CAS CS 357

Discussion Worksheet 1 – Chosen Plaintext Attack (CPA)

1. Perfect Security (Shannon secrecy)
2. In ideal world, plaintext is n bits, cipheredtext is n bits, key is n bits
3. In real world, it is not the case
4. Perfect Secrecy game for the encryption scheme works as follows
5. The adversary chooses two messages m0 and m1. Send m0 and m1 to game master
6. The game master (who knows the secret key k) chooses m0 or m1 at random. In other words, it chooses a random bit b. Then, the game master computes the challenge c\* = Enck(mb) and sends c\* to the adversary
7. The adversary guesses if m0 or m1 was encrypted: outputs a bit b’ (0 or 1) that represents its guess
8. The adversary wins the game if b’ = b
9. The encryption scheme is perfectly secure if the adversary wins the game with probability of exactly ½ or 0.5
10. Chosen Plaintext Attack (CPA)
11. The adversary attemps to break encryption scheme.
12. In CPA, adversary has method of encrypting messages: the adversary ask for message m to be encrypted and see the ciphertext Enc(m)
13. Given this power, the adversary breaks CPA security if it can win perfect secrecy game.
14. However, it cannot choose m0 or m1 to be any message that is already encrypted
15. Example Question 1: Consider an encryption scheme where the first bit of a message is equal to the last bit of its ciphertext. This encryption scheme is not perfectly secure - show an attack.

Adversary:

M0 starts with the bit of 0

M1 starts with the bit of 1

If the returned ciphertext from the game master ends with 0, b’ = 0

If the returned ciphertext from the game master ends with 1, b’ = 1

Here, the adversary can always win, making the encryption scheme not secure

1. Example Question 2: Consider an encryption scheme that works as follows: The plaintext messages m have length 2n. The secret key k has length n. To encrypt, for each bit mi, compute mi ⊕ k⌊i/2⌋ . In other words, XOR 1st two bits of m with the 1st bit of k, the 2nd two bits of m with the 2nd bit of k, etc. This is not a perfectly-secure encryption scheme: show an attack

Adversary

M0 starts with the bit of two same bits (00 or 11)

M1 starts with the bit of two different bits (10 or 01)

If the returned ciphertext from the game master begins with two different bits, outputs b’ = 1 (10 ⊕ 1 produces 01 and 10 ⊕ 0 produces 10) – two different bits as a result

If the returned ciphertext from the game master begins with two same bits, outputs b’ = 0 (00 ⊕ 1 produces 11 and 11 ⊕ 1 produces 00) – two same bits as a result

Here, the adversary can always win, making the encryption scheme not secure

1. Example Question 3: The following “encryption scheme” is not secure. Let k be a n bit key. To encrypt an n-bit plaintext m, output ciphertext c = k ⊕ m. We use the same key k to encrypt every n-bit plaintext message. (The symbol ⊕ is the bitwise XOR; recall that a ⊕ a ⊕ b = b.)
2. Write down the decryption algorithm.

C = k ⊕ m

C ⊕ k = k ⊕ m ⊕ k

C ⊕ k = m

In this case, if the adversary receives the encrypted message and performs XOR operation to the encrypted message with the original message that the adversary sent, the key value is given. The encryption scheme fails therefore in this case since the adversary can find the key using the CPA

k ⊕ m ⊕ m = k 🡪 adversary finds the key value by performing XOR

1. Present an attack that proves that this scheme is not CPA secure.

CPA

Adversary sends message m0 to the game master and receives c, the encrypted version of m0 (Adv 🡪 m0 🡪 game master, game master 🡪 Enck(m0)--> Adv)

Distinguishing Game

Adversary sets m1=m0 but with last bit flipped

Adversary sets m2 as random bits

If the returned ciphertext from the game master gives out encrypted version of m1, the encrypted version should be same as m0, except the last bit. In this case, the adversary outputs b’ = 1

If the returned ciphertext from the game master is not same as m0, the adversary outputs b’ = 2

The idea of CPA is that even if you have the previous sets of messages and its encrypted version, you are not allowed to success in the distinguishing game since the key is independent from one another, making the adversary impossible to success every time.