(x + 2^{64}) \bmod 2^{512}$ form a weak collision, which are clearly different.