INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR		
		Stamp / Signature of the Invigilator

EXAMINATION (End 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 2016–2017

End-Semester Test

25–April–2017 NC-141/142, NR-321/322, 2:00–5:00pm Maximum marks: 75

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

1. Let $M = (Gen, Mac, Vrf)$ be a message-authentication scheme.

(a) What is meant by the existential unforgeability of M. **(5)**

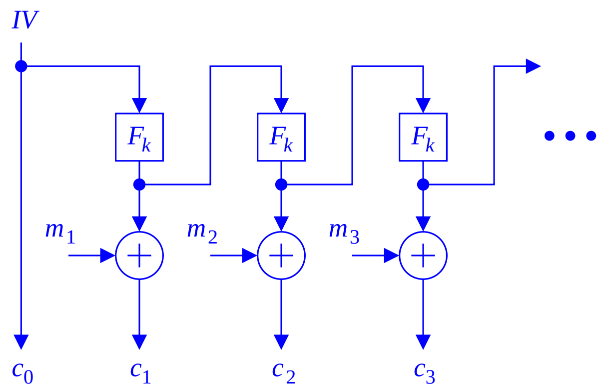
Solution An adversary makes a set Q of queries to the Mac oracle, and receives the corresponding tags. The task of the adversary is to come up with a message $m \notin Q$ and a tag t such that $Vrf(m,t) = 1$. M is called existentially unforgeable if any PPT adversary can succeed in the game with only negligible probability.

(b) Let $F_k : \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom family of functions indexed by keys $k \in \mathscr{K}$ (you may assume $\mathscr{K} = \{0,1\}^n$). Define a message authentication code for $2n$-bit messages (m_1, m_2) (where $m_1, m_2 \in \{0,1\}^n$) as $Mac(m_1, m_2) = (F_{k_1}(m_1), F_{k_2}(m_2))$, where k_1 and k_2 are uniformly random and independent elements of $\mathscr{K}$. Prove/Disprove: The scheme is existentially unforgeable. **(5)**

Solution *False.* Choose two distinct messages $m, m' \in \{0,1\}^n$. Query the Mac oracle about the pairs (m,m) and (m',m'). Let the tags received be (t_1,t_2) and (t'_1,t'_2). Then, a valid tag on (m,m') is (t_1,t'_2).

2. (a) Describe the output feedback (OFB) mode of operation of a block cipher. **(5)**

Solution



(b) Demonstrate that the OFB mode is not IND-CCA2 secure. **(5)**

Solution Let $c^* = (c_0, c_1)$ be the challenge ciphertext of a one-block message M_b. But then, for any randomly chosen non-zero $\rho \in \{0,1\}^*$, $c = (c_0, c_1 \oplus \rho) \neq c^*$ is an encryption of $M_b \oplus \rho$.

3. Let $\Pi = (Gen, Enc, Dec)$ be a *symmetric* encryption scheme. Let us define a game IND-RESTRICTED-CPA played against Π by an adversary $\mathscr{A}$. As in an IND-CPA (or IND-EAV) game, $\mathscr{A}$ supplies two messages m_0, m_1 of the same length to the encryption oracle $\mathscr{O}$. The oracle chooses a uniformly random bit b, and sends an encryption $c^* = Enc_k(m_b)$ to $\mathscr{A}$ as the challenge ciphertext. Before and after this IND-EAV game, the adversary has access to $\mathscr{O}$, and gets encryption assistance on messages chosen by $\mathscr{A}$. The only restriction is that $\mathscr{A}$ is never (neither in the pre-challenge nor in the post-challenge phase) allowed to make an encryption query on m_0 or m_1. Eventually, $\mathscr{A}$ outputs a bit b', and wins if and only if $b' = b$. The scheme Π is called IND-RESTRICTED-CPA secure if no PPT adversary can win this game with non-negligible advantage. We call Π *perfectly* IND-RESTRICTED-CPA secure if any adversary—even if unbounded—cannot have any advantage in winning the IND-RESTRICTED-CPA game against Π.

(a) Consider the IND-EAV secure scheme that encrypts $m \in \{0,1\}^{l(n)}$ to $c = m \oplus G(k)$, where $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ is a pseudorandom generator (PRG), and $k \in \{0,1\}^n$ is the key. Prove that this scheme is not IND-RESTRICTED-CPA secure. **(5)**

Solution The adversary chooses the messages $m_0 = 0^{l(n)}$ and $m_1 = 1^{l(n)}$ during the IND-EAV game. Let the challenge ciphertext be $c^* = m_b \oplus G(k)$. The adversary also chooses $\mu \in \{0,1\}^{l(n)} \setminus \{m_0, m_1\}$, and makes an encryption query on this message. Let $c = \mu \oplus G(k)$ be the ciphertext returned by the encryption oracle. We have $c^* \oplus c = m_b \oplus \mu = \begin{cases} \mu & \text{if } b = 0, \\ \overline{\mu} & \text{if } b = 1. \end{cases}$

(b) Consider the IND-CPA secure construction using a truly random function $f : \{0,1\}^n \to \{0,1\}^n$, that encrypts $m \in \{0,1\}^n$ to $(r, f(r) \oplus m)$, where $r \in_U \{0,1\}^n$. Prove/Disprove: This construction is *perfectly* IND-RESTRICTED-CPA secure. **(5)**

Solution *False.* Each encryption query gives an adversary a pair $(r, f(r))$. Let q be the number of such pairs known to the adversary. During the IND-EAV game, the encryption oracle chooses an r to encrypt m_b, and this r is in the set of known $(r, f(r))$ pairs with probability $\frac{q}{2^n}$. If so, the adversary wins with probability 1. If not, it makes a random guess. Therefore the winning probability of the adversary is

$$\frac{q}{2^n} + \left(1 - \frac{q}{2^n}\right) \times \frac{1}{2} = \frac{1}{2} + \frac{q}{2^{n+1}}.$$

For $q > 0$, the advantage of the adversary is non-zero.

(c) Propose a construction of Π which is IND-RESTRICTED-CPA secure, but not IND-CPA secure. Supply both the security and the insecurity proofs. **(15)**

Solution **The construction**

Let $F_k : \{0,1\}^n \to \{0,1\}^n$ be a family of pseudorandom permutations (PRPs) indexed by n-bit keys k. The three components of the scheme work as follows.

Gen: Choose $k \in_U \{0,1\}^n$.
Enc: $c = F_k(m)$.
Dec: $m = F_k^{-1}(c)$.

IND-CPA insecurity

The scheme is deterministic.

IND-RESTRICTED-CPA security

Let $\mathscr{A}$ be a PPT IND-RESTRICTED-CPA adversary against this scheme with non-negligible advantage Adv. The reduction agent Regent is given a permutation $f : \{0,1\}^n \to \{0,1\}^n$ in the form of a black-box. With probability $\frac{1}{2}$, f is a truly random permutation, and with probability $\frac{1}{2}$, $f = F_k$ for some $k \in_U \{0,1\}^n$. Regent plays the IND-RESTRICTED-CPA game with $\mathscr{A}$ in order to become a distinguisher between random and pseudorandom permutations.

Encryption assistance: Upon the receipt of $m \in \{0,1\}^n$ from $\mathscr{A}$, Regent forwards m to the black-box, and relays its reply as the ciphertext c on m.

IND-EAV game: $\mathscr{A}$ issues two different messages $m_0, m_1 \in \{0,1\}^n$ to Regent. Regent chooses a bit $b \in_U \{0,1\}$, and sends m_b to the black-box, and relays the reply from the black-box back to $\mathscr{A}$ as the challenge ciphertext c^*.

End of game: Eventually, $\mathscr{A}$ outputs a bit b'. Regent concludes that f is pseudorandom if $b' = b$, or random if $b' \neq b$. To calculate the advantage of Regent in arriving at the correct decision about f, consider two cases.

Case 1: f is a random permutation. By the rule of the game, $\mathscr{A}$ can never get the value of $f(m_0)$ or $f(m_1)$. Given that f is truly random, both the cases $c^* = f(m_0)$ and $c^* = f(m_1)$ are equally likely, so $\mathscr{A}$ cannot have any advantage in this case, and therefore Regent's decision $b' \neq b$ is correct with probability $\frac{1}{2}$.

Case 2: $f = F_k$ for some k. In this case, $\mathscr{A}$ has the advantage Adv for deciding b correctly, so Regent sees $b' = b$ with probability $\frac{1}{2} + \text{Adv}$.

Combining these two cases, we conclude that Regent makes the correct decision about f with probability

$$\frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \left(\frac{1}{2} + \text{Adv}\right) = \frac{1}{2} + \frac{\text{Adv}}{2}.$$

Given that Adv is non-negligible (in n), so too is Regent's advantage. This contradicts the assumption that PRPs are computationally indistinguishable from random permutations.

4. Pointcheval (Eurocrypt 1999) proposes IND-CPA and IND-CCA2 secure public-key encryption schemes based on the dependent RSA problem (DRSAP). Let $n = pq$ be an RSA modulus, $\gcd(e, \phi(n)) = 1$, and $d \equiv e^{-1} \pmod{\phi(n)}$. The decisional DRSA problem (DDRSAP) is to decide, given $\alpha, \beta \in \mathbb{Z}_n$, whether $\alpha \equiv a^e \pmod n$ and $\beta \equiv (a+1)^e \pmod n$ for some $a \in \mathbb{Z}_n$. Consider the following encryption scheme for $m \in \mathbb{Z}_n$. The scheme uses a hash function $H : \mathbb{Z}_n \times \mathbb{Z}_n \to \{0,1\}^k$, where k is the security parameter.

1. Choose $a \in_U \mathbb{Z}_n$.
2. Compute $\alpha \equiv a^e \pmod n$ and $\gamma = m(a+1)^e \pmod n$.
3. Compute $h = H(m, a)$.
4. A ciphertext for m is the triple (α, γ, h).

(a) Explain how to carry out decryption in this scheme. **(5)**

Solution The recipient uses the private exponent d to compute $a \equiv \alpha^d \pmod n$, and obtains $m \equiv \gamma(a+1)^{-e} \pmod n$. The recipient then verifies whether $H(m,a) = h$. If so, m is taken as the decryption result, otherwise decryption fails.

In the rest of this exercise, you work out an IND-CCA2 security proof of this encryption scheme in the random-oracle model. The proof is based upon the assumption that the DDRSAP is intractable. Let $\mathscr{A}$ be a PPT adversary against this scheme with non-negligible advantage Adv. Ronald is a random oracle that interacts with $\mathscr{A}$.

(b) What is the objective of Ronald? **(5)**

Solution Ronald is given a pair $(\alpha^*, \beta^*) \in \mathbb{Z}_n^2$. It is provided that $(\alpha^*, \beta^*) \equiv (a^e, (a+1)^e) \pmod n$ for some $a \in_U \mathbb{Z}_n$ with probability $\frac{1}{2}$, or $(\alpha^*, \beta^*) \in_U \mathbb{Z}_n^2$ with probability $\frac{1}{2}$. Ronald's objective is to decide what (α^*, β^*) is (a random DRSA pair or a random pair).

(c) How does Ronald simulate encryption during the IND-CPA game? When is the simulation perfect? **(5)**

Solution Upon the receipt of two distinct messages $m_0, m_1 \in \mathbb{Z}_n$, Ronald chooses $b \in_U \{0,1\}$, computes $\gamma^* \equiv m_b \beta^* \pmod{n}$, selects $h^* \in_U \{0,1\}^k$, and sends the challenge ciphertext $c^* = (\alpha^*, \gamma^*, h^*)$ to $\mathscr{A}$.

If (α^*, β^*) is a DRSA pair, then RSA decryption gives a unique $a^* \equiv (\alpha^*)^d \pmod{n}$, and for this a^* we have $\gamma^* \equiv m_b(a^*+1)^e \pmod{n}$. Therefore c^* is a valid ciphertext of m_b if Ronald defines $H(m_b, a^*) = h^*$.

If (α^*, β^*) is randomly chosen from $\mathbb{Z}_n^*$, c^* is a valid encryption of m_0 or m_1 with probability $\frac{2}{n}$, that is, with probability $1 - \frac{2}{n}$, c^* is an encryption of neither m_0 nor m_1.

(d) How does Ronald respond to random-oracle (H) queries? **(5)**

Solution Ronald maintains a table T of $((m,a),h)$ pairs. When a query $(m,a) \neq (m_b, a^*)$ comes from $\mathscr{A}$, Ronald looks up at T. If some $((m,a),h)$ resides in T, the string h is returned to $\mathscr{A}$. If not, a random $h \in_U \{0,1\}^k$ is chosen by Ronald, $((m,a),h)$ is stored in T, and h is returned to $\mathscr{A}$.

If the hash query $H(m_b, a^*)$ comes (should be in the post-challenge phase, because before seeing α^* it is only with negligible probability that $\mathscr{A}$ makes a query on a^*), Ronald can verify by checking whether $(a^*)^e \equiv \alpha^* \pmod{n}$. If so, h^* is returned (after adding $((m_b, a^*), h^*)$ to T). Otherwise, a uniform random string is returned as usual.

(e) How does Ronald simulate decryption? Comment on the perfectness of the simulation. **(5)**

Solution Let $c = (\alpha, \gamma, h)$ be queried by $\mathscr{A}$ for decryption. Ronald looks up his table T to found out whether it stores an entry $((m,a),h)$ (with the same h as in the query) for which $\alpha \equiv a^e \pmod{n}$, and $\gamma \equiv m(a+1)^e \pmod{n}$. If so, m is returned, otherwise *failure* is reported.

Let (α, γ, h) be a valid ciphertext with $H(m,a)$ not queried. Since all possible strings in $\{0,1\}^k$ are equally likely to be $H(m,a)$, we have $H(m,a) = h$ with probability $\frac{1}{2^k}$, that is, a valid ciphertext is rejected with negligible probability $\frac{1}{2^k}$.

(f) How is Ronald's objective satisfied at the end of the game? **(5)**

Solution If $\mathscr{A}$ makes an H query on (m_b, a^*) (in the post-challenge phase), Ronald can easily check whether $\alpha \equiv (a^*)^e \pmod{n}$ and $\beta \equiv (a^*+1)^e \pmod{n}$, and can solve his decision problem with certainty (actually, with probability $1 - \frac{1}{n}$, since a random pair from $\mathbb{Z}_n^*$ can be a DRSA pair with probability $\frac{1}{n}$ only). So suppose that $\mathscr{A}$ never makes this hash query.

Eventually, $\mathscr{A}$ outputs a bit b'. Ronald decides that (α^*, β^*) is a DRSA pair if $b' = b$ or a random pair if $b' \neq b$.

If (α^*, β^*) is a random DRSA pair (this has probability $\frac{1}{2}$), then $\mathscr{A}$ correctly outputs $b' = b$ with probability $\frac{1}{2} + \text{Adv}$. On the other hand, if (α^*, β^*) is a random pair from $\mathbb{Z}_n^*$, then with probability $1 - \frac{2}{n}$, c^* is a valid ciphertext of neither m_0 nor m_1, that is, $\mathscr{A}$ now has no advantage in guessing b, that is, $b' \neq b$ with probability $\frac{1}{2}$. To sum up, Ronald solves his decision problem correctly with probability

$$\geqslant \frac{1}{2} \times \left(\frac{1}{2} + \text{Adv}\right) + \frac{1}{2} \times \left(1 - \frac{2}{n}\right) \times \frac{1}{2} = \frac{1}{2} + \left(\frac{\text{Adv}}{2} - \frac{1}{n}\right).$$

Since Adv is non-negligible and $\frac{1}{n}$ is negligible, Ronald succeeds with non-negligible advantage.