Assignment 1

CSE565 (B&C), Fall 2024, SUNY Buffalo.

Problems	1	2	3	4	5	Total
Max Score	25	15	20	20	20	
Your Score						

Requirements

- Save and submit your HW 1 submission to UB Learns (Brightspace) as a single typed PDF file. Name your file: Your Last Name Your First Name YourStudents ID Number Assignment Number. Example: **Doe John 55552222 HW1**
- You should view your submission after you upload it to make sure that it is not corrupted or malformed. Submissions that are rotated, upside down, or that do not load will not receive credit. Illegible submissions may also lose credit depending on what can be read. You are responsible for making sure your submission went through successfully.
- The HW 1 deadline is **25 Sep, 11:59PM EST**. Late submissions (within 24 hours with 20 % penalty or 48 hours with a 40% penalty or 72 hours with a 60% penalty) should be submitted via Email to Instructor and Head TAs. Submissions will close 72 hours after the deadline.
- Only the most recent submission is kept on UB Learns (Brightspace).

Problem 1 (25 pts)

Consider an automated teller machine (ATM) to which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system.

Problem 2 (15 pts)

Data compression is often used in data storage and transmission. Suppose you want to use data compression in conjunction with encryption. Which of the following approach makes more sense? Encrypt-then-compress, or Compress-then-encrypt, or both? Explain why.

Problem 3 (20 pts)

Show that the shift (Caesar) and substitution ciphers are all trivial to break using a chose-plaintext attack. How much chosen plaintext is needed to recover the key for each of the cipher? You can assume that the plaintext contains only lowercase English letters.

Problem 4 (20 pts)

An attacker intercepts the following ciphertext (hex encoded):

```
20814804c1767293b99f1d9cab3bc3e7 ac1e37bfb15599e5f40eef805488281d
```

He knows that the plaintext is the ASCII encoding of the message "**Pay Bob 100$**" (excluding the quotes). He also knows that the cipher used is CBC encryption with a random IV using AES as the underlying block cipher.

Show that the attacker can change the ciphertext so that it will decrypt to "**Pay Bob 500$**". What is the resulting ciphertext (hex encoded)? Explain how you get the result.

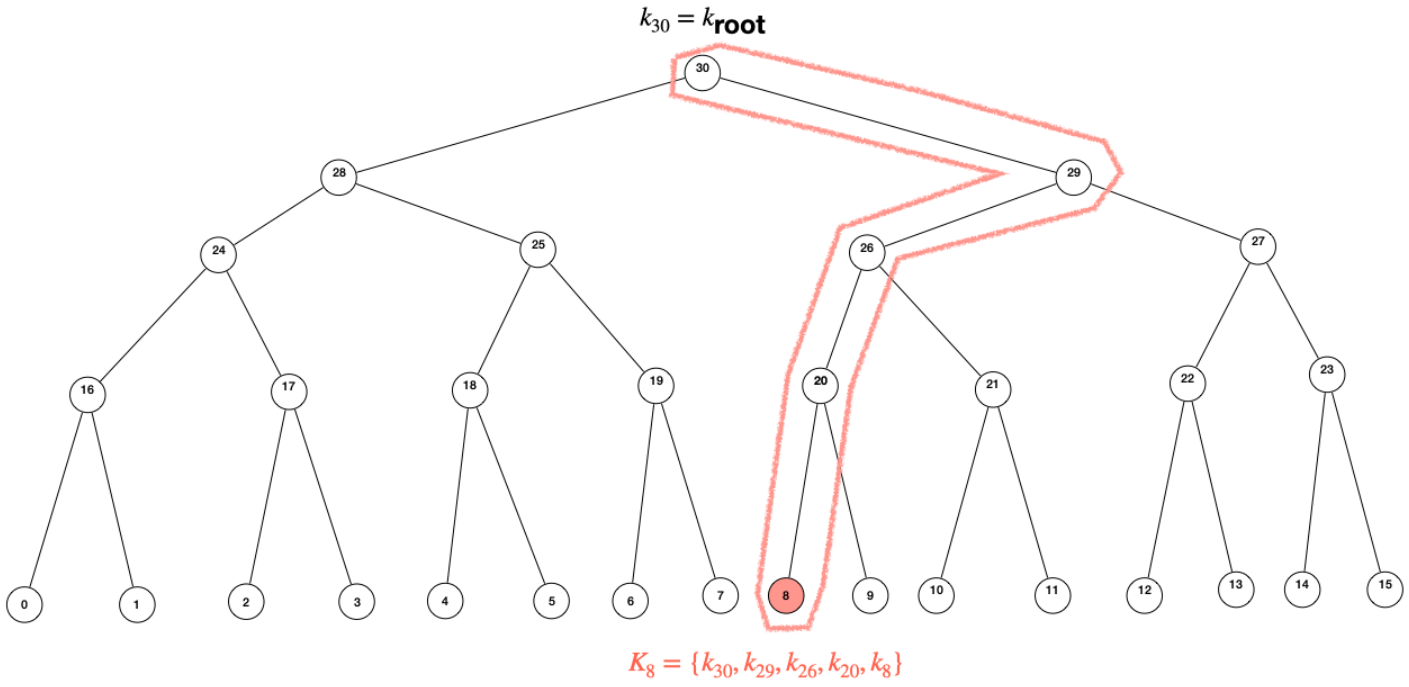
Problem 5 (20 pts)

The movie industry wants to protect digital content distributed on DVD's. We will develop a variant of a method used to protect Blu-ray disks called AACS.

Suppose there are at most a total of n DVD players in the world (e.g. $n = 2^{32}$). We view these n players as the leaves of a binary tree of height $\log_2 n$. Each node in this binary tree contains an AES key k_i. **These keys are kept secret from consumers and are fixed for all time**.

At manufacturing time each DVD player is assigned a serial number $i \in [0, n-1]$. Consider the set of nodes along the path from the root to leaf number i in the binary tree. The manufacturer of the DVD player embeds in player number i all the keys associated with the nodes on the path. Denote K_i as the set of keys possessed by player number i.

For example, in the below figure there are 16 DVD players numbered fro 0 to 15. The player number 8 has all keys along the root-leaf path: $K_8 = \{k_{30}, k_{29}, k_{26}, k_{20}, k_8\}$



When the movie industry release a new DVD movie m, it is encrypted as $E(k_{\text{root}}, k)||E(k, m)$ where k is a random AES key called a content-key and k_{root} is the key associated with the root of the tree. Since all DVD players have the key k_{root} all players can decrypt the movie m. We refer to $E(k_{\text{root}}, k)$ as the header and $E(k, m)$ as the body.

In what follows the DVD header may contain multiple ciphertexts where each ciphertext is the encryption of the content-key
k under some k_i in the binary tree, i.e., the header looks like $E(k_{i_1}, k)||E(k_{i_2}, k)||\cdots||E(k_{i_q}, k)$. So for a DVD player to obtain the content key k, it only needs to have *one of* the k_{i_j} used for encrypting k in the header.

Now consider the following questions:

1. (**10 pts**) In the example shown in the figure, suppose the DVD player 8 is hacked and all of K_8 is exposed in public; Now when the movie industry distributes a new DVD movie, they can encrypt the contents of the DVD using a slightly larger header containing multiple keys so that all DVD players, except for player number 8, can decrypt the movie. What's the least number of keys that should be included in the header to achieve this goal? List these necessary keys.

2. (**10 pts**) In general, suppose there is exactly 1 out of the n DVD players hacked, how many keys are necessary to be included in the header so that this hacked player is ruled out? Explain why.