INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

Stamp / Signature of the Invigilator

EXAMINATION (Mid Semester)	**SEMESTER (Spring)**

Roll Number										**Section**		**Name**	

Subject Number	C	S	6	0	0	8	8	**Subject Name**	*Foundations of Cryptography*

Department / Center of the Student		**Additional sheets**	

Important Instructions and Guidelines for Students

1. You must occupy your seat as per the Examination Schedule/Sitting Plan.
2. Do not keep mobile phones or any similar electronic gadgets with you even in the switched off mode.
3. Loose papers, class notes, books or any such materials must not be in your possession, even if they are irrelevant to the subject you are taking examination.
4. Data book, codes, graph papers, relevant standard tables/charts or any other materials are allowed only when instructed by the paper-setter.
5. Use of instrument box, pencil box and non-programmable calculator is allowed during the examination. However, exchange of these items or any other papers (including question papers) is not permitted.
6. Write on both sides of the answer script and do not tear off any page. **Use last page(s) of the answer script for rough work.** Report to the invigilator if the answer script has torn or distorted page(s).
7. It is your responsibility to ensure that you have signed the Attendance Sheet. Keep your Admit Card/Identity Card on the desk for checking by the invigilator.
8. You may leave the examination hall for wash room or for drinking water for a very short period. Record your absence from the Examination Hall in the register provided. Smoking and the consumption of any kind of beverages are strictly prohibited inside the Examination Hall.
9. Do not leave the Examination Hall without submitting your answer script to the invigilator. **In any case, you are not allowed to take away the answer script with you.** After the completion of the examination, do not leave the seat until the invigilators collect all the answer scripts.
10. During the examination, either inside or outside the Examination Hall, gathering information from any kind of sources or exchanging information with others or any such attempt will be treated as **'unfair means'**. Do not adopt unfair means and do not indulge in unseemly behavior.

Violation of any of the above instructions may lead to severe punishment.

Signature of the Student

To be filled in by the examiner

Question Number	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Total**
Marks Obtained											

Marks obtained (in words)	**Signature of the Examiner**	**Signature of the Scrutineer**

CS60088 Foundations of Cryptography, Spring 2015–2016

Mid-Semester Test

19–February–2016 CSE-107/119/120, 2:00–4:00pm Maximum marks: 45

Roll no: _____ **Name:** _____

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

1. Let $b_1b_2b_3\ldots$ be a bit sequence obtained from a cryptographically secure pseudorandom bit generator G. Prove/Disprove: The bit string $b_1b_3b_5\ldots$ obtained by dropping every alternate bit is again cryptographically secure. **(10)**

Solution *True.* Assume that $b_1b_3b_5\ldots$ is not cryptographically secure. That is, there exists a PPT algorithm $\mathscr{A}$, that given $b_1b_3b_5\ldots b_{n-1}$ (with n even) as input, can predict b_{n+1} with probability $\geqslant \frac{1}{2}+\frac{1}{p(k)}$ for some polynomial $p(k)$ in the security parameter k. Based on this, we write a next-bit predictor for $b_1b_2b_3\ldots b_n$ as follows:

If n is even, invoke $\mathscr{A}$ with $b_1b_3b_5\ldots b_{n-1}$ as input, and output the bit supplied by $\mathscr{A}$ as b_{n+1}. If n is odd, output a uniformly random bit $b_{n+1} \in_U \{0,1\}$.

Now, n can be even or odd with equal probability. Therefore, the probability that b_{n+1} is correctly guessed is

$$\geqslant \frac{1}{2}\times\left(\frac{1}{2}+\frac{1}{p(k)}\right)+\frac{1}{2}\times\frac{1}{2}=\frac{1}{2}+\frac{1}{2p(k)}.$$

Thus, the advantage is $\frac{1}{2p(k)}$ which is non-negligible ($2p(k)$ is again a polynomial expression in k). This means that the bit string $b_1b_2b_3\ldots$ does not pass the next-bit test, a contradiction to the cryptographic security of the generator G.

2. Let E and E' be two public-key encryption schemes with independently chosen key pairs. Assume that both E and E' are length-preserving, that is, encrypt l-bit plaintext messages to l-bit ciphertext messages. Define the composite encryption scheme $\mathscr{E}(m) = E'_{pub'}(E_{pub}(m))$. Prove that $\mathscr{E}$ is IND-CPA secure if at least one of E and E' is IND-CPA secure. **(10)**

Solution Assume that $\mathscr{E}$ is not IND-CPA secure, that is, there exists a PPT distinguisher algorithm $\mathscr{A}$ that given the challenge ciphertext $c^* = \mathscr{E}(m_b)$ outputs the correct bit b with non-negligible advantage. Using this distinguisher, we prove the IND-CPA insecurity of both E and E'.

Insecurity of E: Let m_0, m_1 be the chosen plaintext messages. The encryption oracle supplies the challenge ciphertext $C = E(m_b)$ for $b \in_U \{0,1\}$. We feed m_0, m_1, and $c^* = E'_{pub'}(C)$ to the distinguisher $\mathscr{A}$. The distinguisher outputs the correct bit b with non-negligible advantage.

Insecurity of E': Choose the plaintext messages for E' as $\mu_0 = E_{pub}(m_0)$ and $\mu_1 = E_{pub}(m_1)$ for some messages m_0, m_1. Supply μ_0, μ_1 to the encryption oracle E' to get the challenge ciphertext $c^* = E'_{pub'}(\mu_b)$ for $b \in_U \{0,1\}$. But then c^* is the composite encryption of m_b, and a call of $\mathscr{A}$ with m_0, m_1, c^* as input reveals b with non-negligible advantage.

3. Let us introduce a new security notion IND-CCA1.5. There is a pre-challenge training phase where the attacker can get decryption assistance on indifferent ciphertext messages. This is followed by the IND-CPA game in which the attacker supplies two messages m_0, m_1 (of the same length) to the encryption oracle. The oracle chooses a random bit $b \in_U \{0,1\}$, and sends the challenge ciphertext $c^* = E_{pub}(m_b)$ to the attacker. After this, decryption assistance stops. However, the oracle continues to entertain a particular type of query from the attacker, namely, when a pair (m,c) is submitted to the oracle, it answers *true* if c is an encryption of m, *false* otherwise. The only restriction is that making (m,c) queries with $m = m_0, m_1$ or $c = c^*$ is not allowed. Give an example of an encryption scheme which is IND-CPA secure (under a suitable assumption) but not IND-CCA1.5 secure. Prove the IND-CPA security (unless covered in the class) and the IND-CCA1.5 insecurity of the scheme. **(10)**

Solution We have proved in the class that the Goldwasser–Micali (GM) encryption scheme is IND-CPA secure if the QR assumption holds. We now show that the GM scheme is not IND-CCA1.5 secure. Let m_0, m_1 be l-bit messages, and $c^* = (c_1^*, c_2^*, \ldots, c_l^*)$. Take a random l-bit message m, and let a GM encryption of m be $c = (c_1, c_2, \ldots, c_l)$. But then, $c^*c = (c_1^*c_1, c_2^*c_2, \ldots, c_l^*c_l)$ is a GM encryption of $m_b \oplus m$. If $m \neq 0, m_0 \oplus m_1$, the message $m_b \oplus m$ is different from both m_0, m_1. Moreover, c is not equal to $(1,1,\ldots,1)$ (which is an encryption of the zero message), implying that $c^*c \neq c^*$. Therefore, a post-challenge query $(m_0 \oplus m, c^*c)$ will be answered by the oracle. If the answer is *true*, the attacker concludes with certainty that $b = 0$, otherwise $b = 1$.

4. Zheng and Seberry (1993) propose an encryption scheme that works in $\mathbb{Z}_p^*$ with a generator g. A key-pair is generated in the usual way: Choose $x \in_U [2, p-2]$ (the private key), and compute $y \equiv g^x \pmod{p}$ (the public key). The message is treated as an n-bit string, where $n = |p| - 1$. The scheme uses two additional functions: a one-way function $H : \{0,1\}^n \to \{0,1\}^l$ (like an l-bit hash function), and a cryptographically strong pseudorandom bit generator G to produce $(n+l)$-bit strings.

In order to encrypt an n-bit message m, the sender chooses a session secret $k \in_U [2, p-2]$, and generates an $(n+l)$-bit pseudorandom string $z = G(s)$, where $s \equiv y^k \pmod{p}$ is the seed. The ciphertext is the pair (c_1, c_2), where $c_1 \equiv g^k \pmod{p}$, and $c_2 = z \oplus (m \,||\, H(m))$.

(a) Explain how a ciphertext (c_1, c_2) can be decrypted. **(5)**

Solution The seed is $s \equiv y^k \equiv g^{xk} \equiv c_1^x \pmod{p}$. Thus, the masking string z is reconstructed as $z = G(c_1^x \pmod{p})$. XORing this with c_2 gives an $(n+l)$-bit string $m \,||\, t$ with $|m| = n$ and $|t| = l$. If $H(m) = t$, then m is output as the decrypted message, otherwise failure is reported.

(b) Prove that the Zheng–Seberry scheme is IND-CCA2 insecure. **(5)**

Solution Let (c_1^*, c_2^*) be the challenge ciphertext corresponding to the encryption of m_b. Let $c_2' = c_2^* \oplus (m_0 \,||\, H(m_0)) \oplus (m_1 \,||\, H(m_1))$. Since $m_0 \neq m_1$, $c_2' \neq c_2^*$, so a decryption query for (c_1^*, c_2') can be made to the oracle. But (c_1^*, c_2') is an encryption of $m_{b'}$ (where b' is the complement of b).

(c) Propose a remedy from the attack of Part (b). **(5)**

Solution Take $c_2 = z \oplus (m \,||\, H(m \oplus s))$ (if $|s| = n+1$, discard one bit of it). Decryption verifies the equality $t = H(m \oplus s)$. This countermeasure does not imply the IND-CCA2 security of the scheme. Only the attack of Part (b) is eliminated.