Name: **Roll no:**

Quiz 1

Cryptography & Network Security I
CS 406: Spring 2018

March 6, 2018

[**Total: 100 pts** (4 problems of 25 pts each)]

1. **Computational Indistinguishability.** Let U_k stand for the uniform distribution over $\{0,1\}^k$ (for each value of the security parameter k). Let X_k and Y_k be distributions and $S_k \subseteq \{0,1\}^k$ a set such that:

   i) X_k is uniform over S_k and Y_k is uniform over $\{0,1\}^k \setminus S_k$.

   ii) $X_k \approx U_k$

   iii) $|S_k| = 2^{k-1}$.

   (a) Show that $Y_k \approx U_k$. [18 pts]

   Hint: Can you show that a distinguisher between Y_k and U_k is also a distinguisher between X_k and U_k?

(b) Suppose we remove condition (iii) that $|S_k| = 2^{k-1}$ (but retain conditions (i) and (ii)). Then give an example of S_k such that $Y_k \not\approx U_k$. [7 pts]

2. **Secret-Sharing.**

Alice tells Bob that she has designed a 2-out-of-2 secret-sharing scheme for the message space $\mathcal{M} = \{0,1\}$, using an $m \times n$ matrix D, as follows: to share $b \in \{0,1\}$, the sharing algorithm picks uniformly at random a cell (i,j) in the matrix D such that $D_{i,j} = b$, and lets the two shares be i and j respectively (here, $i \in \{1,\ldots,m\}$ and $j \in \{1,\ldots,n\}$).

(D may contain entries other than 0 and 1. These cells will never be picked by the sharing algorithm.)

(a) What is the condition on D for Alice's scheme to be a valid secret-sharing scheme? State your condition in terms of the following quantities: $R_i(b)$ and $C_j(b)$ are, respectively, the number of occurrences of b in the i^{th} row and j^{th} column of D, and $N(b) = \sum_{i=1}^{m} R_i(b) = \sum_{j=1}^{n} C_j(b)$ is the total number of occurrences of b in D.
Show how you arrive at this condition from the requirements on a valid 2-out-of-2 secret-sharing scheme. [18 pts]

(b) Alice then tells Bob that D is a 3×3 matrix, and its first row is $(0,0,1)$ (i.e., $D_{1,1,} = D_{1,2} = 0, D_{1,3} = 1$).
Choose the correct option from the below and justify your answer: [7 pts]

A. Alice's scheme cannot satisfy correctness and security requirements of a secret-sharing scheme.
(If you choose this option, argue how it follows from your condition above.)

B. There is a unique way to complete the matrix D so that Alice's scheme is a valid secret-sharing scheme.
(If you choose this option, show this D, and briefly justify why it is unique.)

C. There are multiple ways to complete the matrix D so that Alice's scheme is a valid secret-sharing scheme.
(If you choose this option, describe all the valid ways in which D can be completed.)

3. **Symmetric-Key Encryption Using Block-Ciphers.**

   Recall the CPA secure encryption scheme from class, using a block-cipher (or PRF) F: $\mathsf{Enc}(m, K) = (r, F_K(r) \oplus m)$ where r is randomly chosen by Enc, K is the key and m is the message – each being one block long (k bits). The following problems relate to alternate suggestions for encryption.

   In each problem below, if you need any features of a block-cipher that are not guaranteed by a PRF, you should explicitly mention them.

   (a) Consider $\mathsf{Enc}(m, K) = (r, F_K(r \oplus m))$, where F is a block-cipher.

      i. Show that this is a CPA secure encryption scheme. You should describe how an adversary A in the CPA security game can be turned into an adversary A^* against the PRF, and argue that if A had a non-negligible advantage ϵ in its game, then A^* will have a non-negligible advantage ϵ^* in its game. [16 pts]

         Hint: A^* will internally run the CPA security game involving A. Arrange it so that if A^* is interacting with a truly random function, then A will have negligible advantage. Be sure to argue why this is so.

ii. How will you implement a decryption algorithm Dec for this encryption scheme. [4 pts]

(b) Consider $\mathsf{Enc}(m, K) = (r, F_r(K) \oplus m)$, where F is a block-cipher. Give an explicit adversary in the CPA security game to show that this is *not* a CPA secure encryption scheme. [5 pts]

4. **Multiple Choice and fill in the blanks.** (For (a)-(d), select **all** the correct answers.) [25 pts]

(a) For one-time symmetric-key encryption, without loss of generality one may consider the encryption algorithm to be deterministic because: [5 pts]

- ☐ Any randomness needed by the encryption algorithm can be supplied as part of the key.
- ☐ Since it is used only once, the random string in the encryption algorithm can be replaced by a fixed string (say, the all zeros string).
- ☐ Any randomness needed by the encryption algorithm can be considered to be part of the message.
- ☐ The decryption algorithm, which inverts encryption, is deterministic and hence there is no benefit in letting encryption be randomized.
- ☐ None of the above.

(b) Which of the following are correct expressions for computing the CBC-MAC tag, using a key K and a block-cipher F, for a t-block message $m = m_1||\ldots||m_t$ where each m_i is exactly one block long. Below $\overline{0}$ denotes a block of zeros. [5 pts]

- ☐ $x_0 = \overline{0}$; for $i \in \{1, \ldots, t\}$, $x_i = m_i \oplus x_{i-1}$ and $y_i = F_K(x_i)$. Output y_t.
- ☐ $y_0 = \overline{0}$; for $i \in \{1, \ldots, t\}$, $y_i = F_{K \oplus m_i}(y_{i-1})$. Output y_t.
- ☐ $y_0 = \overline{0}$; for $i \in \{1, \ldots, t\}$, $y_i = F_K(m_i \oplus y_{i-1})$. Output y_t.
- ☐ None of the above.

(c) In which of the following groups is squaring guaranteed to be a permutation? [5 pts]

- ☐ $\mathbb{QR}_p^*$ where p is a prime number such that $2p + 1$ is also prime.
- ☐ $\mathbb{QR}_p^*$ where p is a prime number such that $(p - 1)/2$ is odd.
- ☐ $\mathbb{QR}_n^*$ where $n = pq$, where p, q are primes such that either $p \equiv 3 \pmod 4$ or $q \equiv 3 \pmod 4$ (or both).
- ☐ None of the above.

(d) Suppose $n = pq$, where p, q are distinct prime numbers. Let φ denote the Euler's totient function. Then: [5 pts]

- ☐ $\varphi(n) = |\mathbb{Z}_n|$
- ☐ $\varphi(n) = |\mathbb{Z}_n^*|$
- ☐ $\varphi(n) = (pq - 1)/2$
- ☐ $\varphi(n) = (p - 1)(q - 1)$
- ☐ None of the above.

(e) In the El Gamal encryption scheme, the public-key consists of the specification of a cyclic group $\mathbb{G}$, a generator $g \in \mathbb{G}$ and an element $Y \in \mathbb{G}$.

Then, the ciphertext for a message $M \in \mathbb{G}$, using randomness $r \in$ ______________________________

is ____ . [5 pts]