600.472 Theoretical Cryptography January 29, 2008

Handout 1: Homework 1

Instructor: Susan Hohenberger *TA: Matthew Green*

DUE: February 12, 2008 at the start of lecture.

Please review the guidelines on the course website for homework and collaboration policies. You are encouraged to collaborate with other students on the homework, but you must (1) submit your own individually written solution, (2) list your collaborators, and (3) cite any other external sources used. Do not submit a problem solution which you cannot explain orally to the course staff.

A latex template for typing up your homeworks is available on the course website.

Problem 1 *The Wide World of Cryptography (5 points)*

In three sentences or less, state what you hope to get out of this course.

Problem 2 *Historical Ciphers and their Cryptanalysis (15 points)*

1. Bob was passing a note to Alice in class and you intercepted it! You know that they are encrypting their messages using a substitution cipher, but you don't know the permutation they are using. Nevertheless, decrypt Bob's note:

   ```
   INAD N WJACMF PNF XJJA FOQZ QY WVQZEP. QNHF EPNE YOQMVCFP YQV N
   EPQMFNAT DJNVF TQ AQE FLVCAW ML CAEQ XJNMED OCHJ N VJJT.
   ```

2. Encrypt the message "`all is clear`" using the Vigenère cipher with key $k =$`sky`.

Problem 3 *Voting (30 points)*

There are n professors (warlords) in a room. Together they want to determine whether a majority supports the current Dean (kingpin); individually no one wants to announce in public whether they champion the candidate or prefer to oust her. Indeed, the consequences of making such information public could be dire for those in the minority.

We let professor i's vote $v_i = \{0, 1\}$ represent "no" or "yes." The professors exchange messages as follows:

```
Algorithm 1: Voting Protocol: Professor $i$ proceeds as follows on input $v_i$
Uniformly pick $x_{i,1}, \ldots, x_{i,n} \in \{0, 1, \ldots, 2n-1\}$ s.t. $\sum_{j=1}^{n} x_{i,j} = v_i \bmod 2n$.
Send $x_{i,j}$ to professor $j$.
Wait to receive a messages $x_{j,i}$ from each other professor $j$.
Compute $s_i = \sum_{j=1}^{n} x_{j,i} \bmod 2n$. Send $s_i$ to everyone, and wait to receive back a
message $s_j$ from professor $j$.
Compute $S = \sum_{j=1}^{n} s_j \bmod 2n$ and output $S$ as the tally of the votes.
```

1. Describe how to implement line 1. Prove your answer is correct.

2. Prove that if all professors follow the protocol, then S will be the tally of their votes.

3. In this problem, you are asked to devise a meaningful definition of *perfect secrecy* for this protocol in two steps. Intuitively, we do not want any set of colluding parties to learn the votes of any honest party. Note that this is not possible when all the honest parties have voted in the same way. As the first step, briefly explain why the impossibility exists.

   Next, as long as there is at least one honest party that votes yes, and one that votes no, provide a definition of *perfect secrecy* that states that if all parties follow the protocol, then the vote of each individual professor i remains perfectly secure, even if a group C of less than $n-1$ professors collude to try and learn i's vote.

4. Prove that the scheme meets this definition. (Hint: use part 1.)

5. Does the protocol still work if one of the professors deviates from the protocol instructions? Explain either way.

Problem 4 *One-Way Functions (20 points)*

Three notions of one-way functions were discussed in class: (1) worst-case OWF, (2) weak OWF, and (3) strong OWF. We learned that (3) $\Rightarrow$ (2) $\Rightarrow$ (1), i.e. a strong OWF is also a weak OWF and a weak OWF is also a worst-cast OWF. In this problem you will show that (1) is strictly weaker than (2), and (2) is strictly weaker than (3).

1. Assume f is a strong OWF. Construct a function g that is a weak OWF, but not a strong OWF. To show that the constructed function g is a weak OWF, you need to prove that if there exists a non-uniform PPT algorithm A that inverts g (with "high" probability), then there exists a non-uniform PPT algorithm A' that inverts f with non-negligible probability.

2. Assume g is a weak OWF. Construct a function h that is a worst-case OWF, but not a weak OWF.

Problem 5 *Playing with Primitives (30 points)*

Let $F : \{0,1\}^* \to \{0,1\}^*$ be a one-way function. Let $P : \{0,1\}^* \to \{0,1\}^*$ be a one-way permutation. Let $T : \{0,1\}^* \to \{0,1\}^*$ be a trapdoor permutation. (For this problem, we consider only *strong* one-wayness. See lecture notes for formal definitions.) Let $F \circ P$ denote the composition of functions F and P, that is $F \circ P(x) = F(P(x))$. Now, for each of the following, answer either yes or no, and then prove your answer. If you answer no, prove your answer is correct by providing a counterexample. In order to provide this counterexample, you may need to assume the existence of some other F' or P' and then describe how F and P can be constructed from them such that F is still a OWF or P is still a OWP, and yet the question is no for this F and P.

1. Is $F \circ F$ a OWF?

2. Is $P \circ P$ a OWP?

3. Is $P \circ F$ a OWP?

4. Is $P \circ F$ a OWF?

5. Is $T \circ P$ a TDP?

External credit: Part of problem 2 is taken from *Official's Cryptograms* (volume omitted). In general, credit to external sources will only be given in the homework solutions.