Quiz. 3

(Deadline March 21, 2024)

For the following selection questions, each answer must be fully explained in your own words for clarity. Merely copying answers from the internet without proper explanation will not be awarded any points.
† indicates that the question is multiple-choice.

Problem 1

† Data compression is often used in data storage and transmission. Suppose you want to use data compression in conjunction with encryption. Does it make more sense to:

☐ Compress then encrypt.

☐ Encrypt then compress.

☐ The order does not matter – either one is fine.

☐ The order does not matter – neither one will compress the data.

Problem 2

† Let G: $\{0,1\}^s \to \{0,1\}^n$ be a secure PRG. Which of the following is a secure PRG:

☐ G'(k) = G(k) ∥ G(k)

☐ G'(k) = G(k $\oplus$ 1^s)

☐ G'(k) = G(0)

☐ G'(k) = G(1)

☐ G'(k) = G(k) ∥ 0

☐ G'(k_1, k_2) = G(k_1) ∥ G(k_2)

☐ G'(k) = reverse(G(k))

☐ G'(k) = $rotation_n$(G(k))

Hint:
"∥" denotes concatenation.
"reverse(x)" reverses the string x so that the first bit of x is the last bit of reverse(x), the second bit of x is the second to last bit of reverse(x), and so on.
"$rotation_n(x)$" rotates the string x by n positions. If n>0, it rotates right; if n<0, it rotates left, and characters shifted off one end reappear at the other.

Problem 3

Let (E, D) be a (one-time) semantically secure cipher with key space K = $\{0,1\}^k$. A bank wishes to split a decryption key k $\in \{0,1\}^k$ into two pieces p_1 and p_2 so that both are needed for decryption. The piece p_1 can be given to one executive and p_2 to another so that both must contribute their pieces for decryption to proceed.

The bank generates random k_1 in $\{0,1\}^k$ and sets k_1' $\leftarrow$ k $\oplus$ k_1. Note that k_1 $\oplus$ k_1' = k. The bank can give k_1 to one executive and k_1' to another. Both must be present for decryption to proceed since, by itself, each piece contains no information about the secret key k (note that each piece is a one-time pad encryption of k).

Now, suppose the bank wants to split k into three pieces p_1, p_2, p_3 so that any two of the pieces enable decryption using k. This ensures that even if one executive is out sick, decryption can still succeed. To do so the bank generates two random pairs (k_1, k_1') and (k_2, k_2') as in the previous paragraph so that k_1 $\oplus$ k_1' = k_2 $\oplus$ k_2' = k. How should the bank assign pieces so that any two pieces enable decryption using k, but no single piece can decrypt?

- ☐ p_1 = (k_1, k_2), p_2 = (k_1, k_2), p_3 = (k_2')
- ☐ p_1 = (k_1, k_2), p_2 = (k_1', k_2'), p_3 = (k_2')
- ☐ p_1 = (k_1, k_2), p_2 = (k_1', k_2), p_3 = (k_2')
- ☐ p_1 = (k_1, k_2), p_2 = (k_2, k_2'), p_3 = (k_2')
- ☐ p_1 = (k_1, k_2), p_2 = (k_1'), p_3 = (k_2')

Problem 4

Let M = C = K = { 0, 1, 2, . . . , 255 } and consider the following cipher defined over (K, M, C):
E(k, m) = m + k (mod 256); D(k, c) = c - k (mod 256)
Does this cipher has perfect secrecy?

- ☐ No, there is a simple attack on this cipher.
- ☐ Yes
- ☐ No, only the One Time Pad has perfect secrecy.

Problem 5

† Let (E, D) be a (one-time) semantically secure cipher where the message and ciphertext space is $\{0,1\}^n$. Which of the following encryption schemes are (one-time) semantically secure?

☐ E'(k, m) = E(0^n, m)

☐ E'((k, k'), m) = E(k, m) ∥ E(k', m)

☐ E'(k, m) = E(k, m) ∥ MSB(m)

☐ E'(k, m) = 0 ∥ E(k, m) (i.e. prepend 0 to the ciphertext)

☐ E'(k, m) = E(k, m) ∥ k

☐ E'(k, m) = reverse(E(k, m))

☐ E'(k, m) = $rotation_n$(E(k, m))

Problem 6

Suppose you are told that the one time pad encryption of the message "attack at dawn" is 6c73d5240a948c86981bc294814d (the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hex). What would be the one time pad encryption of the message "defend at noon" under the same OTP key?

Problem 7

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

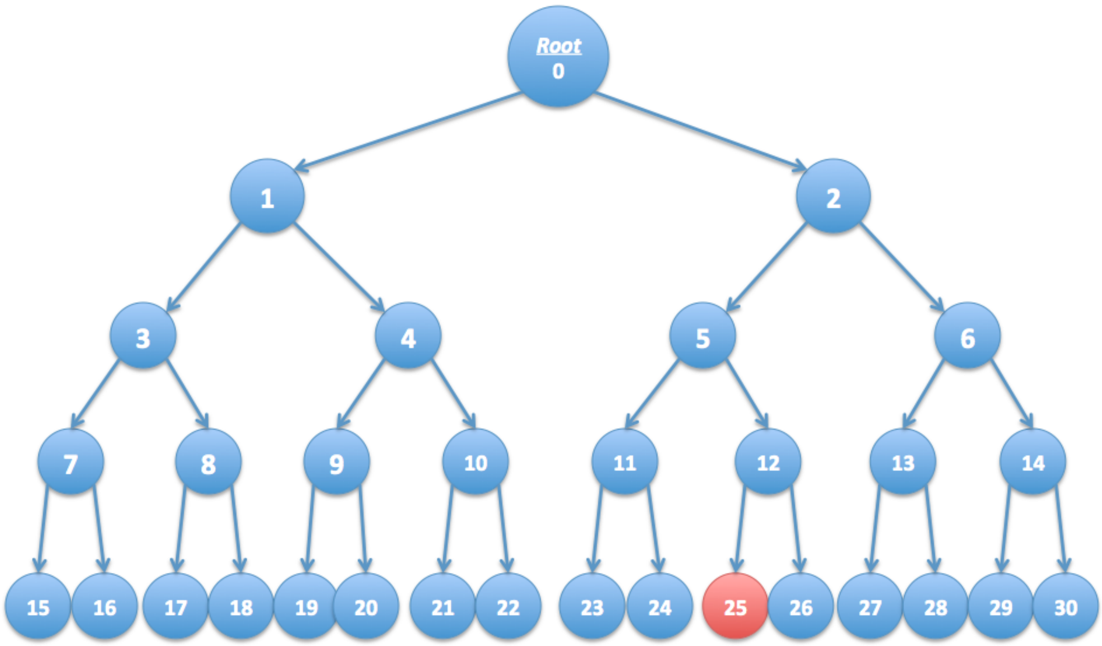
Suppose there are at most a total of n DVD players in the world (e.g. n = 2^{32}). We view these n players as the leaves of a binary tree of height $log_2 n$. Each node in this binary tree contains an AES key k^i. These keys are kept secret from consumers and are fixed for all time. At manufacturing time each DVD player is assigned a serial number i ∈ [0, n-1]. Consider the set of nodes S_i 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 the keys associated with the nodes in the set S_i. A DVD movie m is encrypted as

E(k_{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_{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 key k_i in the binary tree.

Suppose the keys embedded in DVD player number r are exposed by hackers and published on the Internet. In this problem we show that when the movie industry distributes a new DVD movie, they can encrypt the contents of the DVD using a slightly larger header (containing about $log_2 n$ keys) so that all DVD players, except for player number r, can decrypt the movie. In effect, the movie industry disables player number r without affecting other players.

As shown below, consider a tree with n = 16 leaves. Suppose the leaf node labeled 25 corresponds to an exposed DVD player key. Check the set of keys below under which to encrypt the key k so that every player other than player 25 can decrypt the DVD. Only four keys are needed.



- ☐ 21
- ☐ 17
- ☐ 5
- ☐ 26
- ☐ 6
- ☐ 1
- ☐ 11
- ☐ 24

Extra Credit

Did SHA-256 and SHA-512-truncated-to-256-bits have the same security properties? Which one is better? Please explain in detail.

What to turn in:

<student_id>.pdf