**Cryptography Engineering Midterm**

April 2022

**Problem 1 (20 pt)**

In the following let p be a prime. The set is a group with respect to addition modulo (i.e. every element in has an inverse such that . The set is a group with respect to multiplication modulo (i.e. every element in has an inverse such that .

**Another cipher with perfect secrecy**. Consider the following cipher.

Let be the message space, the key space and the ciphertext space.

Alice and Bob share a key uniformly chosen at random. To send a message to Bob, Alice computes the ciphertext .

1. Prove that this cipher provides perfect secrecy using the criterium we proved in class.
2. Why one-time pad is a perfect secrecy?
3. Is the use of one-time pads susceptible to statistical analysis (especially if it is known that the plaintext is in American English?
4. Did public-key encryption scheme provide perfect secrecy? We assume there is a public-key encryption scheme (KeyGen,Enc,Dec) with perfect correctness (i.e., for all messages M and valid key-pairs (**PK,SK**), we have Decsk(Encpk(M))=M

**Problem 2 (20 pt)**

**Predicting generators.** Consider the following *congruential generator*. It uses constants . The seed is a value . The value generated is computed as

The sequence output by the generator is  Assume that an attacker knows and witness the sequence.

1. Prove that after a short prefix (i.e. a few of the values ’s) the attacker is able to predict the rest of the sequence (i.e. the rest of the ’s).
2. What does this say about the security of using the congruential generator as the keystream generator for a stream cipher?
3. If an attacker knows constants and . How many output bits did the attacker to know to rest sequences.
4. However, If an attacker knows but know nothing about constants . In this case, How many output bits did the attacker need to know to recover the rest sequence?

**Problem 3 (10 pt)**

**Non-linear Composition of LFSRs**. Consider the follow LFSR-based generator . It is composed by three LFSR’s . Let be the output of register at clock pulse . Then

where denotes the complement of bit . Prove that

**Problem 4 (10 pt)**

**Passwords with insecure keyboard**

Consider the following scenario:

Alice wants to login on a computer system. In order to gain access, she has to communicate her password to the system.

However, the keyboard (and the cable connection between the keyboard and the system) cannot be trusted since there may be a passive adversary recording the key strokes or tapping the line.

Conversely, let us assume that the display and computer used by Alice (and the connection between the system and the display) is secure, meaning it cannot be monitored by an adversary.

Devise a password protocol that will allow Alice to access the system without disclosing her password to the adversary.

*Hint: You may apply Zero Knowledge Protocol.*

**Problem 5 (15 pt)**

LFSR encryption algorithms to encrypt plaintext are theoretically breakable but if it is possible that you could add some improvement practical scheme to make a LSFR unbreakable. Please explain your methods.

*Hint:https://crypto.stackexchange.com/questions/12754/can-a-lfsr-be-cryptographically-secure*

**Problem 6 (10 pt)**

1.We have an Affine Ciphers  How many keys are possible i.e. the key space

*Hint: are relatively prime therefore GCD* *, and we can always take*

2.What is the key space for a Substitution Cipher 26

3.What is the key space for a Caesar Cipher 26.

**Problem 7 (25 pt)**

Alice and Bob share a secret key *k*. Bob wants an assurance that the message he receives are really coming from Alice. In order to obtain this Alice sends the message *m* and a MAC along with it .

We say that a MAC is secure against chosen message attack if an attacker Eve, after requesting the MAC of n messages of her choice will not be able to produce a new message and a valid .

Recall CBC-MAC, a way of implementing MACs using symmetric encryption scheme. Let

Be a block cipher with key k for example with l = 64, f could be DES.) Let m be a message of length bl bits.

Where denotes concatenation and mi is a block of length l bits. The MAC of m is computed using the cipher f in CBC mode:

(a) Show that the CBC-MAC does not support variable length input. That is show that if messages have variable length it is possible to device a chosen message attack.  
Hint: The idea is to ask for the MACs of two messages of length and construct from them the MAC of a message of length .

(b) Suppose the length of the message is always smaller that . An attempt to get around the above problem would be to append the length of the message at the end as an extra block, before computing the MAC. Show that it is still possible to mount an effective chosen message attack.

**Problem 8 (20 pt)**

Eve intercepted a 4,096 bits encrypted voice message she devised a method to decrypt this encrypted message.

Eve notice that the underline plaintext voice in between Alice and Bob was coding by continues variable slope delta modulation (CVSD).

As we know CVSD is a delta modulation with variable step size (i.e., special case of adaptive delta modulation). As we know CVSD encodes at 1 bit per sample, so when voice is silent the plaintext will be encoded as 010101010101010101010101010

On the contrary, when speech it was encoded as 000000000011111111111110000000000111111111100000000.

Please find out your best way to help Eve break this 4,096 bits ciphertext and save the recovery plaintext into a binary file.

Hint1: You may apply Berlekamp-Massay algorithm to decrypt this ciphertext

Hint2: The key is generated by a lfsr whose length is at most 32

Hint3: The initial seed of the lfsr is 1.

|  |  |
| --- | --- |
| Length of lfsr | Seed (binary) |
| 3 | 001 |
| 5 | 00001 |

Note: Your program should read the bitstream from a file named “ciphertext.bin” and save the plaintext into “plaintext.bin”.