Congratulations! You passed!

TO PASS 80% or higher

Keep Learning

GRADE
80%

Week 1 - Problem Set

LATEST SUBMISSION GRADE

80%

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 / 1 point

- [x] Compress then encrypt.
- [ ] Encrypt then compress.
- [ ] The order does not matter -- neither one will compress the data.
- [ ] The order does not matter -- either one is fine.

Correct
Ciphertexts tend to look like random strings and therefore the only opportunity for compression is prior to encryption.

2. **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 / 1 point

- [x] $G'(k) = \mathrm{reverse}(G(k))$ where 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.

Correct
a distinguisher for G' gives a distinguisher for G.

- [x] $G'(k) = G(k) \bigoplus 1^n$

Correct
a distinguisher for G' gives a distinguisher for G.

- [ ] $G'(k) = G(k) \parallel G(k)$

(here $\parallel$ denotes concatenation)

- [ ] $G'(k) = G(k) \parallel 0$

(here $\parallel$ denotes concatenation)

- [x] $G'(k_1,k_2) = G(k_1) \parallel G(k_2)$

(here $\parallel$ denotes concatenation)

Correct
a distinguisher for G' gives a distinguisher for G.

- [ ] $G'(k) = G(0)$

3. **Let $G: K \to \{0,1\}^n$ be a secure PRG.**

1 / 1 point

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 $\{0,1\}^n$:

$A(x)$ outputs $\mathrm{LSB}(x)$, 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.

Note: Please enter the advantage as a decimal between 0 and 1 with a leading 0. If the advantage is 3/4, you should enter it as 0.75

0.25

Correct
for a random string x we have $Pr[A(x)=1] = 1/2$ but for a pseudorandom string $G'(k_1,k_2)$ we have $Pr_{k_1,k_2}[A(G'(k_1,k_2))=1] = 1/4$.

4. **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 $k \in \{0,1\}^\ell$ 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.**

1 / 1 point

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?

- [ ] $p_1=(k_1,k_2), \quad p_2=(k_1',k_2'), \quad p_3=(k_2')$
- [ ] $p_1=(k_1,k_2), \quad p_2=(k_1'), \quad p_3=(k_2')$
- [x] $p_1=(k_1,k_2), \quad p_2=(k_1',k_2), \quad p_3=(k_2')$
- [ ] $p_1=(k_1,k_2), \quad p_2=(k_2,k_2'), \quad p_3=(k_2')$
- [ ] $p_1=(k_1,k_2), \quad p_2=(k_1,k_2), \quad p_3=(k_2')$

Correct
executives 1 and 2 can decrypt using k_1, k_1',

executives 1 and 3 can decrypt using k_2, k_2', and

executives 2 and 3 can decrypt using k_2, k_2'. Moreover, a single

executive has no information about k.

5. **Let $M=C=K=\{0,1,2,\ldots,255\}$**

1 / 1 point

and consider the following cipher defined over (K,M,C):

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

Does this cipher have perfect secrecy?

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

Correct
as with the one-time pad, there is exactly one key mapping a given message m to a given ciphertext c.

6. **Let (E,D) be a (one-time) semantically secure cipher where the**

0 / 1 point

message and ciphertext space is $\{0,1\}^n$. Which of the following

encryption schemes are (one-time) semantically secure?

- [ ] $E'(k,m) = E(0^n, m)$
- [ ] $E'(\ (k,k'),\ m) = E(k,m) \parallel E(k',m)$
- [ ] $E'(k,m) = \text{compute } c \leftarrow E(k,m) \text{ and output } c \parallel c$ (i.e., output c twice)
- [ ] $E'(k,m) = E(k,m) \parallel k$
- [ ] $E'(k,m) = 0 \parallel E(k,m)$ (i.e. prepend 0 to the ciphertext)
- [ ] $E'(k,m) = E(k,m) \parallel \mathrm{LSB}(m)$

You didn't select all the correct answers

7. **Suppose you are told that the one time pad encryption of the message "attack at dawn" is *6c73d5240a948c86981bc294814d***

0 / 1 point

(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?

6c73d5240a948c86981bc294814d

! **Incorrect**

8. **The movie industry wants to protect digital content distributed on**

1 / 1 point

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 $i \in [0, n-1]$. 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

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

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 $E(k_{\mathrm{root}},k)$ 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

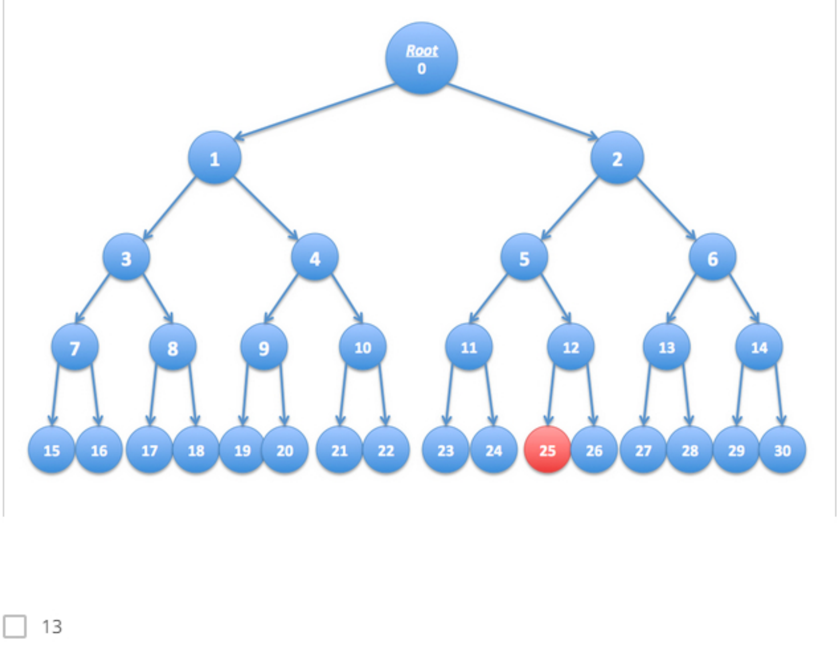
players, except for player number r, can decrypt the movie. In

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.



- [ ] 13
- [ ] 4
- [x] 1

Correct
You cannot encrypt k under the root, but 1's children must be able to decrypt k.

+1

- [ ] 14
- [ ] 0
- [x] 11

Correct
You cannot encrypt k under key 5, but 11's children must be able to decrypt k.

+1

- [x] 6

Correct
You cannot encrypt k under 2, but 6's children must be able to decrypt k.

+1

- [x] 26

Correct
You cannot encrypt k under any key on the path from the root to node 25. Therefore 26 can only decrypt if you encrypt k under key k_{26}.

9. **Continuing with the previous question, if there are n DVD players, what is the number of keys under which the content key k must be encrypted if exactly one DVD player's key needs to be revoked?**

1 / 1 point

- [x] $\log_2 n$
- [ ] 2
- [ ] $\sqrt{n}$
- [ ] $n/2$
- [ ] $n-1$

Correct
That's right. The key will need to be encrypted under one key for each node on the path from the root to the revoked leaf. There are $\log_2 n$ nodes on the path.

10. **Continuing with question 8, suppose the leaf nodes labeled 16, 18, and 25 correspond to exposed DVD player keys. Check the smallest set of keys under which to encrypt the key k so that every player other than players 16,18,25 can decrypt the DVD. Only six keys are needed.**

1 / 1 point

- [x] 26

Correct
Yes, this will let player 26 decrypt.

- [x] 11

Correct
Yes, this will let players 23,24 decrypt.

- [x] 15

Correct
Yes, this will let player 15 decrypt.

- [x] 4

Correct
Yes, this will let players 19-22 decrypt.

- [ ] 29
- [x] 6

Correct
Yes, this will let players 27-30 decrypt.

- [ ] 1
- [ ] 0
- [ ] 23
- [x] 17

Correct
Yes, this will let player 17 decrypt.