CSE 5852: Problem Set 7

Due: November 14, 2016

This assignment is different than previous assignments. Rather than solving problems we are going to read a seminal paper in cryptography. This was the first paper to propose a public-key cryptosystem: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" published in 1977. It is available here. This paper won the authors the Turing Award in 2002 see info here.

Your assignment is to read the paper and answer the following questions.

1. **10 pts** What does the paper claim is the main contribution of the work?
2. **3 pts** Who are Alice and Bob?
3. **10 pts** In section II the paper introduces four properties of a public key cryptosystem. Define (mathematically) each of these properties.
4. **10 pts** This section mentions the topic of a trapdoor function. Describe in words what is meant by a trapdoor function.
5. **5 pts** What is a public file?
6. **5 pts** How does the paper distinguish between authentication and a signature?
7. **5 pts** What is the proposed method for encryption? Consider the encryption scheme as presented in Section V. Provide a mathematical description for the $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ of this scheme.
8. **5 pts** How does it compare to the signature algorithm presented in class?
9. **3 pts** The paper introduces the concept of a public file. What is the public file?
10. **5 pts** Recall we showed that f_e is a permutation on $\mathbb{Z}_N^*$ and showed that f_d is an inverse permutation. For both signatures and encryption, this work assumes messages are an arbitrary message from $\{0, ..., N-1\}$. What is wrong with treating messages this way?
11. **5 pts** Give one reason why the scheme is not secure according to the definition of polynomially secure. The definition is recalled below.

    Definition 1. *A public-key cryptosystem for* 1*-bit messages is polynomially-secure if for all polynomial time* $\mathcal{A}$ *there exists a negligible function* $\epsilon(n)$ *such that*

    $$|\Pr_{pk,sk,\mathsf{Enc}}[\mathcal{A}(pk, \mathsf{Enc}(pk, 0)) = 1] - \Pr_{pk,sk,\mathsf{Enc}}[\mathcal{A}(pk, \mathsf{Enc}(pk, 1)) = 1]| < \epsilon(n).$$

12. **3 pts** How are e, d defined in this paper? (Its different from how they were defined in class.)

13. **10 pts** Provide a brief summary of the primality test recommended in the paper.

14. **5 pts** To quote the paper "Since no techniques exist to *prove* than an encryption scheme is secure, the only test available is to see whether anyone can think of a way to break it." Based on your experience in the class, do you agree? Why or why not?

15. **10 pts** What are the four ways the authors consider that one could compute f_d?

16. **10 pts** Do you think the authors implicitly have a security definition in mind for the encryption scheme, if so what is it?