MIDN ANDRES

SY308

HW03

1. (5 pts) Read the course notes from One-time Pad through Computational Indistinguishability. Honestly declare one of the following:

    a. (0 pt) I didn't read the notes.

    b. (2 pts) I just skimmed the notes.

    c. (3 pts) I read the notes, but I skipped a couple of difficult topics.

    d. (5 pts) I read the notes very carefully and thoroughly.

    Answer: D

2. (5 pts) Solve the quiz candidate problems in the notes from One-time Pad through Computational Indistinguishability. Honestly declare one of the following:

    a. (0 pt) I did nothing.

    b. (2 pts) I looked at the solutions, but didn't attempt to solve the problems on my own. (Recall you should get help from your instructor, if you don't understand the course material.)

    c. (4 pts) I tried to solve **some** of the problems on my own, and then checked the solutions.

    d. (5 pts) I tried to solve **all** problems on my own, and then checked the solutions.

    Answer: D

3. (10 pts: 25 minutes) When using the ℓ-bit one-time pad with the key $k = 0^\ell$ (here, 0^ℓ denotes the ℓ-bit string where every bit is 0, i.e., $0^\ell = \underbrace{00\cdots0}_{\ell \text{ times}}$), it follows that $\mathsf{Enc}_k(m) = k \oplus m = m$ and the message is effectively sent in the clear! It has therefore been suggested to improve the one-time pad by only encrypting with a key $k \neq 0^\ell$; that is,
   - Gen: choose k uniformly at random from the set of **non-zero keys of length** ℓ.

   Is this an improvement? In particular, is it still perfectly indistinguishable? Justify your answer.

   - If your answer is positive, you need to show the modified scheme satisfies the definition of perfect indistinguishability. You can use either of the formulations (game-based or probability-based) that we have seen..
   - If your answer is negative, you need to give a counter-example in the form of an adversary that can win the distinguishing game with non-zero advantage. Also, describe the information (informally) that the adversary gains by observing the ciphertext.

> An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is **perfectly indistinguishable** if and only if for any two messages $M_0, M_1 \in \mathcal{M}$ and any ciphertext $C \in \mathcal{C}$, it holds that
>
> $$\Pr[cipher = C | message = M_0] = \Pr[cipher = C | msg = M_1].$$

This scheme is not perfectly indistinguishable. And is NOT an improvement.

Consider a 2 bit one-time pad
with a key space of $K = \{01, 10, 11\}$
and a message space of $M = \{00, 01, 10, 11\}$
Breaks definition

Gen(): Choose a key K from $\{0,1\}^\ell$ according to the uniform distribution

- $\mathsf{Enc}_K(M)$: Given a key K, and a message $M \in \{0,1\}^\ell$, the encryption algorithm outputs $C = K \oplus M$.
- $\mathsf{Dec}_K(C)$: Given a key K, and a ciphertext $C \in \{0,1\}^\ell$, the decryption algorithm outputs $M = K \oplus C$.

$|K| < |M|$

Adversary A :
1. Choose M0 = 00, M1 = 11.
2. Receive ciphertext C .
3. If C=00 output 0; Else output 1 .

$Pr[A \text{ outputs } 1 \text{ in } Exp_0] = 1$
$Pr[A \text{ outputs } 1 \text{ in } Exp_1] = \frac{2}{3}$

The adversary will always have an advantage because we eliminated one element of the key space, thus it is not completely randomized. If the adversary sends a message of all 0's then they will be able to determine that the key is non-zero. Additionally, the adversary could send a message of all 0's and may be able to find repetition and determine the length of the key or get some insight on it.

4. (10 pts) For each of the following statements, determine whether it is true or not, and briefly justify your answer.

a. In order to communicate securely using symmetric encryption, two parties must first share a common key using a public channel.

FALSE

Justification: The task of sharing the key is often easy to achieve by having the parties physically meet in a secure location; in other cases, sharing a key securely is more difficult. Symmetric encryption itself is not concerned with how the parties got the key, but with how to use it. The key is used to encrypt and decrypt a message; thus, the two parties must share the key but in a physical sense, not in a public channel .

b. The shift cipher with a message size of one character is perfectly indistinguishable.

TRUE

Justification: If we were to implement the shift cipher with a message size of one character the key space would be a size of 26. Thus, it could have at most 26 plaintexts and 26 ciphertexts. And with a message space of on character, where the key is only used once, every outcome would have the same probability (1/26) and thus no advantage for the adversary. Therefore, this scheme is perfectly indistinguishable.

c. One-time pad encryption is perfectly indistinguishable even if the adversary has infinite computational power.

TRUE

Justification: Since there exists a single key that turns any message into any ciphertext, there is no way to know which messages is encoded by a particular ciphertext, meaning that no adversary can ever have an advantage in the distinguishing game.

d. There are some perfectly indistinguishable encryption schemes such that the message space is larger the key space.

FALSE

Justification: The definition of perfect indistinguishability is: An encryption scheme (Gen,Enc,Dec)(Gen,Enc,Dec) with message space M and ciphertext space C is perfectly

indistinguishable if and only if for any two messages $M0,M1 \in M$ and any ciphertext $C \in C$, it holds that

$$Pr[cipher = C \mid message = M0] = Pr[cipher = C \mid msg = M1].$$

If we assume that $|M|>|K|$. And Let M(C) be the set of all possible messages which are possible decryptions of the ciphertext, C. Then M(C) $\{M \mid M = Dec(C)$ for some $k \in K\}$ It is clear that, $|M(C)| \leq$

|K|, but |K|<|M|. Thus, ∃ m0 ∈ M, but !∈ M(C). Pr[M = m0| C = c] = 0 ≠ Pr[M = m1].

Which violates the definition of perfect indistinguishability. The key space must be the same or larger size than that of message space.

e. A5/1 is not a security problem for modern phones which support better ciphers like SNOW-3G.

FALSE

Justification: A5/1 is still a lingering problem for older devices that can only use GSM. These devices have no option to use a better cipher and should be considered insecure at all times. However, even modern phones support GSM and thus A5/1. They prefer not to use it, but there are examples of certain technologies (such as Stingray devices) which can force a phone to use GSM and thus fall back on an insecure communication medium.