

HW # 2

Due Date: Wednesday, September 19th, 2007, 7:20 PM
at the beginning of class

Reading Assignment:

- W. Stallings, *Cryptography and Network Security*, Preface, Chapter 1.
- A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, Chapters 1.1–1.2, 1.4.

Problems:

1. (5 points) Anderson claims in the paper *Why Cryptosystems Fail* that implementations of RSA should use at least a 500-bit key. Considering that this paper is about 10 years old, which key length should be chosen today for a reasonable level of security. Give a reason for your answer (Hint: look at RSA Challenge).
2. (8 points) In this problem we use the DES block cipher with 64-bit input x , 64-bit output y , and 56-bit key k . We use it to construct a message authentication code MAC.
 - (a) Draw the diagram on how to build a MAC using the DES block cipher. And show the size of the output of this MAC.
 - (b) Now we use this MAC to generate authentication codes and we keep the key constant. After how many random inputs do we have a probability of $\epsilon = 0.5$ for a collision? After how many random inputs do we have a probability of $\epsilon = 0.2$ for a collision?
3. (15 points) In this problem we will compare the security services which are provided by digital signatures (DS) and message authentication codes (MAC). We assume that Oscar is able to observe all messages send from Alice to Bob and vice versa. Oscar has no knowledge of any keys but the public one in case of DS. State whether and how (i) DS and (ii) MAC protect against each attack. The signature $sign(x)$ is computed with a DS or a MAC algorithm, respectively.
 - (a) (Message integrity) Alice sends a message x ="Transfer \$1000 to Mark" in the clear and also sends $sign(x)$ to Bob. Oscar intercepts the message and replaces "Mark" with "Oscar". Will Bob detect this?

- (b) (Replay) Alice sends a message x = "Transfer \$1000 to Oscar" in the clear and also sends $sign(x)$ to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this?
- (c) (Sender Authentication with cheating 3rd party) Oscar claims that he sent some message x with a valid $sign(x)$ to Bob but Alice claims the same. Can Bob clear the question in either case?
- (d) (Authentication with Bob cheating) Bob claims that he received a message x with a valid signature $sign(x)$ from Alice e.g. "Transfer \$1000 from Alice to Bob" but Alice claims she has never sent it. Can Alice clear this question in either case?
- (e) (Authentication with Alice cheating) Alice produces the message "Transfer \$100.000 from Bob to Oscar's account" and appends it with a valid signature $sign(x)$. She then claims that she received this message from Bob. Can Bob prove that he could not have signed this message? Hint: Oscar is Alice's little brother.