CS60088 Foundations of Cryptography, Spring 2014–2015

Class Test

10–April–2015 | 6:45–7:45pm | Maximum marks: 20

Roll no: ____________ **Name:** ______________________________

[*Write your answers in the question paper itself. Be brief and precise. Answer all questions.*]

1. Pointcheval (Eurocrypt 1999) proposes an ElGamal-like encryption algorithm based upon RSA. Let $n = pq$ be an RSA modulus, and (e, d) a key pair under this modulus. In order to encrypt a message $m \in \mathbb{Z}_n$, one chooses a random $r \in_U \mathbb{Z}_n$, and computes $\alpha \equiv r^e \pmod{n}$ and $\beta \equiv m(r+1)^e \pmod{n}$. A ciphertext for m is the pair (α, β).

(a) Explain how a ciphertext (α, β) can be decrypted. **(5)**

Solution Using the decryption exponent, r is first recovered as $r \equiv \alpha^d \pmod{n}$. With overwhelmingly large probability, we have $r + 1 \in \mathbb{Z}_n^*$. So m is recovered as $m \equiv \beta(r+1)^{-e} \pmod{n}$.

(b) Is this encryption scheme non-malleable? **(5)**

Solution No. If (α, β) is a ciphertext for m, then $(\alpha, 2\beta \pmod{n})$ is a ciphertext for $2m \pmod{n}$.

2. Let $\mathscr{E}$ be a public-key encryption algorithm, and $\mathscr{D}$ the corresponding decryption algorithm. Let us design a new public-key encryption algorithm $\mathscr{E}'$ as $\mathscr{E}'(m) = \mathscr{E}(m) \,||\, a$ for a randomly chosen bit $a \in_U \{0,1\}$. The corresponding decryption is carried out as $\mathscr{D}'(c \,||\, a) = \mathscr{D}(c)$. Here, $\mathscr{E}$ and $\mathscr{D}$ respectively use the public and the private keys of an entity. Prove/Disprove the following two assertions.

(a) If $(\mathscr{E},\mathscr{D})$ is IND-CCA secure, then $(\mathscr{E}',\mathscr{D}')$ is IND-CCA secure. **(5)**

Solution *True.* We provide a reduction to contradiction. Suppose that $(\mathscr{E}',\mathscr{D}')$ is not IND-CCA secure, that is, there exists a PPT adversary A' that can win the IND-CCA game against $(\mathscr{E}',\mathscr{D}')$ with non-negligible advantage Adv. Using this algorithm, Simon (the simulator) wins the IND-CCA game against $(\mathscr{E},\mathscr{D})$ with the same advantage Adv, contradicting that $(\mathscr{E},\mathscr{D})$ is IND-CCA secure.

The adversary A' needs access to an oracle $\mathscr{O}'$ for $(\mathscr{E}',\mathscr{D}')$. Simon intercepts all communication between A' and $\mathscr{O}'$. Simon has access to an oracle $\mathscr{O}$ for $(\mathscr{E},\mathscr{D})$. Using this, Simon simulates $\mathscr{E}'$ and $\mathscr{D}'$.

[IND-CCA Adversary A' for $(\mathscr{E}',\mathscr{D}')$] $\Longleftrightarrow$ [Simon the simulator] $\Longleftrightarrow$ [Oracle $\mathscr{O}$ for $(\mathscr{E},\mathscr{D})$]

Pre-challenge training session: The adversary A' sends a set of indifferent chosen ciphertexts $c' = c \,||\, a$ to Simon. Simon sends c to $\mathscr{O}$, gets the decryption result $m = \mathscr{D}(c)$, and returns m back to A'. Since $\mathscr{D}'(c') = \mathscr{D}(c)$, Simon's simulation of decryption is perfect.

The IND-CPA game: When A' is happy with the cryptanalysis training, it sends two messages m_0, m_1 (of the same length) to Simon. Simon forwards the same messages to the oracle $\mathscr{O}$. The oracle chooses a random bit $b \in_U \{0,1\}$, encrypts m_b, and sends the challenge ciphertext $c^* = \mathscr{E}(m_b)$ back to Simon. Simon chooses a random bit $a \in_U \{0,1\}$, and sends $c^* \,||\, a$ back to A'. Clearly, $c^* \,||\, a$ is a valid ciphertext of m_b under the encryption algorithm $\mathscr{E}'$, that is, Simon's simulation of $\mathscr{E}'$ is perfect.

End of game: After receiving the challenge ciphertext, A' unleashes its cryptanalytic prowess and outputs a bit b'. Simon outputs the same bit b'. We have $b = b'$ with probability $\frac{1}{2} + \text{Adv}$.

(b) If $(\mathscr{E}, \mathscr{D})$ is IND-CCA2 secure, then $(\mathscr{E}', \mathscr{D}')$ is IND-CCA2 secure. **(5)**

Solution *False*. Let $c^* = c \,||\, a = \mathscr{E}'(m_b)$ be the challenge ciphertext. Then, $d^* = c \,||\, \bar{a}$ is also a ciphertext of m_b under $\mathscr{E}'$, where $\bar{a}$ is the complement of the bit a. In the post-challenge phase, the adversary queries the oracle to decrypt d^*. Since $d^* \neq c^*$, this is allowed. So the oracle decrypts d^*, and reveals m_b to the adversary.

For leftover answers and rough work