Problem 1 [10 pt]

- **1 pt** for each part
- **0 pt** if you gave more than one term

Problem 2 [5 pt]

Section 0101

- [1, 4, 3, 5, 2] **5 pt**
  [k is never stored in the file system.]
- 1 not at start **–2 pt**
- 2 not at end **–2 pt**
- [4, 3, 5] not a subsequence **–2 pt**

Section 0201

- [5, 1, 4, 2, 3] **5 pt**
  [user-pwds file has same access as the file with k. So if attacker can access one, it can access the other.]
- [1, 4, 2, 3, 5] **4 pt**
- [1, 4, 2, 3] not a subsequence **–3 pt**
- 5 not at an end **–2 pt**

Problem 4 [5 pt]

- $y \leftarrow n/x$ **[2 pt]**
- $\phi \leftarrow (x-1)\cdot(y-1)$ **[1 pt]**
- $d \leftarrow e{-}1 \bmod \phi$ **[2 pt]**
- [update] **0 pt** or **1 pt** if you say the prime factors of n are not obtainable given x (as mentioned in class).

Problem 5 [5 pt]

Section 0101

- For $i = 1, \cdots, n$:
  $m_i \leftarrow \underbrace{\mathsf{E}_{\mathsf{AES}}(k,\, c_0 + i)}_{\textbf{3 pt}} \underbrace{\oplus\, c_i}_{\textbf{2 pt}}$
- $\mathsf{E}_{\mathsf{AES}}()$ arguments wrong **[–2 pt]**
- $\mathsf{E}_{\mathsf{AES}}()$ missing **[–1 pt]**

Section 0201

- For $i = 1, \cdots, n$:
  $m_i \leftarrow \underbrace{\mathsf{D}_{\mathsf{AES}}(k,\, c_i)}_{\textbf{3 pt}} \underbrace{\oplus\, c_{i-1}}_{\textbf{2 pt}}$
- $\mathsf{D}_{\mathsf{AES}}()$ arguments wrong **[–2 pt]**
- $\mathsf{D}_{\mathsf{AES}}()$ missing **[0 pt]**

Problem 6 [20 pt]

- **Problem 6.1 [7 pt]**: no, yes, yes, yes, no, no, yes **[1 pt for each]**
- **Problem 6.2 section 0101 [5 pt]**
  $\mathsf{Sgn}(sk_A,\, s)$ may or may not allow recovery of s.
  - If you assumed it allows recovery of s: no, no, no, no, no **[1 pt each]**
  - Otherwise: yes, –, –, –, – **[5 pt]** ('–' is don't care)
- **Problem 6.2 section 0201 [5 pt]**: yes, –, –, –, – **[5 pt]** ('–' is don't care)
- **Problem 6.3 section 0101 [6 pt]**: no, yes, no, no, yes, no **[1 pt for each]**
- **Problem 6.3 section 0201 [5 pt]**: no, yes, no, no, yes, yes **[1 pt for each]**
- **Problem 6.4 section 0101 [7 pt]**: no, yes, no, yes, no, yes **[1 pt for each + 1 pt]**
- **Problem 6.3 section 0201 [5 pt]**: no, yes, no, no, yes, no **[1 pt for each + 1 pt]**

Problem 7

- **Grading: all or nothing**