CSE 667, Assignment 1

**Due:** Wednesday, September 16, 2020, by 11:59 pm.

**Note 1:** The total mark for this assignment is **30**.

**Note 2:** You should*NOT*directly copy anything from slides or other resources. You may get theideas from slides but what you submit *must be in your own words*. Any help must be acknowledged.

1. Can a quantum computer break OTP? Prove your claim. (**6 points**)

Although quantum computers will eventually break a lot of modern Cryptographic

Techniques, OTP practices perfect secrecy and is unbreakable as long as a pad is not

used more than once.

Recall that the way OTP works is that a given message is XORed with a a key to produce

Ciphertext. Within the XOR process; however, is a very important property. When the

the key is chosen as an independent uniform variable on {0,1}n paired with our

message, the ciphertext produced will also be a uniformly random variable on {0,1}n.

The XOR of the ciphertext (uniform variable) with the key (independent

uniform variable) will produce a plaintext that is a random variable over {0, 1}n. A

message with equal probability of all other messages in the messagespace, telling the

attacker nothing about the validity of the message solely from the ciphertext, regardless

of its abilities to try every possible key quickly. This prevents even a quantum computer

the ability to crack OTP.

1. For each of the following determine whether it is true or false. **(4 points)**

If the attacker cannot recover the secret key then the cipher is secure

False. (If someone sneaks into my house and steals my ssh key, it doesn’t say

anything about the security of the cipher under Shannon’s definition, security is

determined by whether the ciphertext reveals anything about the plaintext

* 1. Stream ciphers are malleable

True. A bad guy can XOR an obtained ciphertext with a known ciphertext and send it

to the intended recipient, with the recipient being completely unaware of the

change

* 1. An insecure PRG is predictable

True. If even a single bit of a PRNG is predictable, the PRNG is insecure

* 1. A secure PRG is unpredictable

True. If all bits are unpredictable, the PRNG is secure

1. Describe in details three security issues in 802.11b WEP. Also, explain how 802.11b WEP could be constructed in a more secure way. (**8 points**)

Recall that 802.11b WEP uses what is known as the IV (Initialization Vector) to build

the key that is used to code messages across devices that make use of this protocol

(from class, the network example). As a result, three problems discussed in class arrive

1. IV is only 24 bits long (only 224 = 16777216 total possible IVs)
2. IVs are repeated after only 16M frames of data
3. After power cycle in some of these cards, IV resets to 0 automatically

All of these issues make this protocol easily crackable. To address potential fixes to the

Construction in order

1. Make the IV longer (some of the keys in the modern day are 128 or 256 bits that we have discussed in class so far) making it less susceptible to brute force.
2. Avoid cheaping out and using secure hardware-based RNGs or PRNGs that do not recycle IVs (I personally have a one-time password token that implements this change)
3. Powercycle should never reset the IV to a fixed value
4. When using the one-time pad with the key *k =* 0*ℓ*, the message is sent in the clear! It has therefore been suggested to modify the one-time pad by only encrypting with *k ≠* 0*ℓ* (i.e., to choose *k* uniformly at random from the set of *nonzero* keys of length *ℓ*). Is this modified scheme still perfectly secret? Explain. (**6 points**)

Recall that one of the main principles of perfect secrecy is that idea that |K| >= |M|, or that the number of potential keys must be greater or equal to the number of potential messages. Let’s suppose the optimal space provided by OTP, where |K| = |M| (the keyspace and messagespace have the same number of elements. By removing the all-zero key for a key of a particular length, we break the inequality, |K| = |K| - 1 < |M|

Since the keyspace is smaller than the messagespace, we have broken perfect secrecy, and the modified scheme is no longer perfectly secret.

1. Prove that in a semantically secure encryption scheme no bit of plaintext is revealed to an *efficient* adversary. Generally, in a semantically secure encryption scheme it is *infeasible* to learn anything about the plaintext from the ciphertext (i.e., impossibility inthe case of perfect secrecy is replaced by infeasibility). (**6 points**)

Recall that in layman’s terms, advantage is the ability of an adversary to distinguish

Between a created randomizer (Numbers pulled from PRNG) and a statistical

randomizer (Numbers pulled from a uniformly random distribution)

For an encryption scheme to be semantically secure, for all possible efficient

adversaries, the advantage value for an adversary to determine information from a

given encryption scheme must be negligible (Really small).

We propose a ‘game’ to test an adversary’s advantage. The adversary sends the

challenger two messages, the challenger chooses one of those messages, encrypts it

and sends it back. If the adversary can determine which message is the one that is

Encrypted, the adversary possesses perfect advantage (denoted 1), and if they cannot,

their advantage is nonexistent (0).

With that in mind, for the sake of argument, let’s suppose that an adversary is aware

of exactly one bit of data of the plaintext, and let’s fix that as the LSB (Least Significant

Bit). Let’s create two messages, one with the LSB as 0, and one with the LSB as 1,

called m0 and m1 respectively. The adversary sends both messages to the challenger, the challenger encrypts one, and then sends it back. Normally, determining which plaintext the ciphertext would be an issue, however, as established in the first line, the adversary is made aware of exactly one bit(the LSB). Since the adversary knows the LSB, if the LSB of the returned cipher text’s plaintext is 0, the adversary knows this is m0, and m1 if the opposite is true. As such, the advantage of the adversary given by the equation

Adv [A, E] = | Pr[EXP(0)=1] - Pr[ EXP(1)=1| = | 0 - 1 | = 1 (Perfect Advantage, non negligible.

The above equation is provided directly by Dr. Bibak (which I wanted to offer for clarity even though it is written nearly verbatim), but in summary, it essentially

Says that the advantage of our adversary choosing correctly in this encryption scheme is equal to the difference between the adversary choosing m1 in experiment 0 (where the LSB is 0) and the adversary choosing m1 in experiment (where the LSB is 1) is | 0 - 1 | = 1. Since 1 represents perfect advantage, an adversary knowing even 1 bit of plaintext breaks an encryption scheme's semantic security. By this proof by

contrapositive (a semantically secure encryption scheme cannot allow even one bit of plaintext to be known), we show that a semantically secure encryption scheme

requires that not a single bit of plaintext is revealed.