Homework 1[1]

Question 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:

1. Compress then encrypt.

2. Encrypt then compress.

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

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

Question 2

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 ”attack at dusk” under the same OTP key?

Question 3

Let $G : \{0,1\}^s \to \{0,1\}^n$ be a secure PRG. Which of the following is a secure PRG (there is more than one correct answer):

1. $G\ (k) = G(0)$

2. $G'(k) = G(k \oplus 1^s)$

3. $G'(k) = G(k) \,\|\, 0$ (here $\|$ denotes concatenation)

4. $G'(k) = \text{reverse}(G(k))$ where $\text{reverse}(x)$ reverses the string x so that the first bit of x is the last bit of $\text{reverse}(x)$, the second bit of x is the second to last bit of $\text{reverse}(x)$, and so on.

[1] https://class.coursera.org/crypto-012/

Question 4

Let $G : K \to \{0,1\}^n$ be a secure PRG. Define $G'(k_1, k_2) = G(k_1) \bigwedge G(k_2)$ where $\bigwedge$ is the bit-wise AND function. Consider the following statistical test A on $\{0,1\}^n$:

$$A(x) \text{ outputs } \mathrm{LSB}(x), \text{ the least significant bit of } x.$$

What is $Adv_{\mathrm{PRG}}[A, G']$? You may assume that $\mathrm{LSB}(G(k))$ is 0 for exactly half the seeds k in K.

Question 5

Let (E, D) be a (one-time) semantically secure cipher with key space $K = \{0,1\}^\ell$. A bank wishes to split a decryption key $K = \{0,1\}^\ell$ 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 $\{0,1\}^\ell$ 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?

1. $p_1 = (k_1, k_2), \quad p_2 = (k_1, k_2), \quad p_3 = (k_2')$

2. $p_1 = (k_1, k_2), \quad p_2 = (k_2, k_2'), \quad p_3 = (k_2')$

3. $p_1 = (k_1, k_2), \quad p_2 = (k_1'), \quad p_3 = (k_2')$

4. $p_1 = (k_1, k_2), \quad p_2 = (k_1', k_2), \quad p_3 = (k_2')$

5. $p_1 = (k_1, k_2), \quad p_2 = (k_1', k_2'), \quad p_3 = (k_2')$

Question 6

Let $M = C = K = \{0, 1, 2, \ldots, 255\}$ and consider the following cipher defined over (K, M, C):

$$E(k, m) = m + k \pmod{256} \qquad ; \qquad D(k, c) = c - k \pmod{256}\ .$$

Does this cipher have perfect secrecy?

Question 7

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?

1. $E'(k, m) = E(k, m) \parallel k$

2. $E'(k, m) = E(k, m) \parallel \mathrm{LSB}(m)$

3. $E'(\ (k, k'),\ m) = E(k, m) \parallel E(k', m)$

4. $E'(k, m) =$ compute $c \leftarrow E(k, m)$ and output $c \parallel c$ (i.e., output c twice)

5. $E'(k, m) = E(0^n, m)$

6. $E'(k, m) = 0 \parallel E(k, m)$ (i.e. prepend 0 to the ciphertext)

Question 8

The movie industry wants to protect digital content distributed on DVD's. We study one possible approach. 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 v_i 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 S_i of $1+\log_2 n$ 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 the $1+\log_2 n$ keys associated with the nodes in S_i. In this way each DVD player ships with $1+\log_2 n$ keys embedded in it (these keys are supposedly inaccessible to consumers). A DVD movie M is encrypted as

$$E(k_{\text{root}}, k) \big\| E(k, m)$$

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 key k_i in the binary tree.

1. Suppose the $1 + \log_2 n$ keys embedded in DVD player number r are exposed by hackers and published on the Internet (say in a program like DeCSS). Show that when the movie industry is about to distribute a new DVD movie they can encrypt the contents of the DVD using a header of size $\log_2 n$ so that all DVD players can decrypt the movie except for player number r. In effect, the movie industry disables player number r.
Hint: the header will contain $\log_2 n$ ciphertexts where each ciphertext is the encryption of the content-key k under certain $\log_2 n$ keys from the binary tree.

2. Suppose the keys embedded in k DVD players $R = \{r_1, \cdots, r_k\}$ are exposed by hackers. Show that the movie industry can encrypt the contents of a new DVD using a header of size $O(k \log n)$ so that all players can decrypt the movie except for the players in R. You have just shown that all hacked players can be disabled without affecting other consumers.

Side note: the AACS system used to encrypt Blu-ray and HD-DVD disks uses a related system. It was quickly discovered that bored hackers can expose player secret keys faster than the MPAA can revoke them.